Krasznay Csaba

A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban[1]

A kibertérben történő események vitathatatlanul hatással vannak a fizikai világra, ezt 2017 még azok számára is megtanította, akik magukat a lehető legjobban megpróbálják kizárni a digitális létből. Elég csak arra gondolni, hogy januárban beiktatták az első amerikai elnököt, akinek a megválasztásában fontos szerepet játszott a közösségi hálózatokon keresztüli befolyásolás egy külső szereplő által, vagy éppen arra, hogy a magyar médiát egy informatikai támadás és annak utózöngéi uralták majdnem egy hónapon keresztül augusztusban. De érdemes megemlíteni azt a két globális kártékonykód-kampányt (Wannacry, NotPetya), amely májusban és júniusban több országban és iparágban is komoly károkat okozott, bemutatva a kiberfegyverek lehetséges hatásait. Mind olyan esemény, amelyre az ország védelmében részt vevő szervezeteknek reagálniuk kell. Kérdéses viszont, honnan lesznek olyan közszolgálati szakemberek, akik érdemben tudnak reagálni a nagyon sokszor nem műszaki természetű kihívásokra. Jelen tanulmány áttekinti, milyen kibervédelmi képességekre van szükség Magyarországon, hogyan lehet ezeket megteremteni, illetve milyen szerepe van mindebben a Nemzeti Közszolgálati Egyetemnek.

Kulcsszavak: *kiberbiztonság, oktatás, közszolgálat, védelem*

Krasznay Csaba: Educational Issues of Strategic Aspects of Cyber Security in Public Service

Events in cyberspace have an indisputable impact on the physical world, and 2017 taught this even for those who try to exclude themselves from digital existence. Just to think that the first American president was inaugurated in January, whose election was seriously influenced by an external actor using social networks or the fact that the Hungarian media was dominated by an IT attack and its effects almost for a month in August. But it is worth mentioning the two global malicious code campaigns (Wannacry, NotPetya) that caused massive damage in May and June in several countries and industries, demonstrating the potential impact of cyber-weapons. These are events that organizations participating in the country's defense must respond. It is questionable, however, where are those public service professionals who are able to respond to the many-time non-technical challenges? This paper looks at what kind of cyber defense capabilities are needed in Hungary, how to create them, and what role has the National University of Public Service in that.

Keywords: *cyber security, education, public service, defense*

[1] A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosító számú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Bevezetés

A 21. század embere visszavonhatatlanul kibővítette a saját életterét, a fizikai lét mellett az informatikai eszközök és ezek hálózatai által alkotott virtuális tér is meghatározó a modern társadalom működésében. Ez az állítás igaz minden országra és gyakorlatilag a Föld teljes lakosságára, annak ellenére, hogy a Nemzetközi Távközlési Egyesület *(International Telecommunication Union – ITU)* friss statisztikája szerint a Föld népességének csupán 48%-a használja aktívan az interneten elérhető szolgáltatásokat.[2] Igaz, hiszen az államok és a privát szféra szereplőinek infokommunikációs eszközei nélkül az egyes gazdasági szektorok működésképtelenek lennének, így sokszor közvetve ugyan, de mindannyiunk életére hatással vannak a legtöbb ember számára megfoghatatlan, értelmezhetetlen és sokszor teljesen érdektelen műszaki megoldások. Így annak ellenére, hogy a legtöbben a virtuális tér biztonságával kapcsolatos kérdéseket mérnöki problémának tartják, ez a megközelítés napjainkban tarthatatlanná vált, hiszen egyre többször kell megfelelő válaszokat adni a nemzetbiztonság, a katasztrófavédelem, a belbiztonság, a honvédelem vagy éppen a nemzetközi biztonságpolitika szakterületére tartozó kihívásokra. Az államoknak tehát komoly felelősségük van a saját állampolgáraik védelmében, ami felkészült közszolgálati szakemberek nélkül nem megvalósítható.

Ez az új nézőpont követeli meg azt, hogy bevezessük és használjuk a *kiberbiztonság* fogalmát a szűkebb értelmű, elsősorban műszaki megközelítésű *információbiztonság* helyett. A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (továbbiakban Ibtv.) jól mutatja a két fogalom közötti különbséget.[3] Eszerint az elektronikus információs rendszer biztonsága, „az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos", míg a kiberbiztonság „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez". Hasonló megközelítést mutat Magyarország Nemzeti Kiberbiztonsági Stratégiája is, amelynek „célja, hogy az Alaptörvény elveivel összhangban, az értékek és érdekek számbavétele, valamint a kibertér biztonsági környezetének elemzése alapján meghatározza azon nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is", tehát közel sem a mérnöki feladatokra koncentrál.[4] A kiberbiztonság fogalmának helykeresését és elfogadottságát azonban jól mutatja a mérnöki társadalomban Veres-Szentkirályi András, Magyarország egyik legjobb információbiztonsági szakemberé-

[2] International Telecommunication Union: ICT Facts and Figures 2017, [online]. Forrás: *itu.int* [2017. 07. 31.].
[3] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
[4] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

nek Facebook-bejegyzése: „Tulajdonképpen nincs baj ezzel a »kiber« dologgal, jó heurisztika a megléte arra, hogy felmérhesd a beszélgetőpartner komolyságát."

Az államoknak, így Magyarországnak is biztosítania kell kiberterének védelmét, amely megkívánja az egyes közszolgálati hivatásnemekben olyan szakértők jelenlétét, akik a szükséges és elégséges mértékben értik az információbiztonság műszaki megközelítését, de saját szakterületükön is magas szintű hozzáértésről tesznek tanúbizonyságot. Bányász Péter tanulmányában az alábbiakat írja a közösségi média jelentette fenyegetésről: „Nem szabad eltekinteni attól, hogy a bemutatott műveletek komoly nemzetbiztonsági fenyegetésként jelentkeznek, amennyiben a befolyásolási kísérlet hatására a belpolitikai döntéshozatal valamilyen külső érdeknek megfelelő módon történik. Ez akár a szuverenitás csökkenését is eredményezheti megítélésem szerint. Hatással lehet a szövetségi rendszerünkre, ami többek között nemzetgazdasági, védelempolitikai területen is nemzetbiztonsági fenyegetésként értékelhető."[5] A közösségi média pedig csak egy a számos, virtuális térből érkező fenyegetés közül. Jelen tanulmány azt vizsgálja, hogy az egyes hivatásnemek milyen kiberbiztonsági képességeket kívánnak meg, ezt milyen oktatási metódusokkal lehet támogatni, illetve mit jelent a „szükséges és elégséges" műszaki tudás az alapvetően a gazdasági és jogtudományok területén képzettséget szerzett szakértőknek. A javaslatok a nemzetközi kiberbiztonsági oktatási rendszerek áttekintése mellett a kiberbiztonságért felelős szervezetek vezetőivel készült mélyinterjúk alapján készültek.

Kiberképességek a közszolgálatban

Petró Csilla és Stréhli-Klotz Georgina 2014-es cikkükben részletesen kifejtik, hogy „az állami feladatok biztonságos és hatékony ellátása érdekében hangsúlyt kell fektetni a feladatellátást végző személyi állomány minőségére, munkavégzési képességére, közérzetére" mindhárom hivatásrend (civil közigazgatás, rendvédelmi, honvédelmi) esetében.[6] Ez különösen igaz azokra, akik a kiberbiztonsági területen dolgoznak, hiszen egyrészt főleg a fiatalabb, 20–30 éves korosztály választja magának ezt a területet, akiknek a szigorú szabályok szerint működő közszolgálat esetleg túl kötött lehet, másrészt a piaci szféra elszívó hatása minden más specializációnál komolyabban jelentkezik, hiszen globális szinten egymillió betöltetlen kiberbiztonsághoz kapcsolódó állás van, jóval magasabb bérezéssel, mint amit az államok biztosítani tudnak.[7] A magyar közszolgálatból Rajnai Zoltán, Magyarország kiberkoordinátorának közlése szerint 2000 szakember hiányzik.[8] Fontos tehát meghatározni, milyen képességfejlesztés szükséges hazánk kibervédelmének megerősítéséhez rövid és középtávon.

Hazánk kibervédelmi rendszere egyrészt erősen centralizált, hiszen a feladatok nagy része a Belügyminisztérium alá tartozó szervezeteknél jelenik meg, rajta kívül

---

5 Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében, *Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata,* 13. évf., 2016/1, 61–81. o., 76. o.

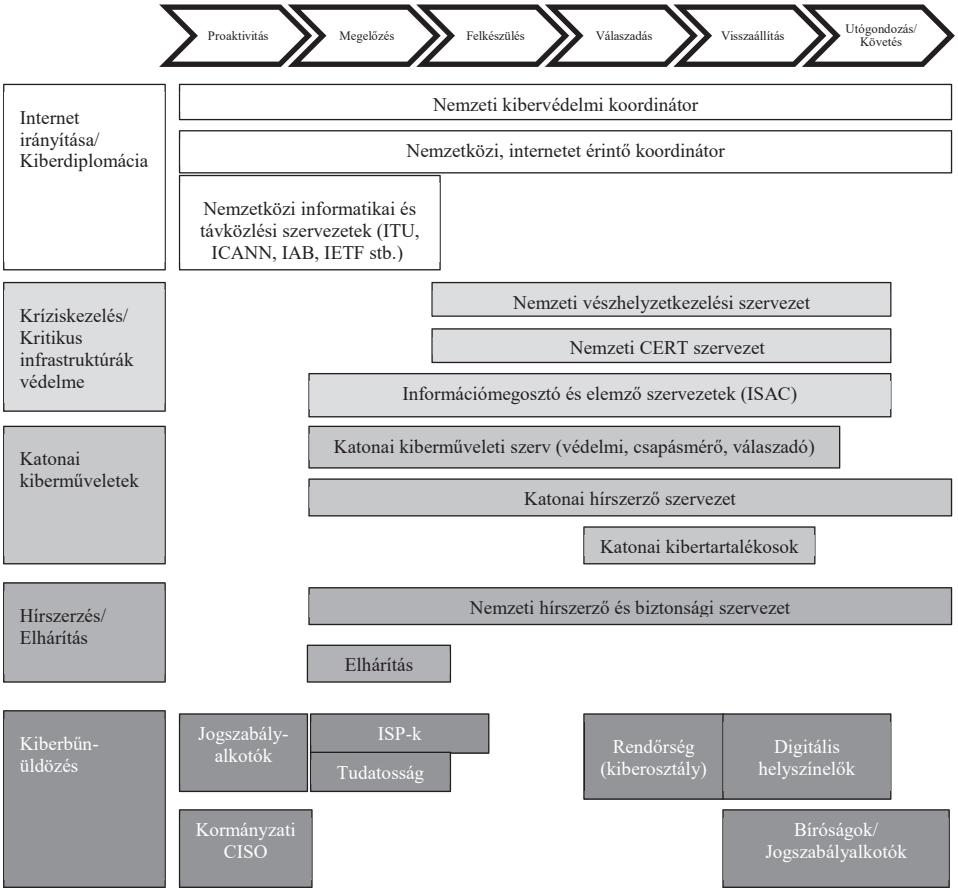
6 Petró Csilla – Stréhli-Klotz Georgina: Formálódó új közszolgálati életpálya, különös tekintettel a munkaköralapú rendszer bevezetése irányába tett hazai kísérletekre, *Polgári Szemle: Gazdasági és Társadalmi Folyóirat,* 10. évf., 2014/3–6, 369. o.

7 Steve Morgan (ed.): *Hackerpocalypse: A Cybercrime Revelation,* Cybersecurity Ventures, 2016.

8 Elhangzott: Kiberkarrierek az állami szférában rendezvény, Nemzeti Közszolgálati Egyetem, 2017. október 24.

pedig a Honvédelmi Minisztérium, a Külgazdasági és Külügyminisztérium, valamint a Miniszterelnökség rendelkezik kisebb-nagyobb feladatrendszerrel, másrészt viszont meglehetősen fragmentált, hiszen az egyes minisztériumokon belül, illetve alárendeltségükben számos szervezet munkáját kell összehangolni. Az 1. ábra a NATO Kiberbiztonsági Kiválósági Központjának Nemzeti Kiberbiztonsági Keretrendszerét mutatja be, amely felsorolja, hogy milyen feladatok adódhatnak állami részről.[9]

1. ábra: A kibervédelem életciklusmodellje



Forrás: NATO CCDCOE National Cyber Security Framework Manual

Magyarországon jelenleg a következő szervezetek töltenek be kulcsfontosságú szerepet a fenti keretrendszerben:

– *Nemzeti kibervédelmi koordinátor:* a 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiber-

[9] Eric Luiijf – Jason Healey: Organisational Structures & Considerations. In: Alexander Klimburg (ed.): *National Cyber Security Framework Manual,* NATO CCD COE Publications, Tallinn, 2012, 108–145. o., 129. o.

biztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről hozta létre ezt a pozíciót kiberkoordinátor néven. Bár hivatalosan a Miniszterelnökség delegáltja, a gyakorlatban a Belügyminisztérium alá tartozó Nemzeti Kibervédelmi Intézet támogatja.

– *Nemzetközi, internetet érintő koordinátor:* a 19/2016. (VIII. 31.) KKM-utasítás a Külgazdasági és Külügyminisztérium Szervezeti és Működési Szabályzatáról szerint a minisztérium Erőforrás-diplomácia és Új Típusú Biztonsági Kihívások Főosztályon működő kibertér koordinátor feladata ennek a szerepkörnek a betöltése.
– *Nemzetközi, informatikai és távközlési szervezetek:* a fontosabb nemzetközi szervezetek kiberbiztonságért felelős vezető pozícióit több esetben is Magyarország delegáltjai töltik be. 2017 novemberétől például Vass Sándor dandártábornok a csoportfőnöke a NATO Szövetséges Fegyveres Erők Európai Főparancsnokság (SHAPE) újonnan felállított híradó, informatikai és kibervédelmi csoportfőnökségének.
– *Nemzeti vészhelyzetkezelési szervezet:* alapvetően a 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről alapján a létfontosságú rendszerek kibervédelméért a Belügyminisztériumon belül működő Országos Katasztrófavédelmi Főigazgatóság tartozik felelősséggel. Ezt pontosítja a 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról, amely létrehozta a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központját.
– *Nemzeti CERT-szervezet:* a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról hozta létre a kormányzati eseménykezelő központot, amely funkciót jelenleg a Belügyminisztérium alá tartozó Nemzetbiztonsági Szakszolgálaton belül a Nemzeti Kibervédelmi Intézet látja el, ezen belül is a Kormányzati Eseménykezelő Központ, azaz a CERT-Hungary.
– *Információmegosztó és -elemző szervezetek (ISAC):* kimondottan ilyen szervezet a tanulmány írásának idején nem működik Magyarországon (bár kezdeményezések vannak rá), az információ megosztása jellemzően informális keretek között történik. Az elvárt működéshez a Nemzeti Kibervédelmi Intézeten belül működő Nemzeti Elektronikus Információbiztonság Hatóság áll a legközelebb.
– *Katonai kiberműveleti szerv (védelmi, csapásmérő, válaszadó):* a Honvédelmi Minisztérium, a Magyar Honvédség és a Katonai Nemzetbiztonsági Szolgálat lát el részfeladatokat ezen a területen, de a katonai kiberműveletek fő letéteményese ez utóbbi szervezet a 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról alapján. Hangsúlyozni kell azonban, hogy jelenleg sem a csapásmérés, sem a válaszadás módja nem jelenik meg a magyar jogrendben és gyakorlatban.

- *Katonai hírszerző szervezet:* a kibertérben történő katonai hírszerzés a Katonai Nemzetbiztonsági Szolgálat feladata, amelyet az 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról egyértelműen megfogalmaz.
- *Katonai kibertartalékosok:* a tartalékosok bevonása a katonai célú kibervédelembe jelenleg nincs megoldva, bár az Önkéntes Kibervédelmi Összefogás (KIBEV) 2011-es létrehozása egy civil kezdeményezés volt ebbe az irányba.[10] Amennyiben a magyar katonai gondolkodásban megjelenik a csapásmérésre és a válaszadásra való igény, újra előkerülhet a kibertartalékosok kérdése.
- *Nemzeti hírszerző és biztonsági szervezet:* bár a magyar jogrend egyetlen polgári nemzetbiztonsági szervezetnél sem nevesíti a kibertér védelmét, a már említett 1995. évi CXXV. törvény egyértelművé teszi, hogy valamennyi magyar titkosszolgálatnak közvetve van feladata, bár a nemzetközi gyakorlat alapján ez elsősorban belbiztonsági feladatkört takar, amely a belügyminiszterhez tartozó titkosszolgálatok érintettségét jelenti.
- *Elhárítás:* megerősítve az előző pontot, kimondottan a kibertérből érkező fenyegetések titkosszolgálati elhárítása sincs nevesítve. A 282/2016. (IX. 21.) Korm. rendelet az államtudományi képzési terület alap- és mesterképzési szakjainak meghatározásáról és azok képzési és kimeneti követelményeiről, valamint az azzal összefüggő kormányrendeletek módosításáról azonban a polgári nemzetbiztonsági mesterképzési szak követelményeinél mind a technikai felderítő, mind a terrorelhárítási specializációnál megemlíti a kibertámadások elhárításának fontosságát, így közvetve arra a következtetésre lehet jutni, hogy az érintett titkosszolgálatok, illetve a Terrorelhárítási Központ épít ilyen képességeket.
- *Jogszabályalkotók:* a kiberbiztonsággal kapcsolatos jogszabályalkotást bármelyik érintett minisztérium, de jellemzően a Belügyminisztérium kezdeményezi a szakterület jogszabályalkotását.
- *ISP-k:* az internetszolgáltatók a HUN-Cert-en keresztül vesznek részt a magyar kibervédelemben. Emellett több szolgáltató is megállapodást kötött a Nemzeti Kibervédelmi Intézettel a hazai kibertér védelme érdekében.
- *Tudatosság:* annak ellenére, hogy a Nemzeti Kiberbiztonsági Stratégia egyértelműen kiemeli a tudatosságépítés fontosságát, nincsen egyértelmű felelőse a kérdésnek. A Nemzetközi Kiberbiztonsági Hónap szervezését a Nemzeti Kibervédelmi Intézet látta el, az online gyermekvédelemben a Nemzeti Infokommunikációs Zrt. jelenik meg, így a társadalmi tudatosságépítés szintén belügyi feladatnak tűnik.
- *Kormányzati CISO:* a 2013. évi L. törvény rendelkezései alapján nem egy kiemelt kormányzati információbiztonsági vezető van, hanem minden, a törvény hatálya alá tartozó szervezetnél van egy dedikált felelős. A kormányzati Chief Information Security Officer pozíciót tehát körülbelül 5000 fő kell hogy betöltse. A közöttük való koordinációban kiemelt szerepe lenne a korábban említett ISAC-nek.

[10] Muha Lajos – Zala Mihály – Frész Ferenc – Mádi-Nádor Anett – Birkás Bence: Átfogó megközelítés a kibervédelemben. In: Keszely László (szerk.): *Az átfogó megközelítés és a védelmi igazgatás,* Zrínyi Kiadó, Budapest, 2013, 163–196. o.

– *Rendőrség:* a Nemzeti Nyomozó Irodán belül működő Kiberbűnözés Elleni Főosztály az utóbbi években kiemelt csúcsszervként foglalkozik az informatikai bűncselekményekkel, de mivel egyre több bűncselekménytípus során használnak fel infokommunikációs eszközöket, szinte valamennyi rendőri szervezet találkozik a jelenséggel.
– *Digitális helyszínelők:* bár statútuma szerint a Nemzetbiztonsági Szakszolgálat is rendelkezik ilyen képességekkel, a kiberbűnözés esetében elsődlegesen a Kiberbűnözés Elleni Főosztály Forenzikus Osztálya hajtja végre a digitális nyomrögzítéssel kapcsolatos feladatokat.
– *Bíróságok:* a magyar gyakorlatban a kiberbűnözéshez kapcsolódóan elsősorban az ügyészségi szervezetek részéről érezhető aktivitás, a bíróságok elsősorban igazságügyi szakértők bevonására építenek, ahogy ez Som Zoltán és Papp Gergely Zoltán cikkéből kiderül.[11]

Kihívások a kiberbiztonság oktatásában

A magyar kibervédelem rendszere tehát meglehetősen szerteágazó, számos szakterületi specializáció tűnik szükségesnek, de valószínűsíthetően meg kell teremteni egy olyan közös tudásbázist is, amelyet minden hivatásrendben dolgozó munkatársnak ismernie kell. Ez a tudásmag kell hogy tartalmazzon stratégiai, jogi, szervezeti és műszaki ismereteket is. Illéssy Miklós és szerzőtársai 2014-es kutatásukban arra az eredményre jutottak, hogy „egybehangzó szakértői vélemények alapján ugyanakkor egyrészt közigazgatási rendszereink heterogenitása és decentralizáltsága, valamint a nehezen belátható költséghatékonyság-javulás miatt továbbra is lemaradásban leszünk, amennyiben ezeken a területeken nem történik szisztematikus építkezés. Interjúink megerősítik, hogy ezen nagymértékben segíthet az információbiztonsággal kapcsolatos humánerőforrás-fejlesztés vezetői és alkalmazotti szinteken is. Az információbiztonság vonatkozásában egyértelmű az egyetértés az egymás közötti kommunikáció hangsúlyozásában, a pontos egyéni és szervezetek közötti felelősség meghatározásában, a viselkedés és a kultúra meghonosításában; azaz nem elsősorban a technikai, hanem a humán területek húzó hatásának kihasználásában."[12]

A megfelelő egyensúly megtalálása azonban nem könnyű. A nemzetközi oktatási paletta mintavételszerű áttekintése azt a benyomást kelti, hogy mind a graduális, mind a posztgraduális képzések elsősorban a szűkebb, műszakibb megközelítés, azaz az információbiztonság irányába mutatnak, komplex kiberbiztonsági tanfolyamok kevésbé érhetők el.

A világ egyik legfejlettebb kibervédelmi oktatási rendszerével az Egyesült Királyság rendelkezik. Az *ITU Global Cybersecurity Index* (GCI) 2017-es felmérése alapján a kiberképességek fejlesztésében az európai éllovas, már az elemi oktatási szinttől foglalkozik az utánpótlásképzéssel.[13] Ahogy Molnár Dóra fogalmaz cikkében: „A kiberismeretek oktatását már az alsófokú oktatásban megkezdték: 800 általános iskola bevonásával mintegy 23 000 diák

[11] Som Zoltán – Papp Gergely Zoltán: Tudásfejlesztés a kiberbűnüldözésben – Lehetőségek és kihívások, *Hadmérnök,* 11. évf., 2016/2, 170–182. o.

[12] Illéssy Miklós – Nemeslaki András – Som Zoltán: Elektronikus információbiztonság – tudatosság a magyar közigazgatásban, *Információs Társadalom – Társadalomtudományi Folyóirat,* 2014/1, 52–73. o., 72. o.

[13] International Telecommunication Union: Global Cybersecurity Index, [online]. Forrás: Itu.int [2017. 07. 05].

szerzett alapvető ismereteket 2012 óta. A felsőoktatásban valamennyi alapképzés esetében bevezettek egy kiberbiztonsági közös modul tárgyat, a mesterképzésen pedig a GCHQ által kiadott standardnak megfelelően már 12 akkreditált kibermesterképzés létezik. Jelenleg három kutatóintézet rendelkezik kiberbiztonsági profillal, 13 kiválósági központot hoztak létre, és cél, hogy 2019-re 100 doktoranduszt tudjon magáénak a már működő két kiberbiztonsági doktori iskola."[14]

Urbanovics Anna részletes elemzést végzett dolgozatában azzal kapcsolatban, hogy pontosan milyen jellegű tárgyak tartoznak a kiberbiztonsági képzés alá. A szerző hét tantárgycsoportot azonosított, amelyek a következők:

1. kriptográfia és adatelemzés;
2. bűnügyi informatika;
3. hálózatbiztonság;
4. szoftverbiztonság;
5. hardverbiztonság;
6. informatika más aspektusból (jog, menedzsment és pszichológia);
7. kutatás és elméleti ismeretek.

Ezek közül egyedül a 6. terület, az informatika „más" aspektusból való vizsgálata az, amely kimutat a műszaki megközelítésből. A szerző szavaival: „A következő tárgykör talán a legsokrétűbb, mert ez az informatika egyéb aspektusait vizsgálja. Minden olyan ismeretet kínál, amely az üzleti életben való helytálláshoz elengedhetetlen. Ilyenek például a jogi háttér ismerete, a projektmenedzsment, a biztonság- és védelem irányítása, a kockázatelemzés és a pszichológiai vonatkozások." A képzési programoknak azonban ezek a „soft" tantárgyak jellemzően a kisebbik részét fedik csak le. A 2. ábra Urbanovics Anna szerkesztésében mutatja meg az arányokat, egyben a kiberbiztonsággal foglalkozó brit felsőoktatási intézményeket.[15]

[14] Molnár Dóra: Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia, *Hadmérnök*, 12. évf., „KÖFOP" szám, 2017. 10., 141. o.

[15] Urbanovics Anna: *Az Egyesült Királyságban működő kiberbiztonsági képzések elemzése,* TDK-dolgozat, Nemzeti Közszolgálati Egyetem, Nemzetközi és Európai Tanulmányok Kar, 2017.

2. ábra: Témakörönként, felsőfokú intézményenként meghirdetett kurzusok száma

Felsőfokú intézmény/ Témakör/Kurzusok száma (db)	Kriptográfia és adatelemzés	Bűnügyi informatika	Network-biztonság	Szoftver-biztonság	Hardver-biztonság	Informatika más aspektusból	Kutatás és elmélet
Cranfield University		3	2	4		3	2
Lancaster University		2	1	1		3	2
Edinburgh Napier University		1	2	2		1	1
Queen's University Belfast	1	2	1	1		1	
Royal Holloway University of London	3	2	1	3	2	3	2
UCL	3	2		2	1	3	3
University of Birmingham	3	1	3	6	1	1	3
University of Oxford	1	2	4	2		5	1
University of South Wales		3	1			2	1
University of Southampton	4	2		2	1	4	5
University of Surrey	3		2	2		3	
University of York	1	2	1			2	2

Forrás: Urbanovics Anna: *Az Egyesült Királyságban működő kiberbiztonsági képzések elemzése: i. m.*

Tovább nehezíti az egységes megközelítés kialakítását az, hogy a hivatásrendek képzése jellemzően különböző intézményekben történik, így egy komplex kiberfizikai katasztrófaesemény során hiába kellene együttműködnie rendészeti, katasztrófavédelmi, titkosszolgálati, katonai és közszolgálati szakembereknek, hiányzik az a közös nyelv, amire az összehangolt védelmet építeni lehetne.

A szerző 2017 folyamán több mélyinterjút folytatott az előző fejezetben felsorolt szervezetek illetékes vezetőivel annak érdekében, hogy megismerje az egyes intézmények kiberbiztonsági szakemberekkel szembeni elvárásait, ezek alapján ki tudjon alakítani bizonyos profilokat, majd meg tudja állapítani, mi az a közös tudásmag, amely a közszolgálati kibervédelemben feltétlenül szükséges. Emellett fontos szempontként szerepelt az is, hogy kiderüljön, hol lehet kapcsolat az egyes hivatásrendek között, hiszen a közszolgálati életpályamodell egyik elengedhetetlen eleme az átjárhatóság. Az interjúk alapján az alábbi kiberképességekre van szükség a közszolgálatban:

– *A kiberbiztonság általános megértésének képessége:* tekintettel arra, hogy mindegyik hivatásrend munkatársai intenzíven használják az információs rendszereket, alapvető elvárásként jelentkezett a biztonságtudatosság növelésének igénye. Ez nemcsak szervezeti igény, de a 2013. évi L. törvény alapján jogszabályi kötelezettség is. Nem elégséges azonban kizárólag arra koncentrálni, hogy a munkatársak csak a biztonságos eszközhasználatot (Hogyan?) sajátítsák el, segíteni kell őket kibertér kihívásainak megismertetésével is, a stratégiai összefüggések és a nem megfelelő eszközhasználat következményeinek elmagyarázásával (Miért?). Bár nagy számban kell műszaki ismeretekkel nem rendelkező embereket oktatni, mégis szükséges életszerűen bemutatni a veszélyeket, akár laborgyakorlatok, szimulációk segítségével. Ez a megközelítés egyben segítséget nyújt abban is, hogy a több százezer közszolgálati dolgozó közül később kikerüljön az a néhány ezer, akik kibervédelemre specializálódnak, hiszen az általános megértésen keresztül egyrészt felkelthető az érdeklődés, másrészt megteremtődik az az alap, amit a későbbiekben tovább lehet építeni.
– *Incidensmenedzselési képesség:* „Mindazonáltal egy szervezet működtetheti a legfejlettebb információvédelmi rendszert, ha a szervezet dolgozói nem rendelkeznek megfelelő ismeretekkel, biztonságtudattal, a bevezetett védelmi megoldásokat nem tudják hatékonyan használni, akkor az információvédelem nem tud, nem képes hatékonyan működni" – írja Sági Gábor.[16] Ezt erősítették meg a vezetői interjúk is. A biztonságtudatos működés mellett szükség van olyan szakemberekre, akik a műszaki eszközöket üzemeltetni tudják. Ez egyrészt mérnöki tudással rendelkező munkatársakat igényel, de a szervezeti visszajelzések alapján nagy számban van szükség olyan kollégákra is, akik az úgynevezett biztonsági műveleti központokban *(Security Operation Center – SOC)* látnak el biztonsági elemző feladatot. Ez a gyakorlatban nem igényel mély informatikai ismereteket, igényli viszont az egyes biztonsági események megértését, a közöttük levő összefüggések feltárását, egyben az információkat kezelő rendszerek használatának elsajátítását. Az incidensmenedzselés egyben kiváló tanulóterep azoknak, akik később specialistákká válnak, hiszen mély ismereteket szerezhetnek a kibertámadások valódi természetéről.
– *Stratégiai, vezetői képességek:* minden hivatásrend elvárja, hogy legyenek saját specialistái. Alaposabban megvizsgálva az ideális jelölteket, közös igény mutatkozik olyan szakértőkre, akik jártasak a jog és a biztonságpolitika kérdéseiben, képesek állami delegáltként vagy valamilyen alakulat parancsnokaként Magyarország és szövetségeseinek stratégiai érdekeit képviselni akár polgári, akár katonai területen, illetve képesek más entitásokkal a szükséges és elégséges információ megosztására. Hasonló képességekre van szükség hazai viszonylatban is, hiszen nagy szükség van olyan szervezeti információbiztonsági felelősökre, jogszabályalkotókra, közigazgatási tervezőkre, hatósági munkatársakra, ügyészekre, bírókra, akik összefüggéseiben tudják vizsgálni saját szakterületükön a kibertér kihívásait. Műszaki ismereteik nem feltétlenül kell, hogy meghaladják az előző két képességben foglaltakat. Fontos, hogy valamilyen

[16] Sági Gábor: Megvédhetőek-e a kritikus információs infrastruktúrák?, *Hadmérnök,* 11. évf., 2016/2, 154–169. o. 163. o.

szinten a specialisták ismerjék más specialisták szakterületeit, hiszen folyamatosan rá lesznek kényszerülve a szoros együttműködésre.

Képességfejlesztés az egyes felsőoktatási szinteken

Magyarországon a közszolgálati oktatások erősen centralizáltak, a legtöbb feladatot a Nemzeti Közszolgálati Egyetem látja el, amely „oktató- és kutatótevékenysége az államra, annak alapvető jelenségeire, szolgáltatásaira, funkcióira irányul, képzései ezek megértésére, gyakorlására, biztosítására készítik fel a hallgatókat. Az intézmény elsődleges célja a közigazgatás, a rendvédelem, a honvédelem és a nemzetbiztonsági szolgálatok leendő és jelenlegi személyi állományának magas színvonalú képzése, alap-, mester- és doktori szinten" – ahogy az Patyi András rektornak az egyetemet bemutató szavaiból kiderül. Az egyetem intézményfejlesztési tervében és küldetésében a közszolgálati utánpótlásképzés biztosítása mellett kiemelt hangsúlyt kap a közszolgálati életpályamodellt támogató továbbképzési rendszer működtetése. A kiberbiztonsági képességfejlesztésnek tehát az egyetem kiváló helyszíne lehet. A kibervédelmi szervezetek vezetőivel készült interjúk alapján az előző fejezetben leírt képességek a felsőoktatási keretrendszerben az alábbiak szerint fejleszthetők.

– *A kiberbiztonság általános megértésének képessége*

  Alapszinten: Elengedhetetlenül fontos minden alapképzési szakon, lehetőleg az első év folyamán a kiberbiztonság kérdésével foglalkozni, már csak azért is, mert az infokommunikációs eszközök használata minden hivatásrend esetében végig fogja kísérni a végzettek pályafutását. Ehhez szükség van egyrészt egy olyan gyakorlati foglalkozásra, ahol a hallgatók számítógép mellett, élményszerűen élhetik át az olyan gyakori informatikai támadásokat, mint például az adathalászat, a gyenge jelszóhasználatból eredő visszaélések vagy a kártékonykód-fertőzés. Másrészt egy elméleti előadás során az átélt támadásokat rendszerbe kell helyezni, elmagyarázva, hogy egy felhasználó hibája a legrosszabb esetben az egész ország biztonságát fenyegetheti. A Nemzeti Közszolgálati Egyetem képzési rendjében egyrészt az Egyetemi Közös Modul keretein belül van lehetőség ezt a struktúrát kialakítani, másrészt az informatikához kapcsolódó kari képzések adhatnak teret ezeknek, egységes egyetemi tematikával.

  Alap- és mesterszinten: Tekintettel arra, hogy a hallgatók a saját digitális létük védelmében is érdekeltek, érdemes olyan választható tárgyakat indítani, amelyek egy félév során, gyakorlati óra keretében, részletesen is be tudják mutatni, milyen kihívásokkal találkozhatnak a számítógépek és mobileszközök használata során. Az egyetem Államtudományi és Közigazgatási Karán jelenleg is elérhető egy információbiztonsági tudatosság nevű tárgy, amelynek hallgatói az éves visszajelzések alapján igénylik az egyes támadások kivédéséhez szükséges alapvető műszaki ismereteket is, így a tárgyat érdemes számítógépes támogatással tanítani. Ez nem kell, hogy mélyebbre menjen az eszközök, okostelefonok biztonságos beállításánál, az otthoni hálózati eszközök konfigurálásánál vagy a közösségi hálózatok adatvé-

delmi és biztonsági beállításainak megértésénél. Ezek az ismeretek azonban szükségesek (de még nem elégségesek) a kiberbiztonság mélyebb elsajátításához.
Továbbképzési szinten: Az egyetem Vezető- és Továbbképzési Központja évente több mint 70 000 közszolgálati tisztviselő továbbképzéséről gondoskodik, sok esetben e-learning formában. Ezen e-learning-tananyagok közül egyre több foglalkozik a kiberbiztonsággal és speciálisan a biztonságtudatosság növelésével. Mivel a tisztviselőknek kötelező a továbbképzéseken részt venni, a kiberbiztonsági képzési kínálat bővülésével esély mutatkozik arra, hogy egyre többen fogják ezeket a tematikus tanfolyamokat választani, ezzel pedig betekintést kaphatnak a területre.

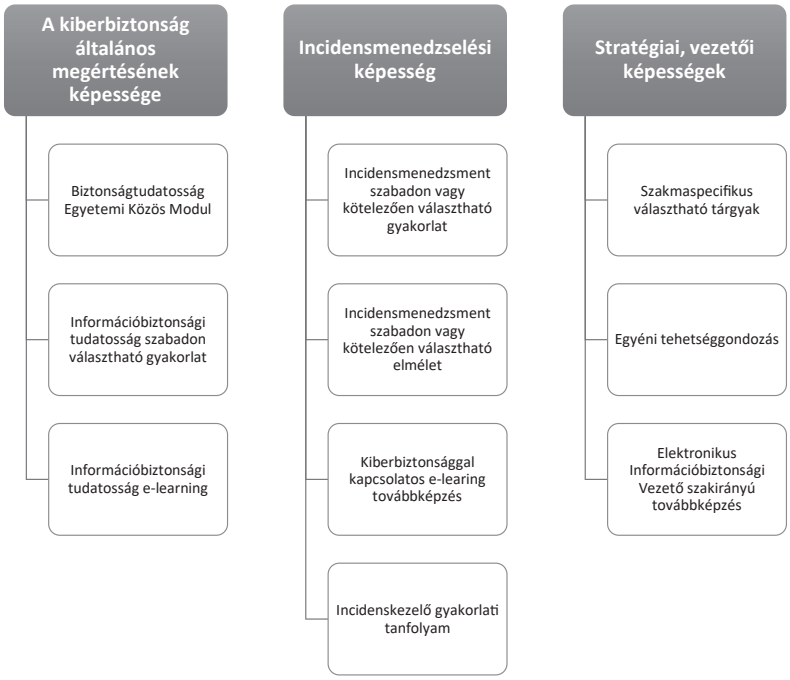
– *Incidensmenedzselési képesség*
Alapszinten: a gyakorlati megközelítésű, biztonságtudatossággal foglalkozó gyakorlati tárgyra építve lehetőség nyílik arra, hogy a kiberbiztonsági incidensek hátterét és összefüggéseit mélyebben is megismerjék a hallgatók, választható vagy műszaki területhez közelebb álló specializációk esetén (egyes katonai és rendészettudományi képzések esetében) kötelezően választható tárgy keretében. Ez a tantárgy már igényel bizonyos fokú hálózati és informatikai ismereteket, így érdemes az elméleti és gyakorlati ismereteket is vegyíteni. A cél az, hogy a hallgatók alapszinten megértsék a modern kibervédelmi rendszerek működését, a támadások műszaki alapjait és a biztonsági műveleti központok jellegzetességeit. A tárgyat abszolváló hallgatók megfelelő utánpótlást jelenthetnek akár a belügyi, akár a honvédelmi eseménykezelő központok számára, ami egyrészt rövid távon csökkentheti az ott jelentkező munkaerőhiányt, másrészt máshonnan nem megszerezhető gyakorlati hátteret ad a frissdiplomások számára.
Továbbképzési szinten: A 26/2013. (X. 21.) KIM-rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról előírja az egyetem számára azt, hogy minden évben új e-learning-képzéseket készítsen a rendeletben megfogalmazott három célcsoport (elektronikus információs rendszer biztonságáért felelős személy, elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy, elektronikus információs rendszerek védelméért felelős vezető) részére. Ezek az oktatások a teljes közszolgálat számára hozzáférhetők, és megfelelő alapot nyújtanak azoknak, akik már aktív tisztviselőként szeretnének kiberbiztonságra specializálódni. Az incidenskezelési képesség kiépítéséhez azonban laboratóriumi gyakorlatra is szükség van. Mindazok számára, akik sikerrel elvégzik a vonatkozó e-learning-képzéseket, tehát az elméleti ismereteket, lehetőséget lehet teremteni arra, hogy egy ötnapos (30 órás) kurzussal megszerezzék ugyanazt a gyakorlati alapot, amelyet az alapképzésben tanulók is megkaphatnak.

– *Stratégiai, vezetői képességek*
Alap-, mester- és doktori szinten: A vezetői információk alapján a magyar közszolgálat évente 30-50 nem műszaki orientációjú specialistát, szakértőt, vezetőt tud felszívni és beépíteni a kiberbiztonsággal foglalkozó szakterületekre. Semmiképpen sem tömegképzésről beszélünk tehát, sokkal inkább egyéni tehetséggondozásról,

amelyben ugyanannyira fontos a saját specializáció mély megismerése, mint a társterületekkel való együttműködésre való képesség. Az egyetem képzési struktúrájának egyik előnye, hogy bizonyos feltételek mellett a választható tantárgyak minden hivatásrend számára elérhetők, ezért érdemes olyan tárgyakat indítani az egyes karokon, amelyek a hivatásrendi specializációkat más karokon tanuló hallgatókkal is megismertetik. Ez egyben segíti azt is, hogy a jövőbeli felelősök, vezetők között jó személyes kapcsolat alakuljon ki. A választható tárgyak mellett azonban a szakkollégiumoknak, a TDK-köröknek és a témavezetőknek is fontos felelősségük van abban, hogy az egyéni képességek az éppen hiányzó niche területek irányába fejlődjenek, ezek alapján pedig a hallgató a megfelelő életpályára kerüljön.

Továbbképzési szinten: A már gyakorló közszolgálati szakemberek közül is egyre többen szeretnének a hivatásrenden belül új specializációt választani és a kiberbiztonságra váltani. Számukra a hivatásrend ismert, így a kibertér specialitásait kell velük megismertetni. Erre ad lehetőséget az egyetemen a 2013. évi L. törvény alapján elindított elektronikus információbiztonsági vezető szakirányú továbbképzés, amely két félévből áll, és mind elméleti, mind gyakorlati tantárgyakat tartalmaz. A képzés nemcsak a törvény hatálya alá tartozó szervezetek információbiztonsági felelősei számára nyitott, népszerűségét mutatja, hogy a 2017/18-as tanévre 66 fő jelentkezett, többségük nem a törvényi kötelezettségei miatt. A javasolt képzési struktúrát a 3. ábra mutatja be.

3. ábra: Javasolt kiberbiztonsági képzési struktúra



Forrás: saját szerkesztés

A Kiberbiztonsági Akadémia koncepciója

A Nemzeti Közszolgálati Egyetem oktatási és kutatási tevékenysége öt karon (Államtudományi és Közigazgatási Kar, Hadtudományi és Honvédtisztképző Kar, Nemzetközi és Európai Tanulmányok Kar, Rendészettudományi Kar, Víztudományi Kar) és három önálló intézetben (Államkutatási és Fejlesztési Intézet, Katasztrófavédelmi Intézet, Nemzetbiztonsági Intézet) folyik. Ezek mindegyike valamilyen módon foglalkozik a kiberbiztonság egyes részkérdéseivel, a szervezeti önállóság miatt azonban az oktatás-kutatás területén egyetemi szintű koordinációra volt szükség. A karok többségénél egy-két oktató foglalkozott a kiberbiztonsággal, jellemzően választható tárgyak keretében, így nem volt sem órarendi lehetőségük, sem pedig széles körű szakismeretük arra, hogy a szükséges alapismereteket átadják az érdeklődő hallgatóknak. A karok eltérő órarendje és az egyes campusok távolsága miatt a meglevő szinergiák kihasználására sem nyílt lehetőség.

Az egyetem vezetése időben észlelte ezt a kihívást, és megállapította, hogy a kiberbiztonság olyan horizontális szakterület, amely megköveteli a szakmai koordinációt az oktatással és a kutatással foglalkozó szereplők között. Ezen koordináló tevékenység megvalósítása érdekében jött létre 2017. március 1-jén a Kiberbiztonsági Akadémia, amely az NKE rektora által alapított egyetemi központi programkeret. Az akadémia a programigazgató vezetésével és egy szakmai irányító testület (SZIT) támogatásával integrálja és szervezi az NKE képzési egységei (karok, intézetek), a kutatóműhelyek kiberbiztonsági munkáinak szinergiáit, képzési és kutatási programok szervezésével növeli azok eredményességét és hatékonyságát.

A Szakmai Irányító Testület (SZIT) irányításával és a programigazgató vezetésével a Kiberbiztonsági Akadémia elsődleges feladata olyan nemzetközi és hazai célcsoportokra irányuló képzési programok, szakmai rendezvények és publikációk szervezése, amelyek

- az NKE-n folyó képzési és kutatási erőforrások szinergiáira épülnek;
- rugalmasan és gyorsan reagálnak a kormányzati fejlesztési igényekre;
- az NKE IT erőforrásait hatékonyan integrálják egy közös cél érdekében;
- az eltérő hivatásrendeket is „átfogó szemléletet" érvényesítenek;
- a legkorszerűbb IT-technológiával összhangban készülő fejlesztéseket generálnak.

Az NKE részéről a SZIT tagja az öt kar és az érintett karközi intézetek kiberbiztonsági kérdésekkel megbízott vezető oktatói, valamint azok a külső szervezetek, amelyek meghatározó szerepet játszanak a magyar kibervédelem rendszerében. A SZIT tagjai a következő szervezetek:

- Nemzeti Adatvédelmi és Információszabadság Hatóság, amelynek elnöke egyben a SZIT elnöke is;
- Belügyminisztérium;
- BM Országos Katasztrófavédelmi Főigazgatóság;
- Alkotmányvédelmi Hivatal;
- Nemzetbiztonsági Szakszolgálat;
- Katonai Nemzetbiztonsági Szolgálat;
- Igazságügyi Minisztérium;

- Honvédelmi Minisztérium;
- Országos Rendőrfőkapitányság, Nemzeti Nyomozó Iroda, Kiberbűnözés Elleni Főosztály;
- Magyarország kiberkoordinátora;
- Külgazdasági és Külügyminisztérium;
- Miniszterelnökség.

A kiberbiztonsággal kapcsolatos kutatási hátteret a Ludovika Kiemelt Kutatóműhely KÖFOP-pályázat keretében benyújtott Kiberbiztonsági Kiemelt Kutatóműhely nyújtja, aminek jelentősége az, hogy hozzájárul a magyar állam, a közszolgálat és a közigazgatás információbiztonságának növeléséhez. A kutatások időtartama alatt célja olyan kutatói kapacitás integrációjának létrehozása az NKE-n, amely tudományos kutatásokkal megalapozza a közszolgálat számára szükséges információbiztonsági képzések (alap-, mester- és doktori képzések, valamint kiemelten a továbbképzések) elméleti, valamint gyakorlati kérdéseit.

A kutatóműhely szervezetfejlesztési célja ezek alapján, hogy az itt folyó kutatásokkal és azok kutatási eredményeivel az egyetem karain és intézeteiben meglévő széttagoltságot megszüntesse, ezek hatékonyságát koordinációs segítséggel, szoros belső együttműködéssel és a pályázati indikátorok szisztematikus érvényesítésével javítsa. A hazai és nemzetközi partnerekkel végzett kutatás-fejlesztési munkával katalizálni kívánja az egyetem (kiberterületen) meglévő kutatói potenciáljának kihasználását, illetve azok extenzív és intenzív fejlesztését. A műhely programja két fő részre osztható:

- kiberbiztonsági kutatások (nemzetközi és hazai K+F);
- a kutatások eredményeire építő nemzetközi/hazai kiberbiztonsági képzési program(ok) tartalmi kidolgozása (képzésfejlesztés).

A kutatóműhelyben hat kutatási fejezetben folyik a munka 2017. február és 2018. december között:

- a kibertér szereplőinek biztonságtudatossági vizsgálatai;
- a korszerű technológia hatása az urbanizált terek társadalmi folyamataira;
- közösségi média lehetőségei és biztonsági kockázatai;
- a kibertér szervezeti és vezetési kihívásai;
- kiberstratégiai kutatások;
- kiberbűnözés/IT Forensics.

Összefoglalás

A virtuális térből érkező fenyegetések kezelése tehát nem kizárólag műszaki probléma többé. A kihívások nagy része pedig közvetve vagy közvetlenül fenyegeti az ország biztonságát, illetve kezd kialakulni egy olyan negatív társadalmi biztonságpercepció, amelyre az államnak reagálnia kell. Felkészült közszolgálati szakembergárda nélkül mindez nem lehetséges. Magyarországon a Nemzeti Közszolgálati Egyetem feladata és felelőssége a közszolgálati hivatásrendek oktatása, így ebben az intézményben is gondoskodni kell a megfelelő kiberbiztonsági oktatási-kutatási háttér megteremtéséről.

A nemzetközi példák jó kiindulási alapot adnak az oktatás irányainak meghatározására, de nincsen olyan univerzális recept, amelyet egy az egyben adaptálni lehetne. Egyrészt azért, mert világszerte még mindig az információbiztonság, azaz a műszaki szemlélet oktatása a jellemző, másrészt azért, mert kevés olyan felsőoktatási intézmény létezik, amely az NKE-hez hasonló módon a teljes közszolgálatot lefedi. Jelen tanulmány a nemzetközi példákra és az intézményrendszer felelős vezetőivel történt interjúkra alapozva bemutatta, milyen oktatási irányok szükségesek Magyarország kibervédelmének kiteljesítéséhez. A Kiberbiztonsági Akadémia és a Kiberbiztonsági Kiemelt Kutatóműhely olyan kezdeményezések, amelyek a cikkben felvázolt irányok megvalósítására alkalmasak. A kezdeményezések sikere már csak azért is létfontosságú, mert a már idézett ITU Global Cybersecurity Index 2017-es felmérésben Magyarország egyetlen területen, a kapacitásépítésben kapott elégtelen osztályzatot. Megfelelő képességek nélkül pedig elképzelhetetlen a biztonságos magyar kibertér.

FELHASZNÁLT IRODALOM

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében, *Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata,* 13. évf. 2016/1, 61–81. o.

Illéssy Miklós – Nemeslaki András – Som Zoltán: Elektronikus információbiztonság – tudatosság a magyar közigazgatásban, *Információs Társadalom – Társadalomtudományi Folyóirat,* 2014/1, 52–73. o.

International Telecommunication Union: Global Cybersecurity Index, [online]. Forrás: Itu.int [2017. 07. 05.]

International Telecommunication Union: ICT Facts and Figures 2017, [online]. Forrás: Itu.int [2017. 07. 31.]

Kiberkarrierek az állami szférában rendezvény, Nemzeti Közszolgálati Egyetem, 2017. 10. 24.

Luiijf, Eric – Healey, Jason: Organisational Structures & Considerations. In: Alexander Klimburg (ed.): *National Cyber Security Framework Manual,* NATO CCD COE Publications, Tallinn, 2012, 108–145. o.

Molnár Dóra: Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia, *Hadmérnök,* 12. évf., „KÖFOP" szám, 2017. 10. 136–148. o.

Morgan, Steve (ed.): *Hackerpocalypse: A Cybercrime Revelation,* Cybersecurity Ventures, 2016

Muha Lajos – Zala Mihály – Frész Ferenc – Mádi-Nádor Anett – Birkás Bence: Átfogó megközelítés a kibervédelemben. In: Keszely László (szerk.): *Az átfogó megközelítés és a védelmi igazgatás,* Zrínyi Kiadó, Budapest, 2013, 163–196. o.

Petró Csilla – Stréhli-Klotz Georgina: Formálódó új közszolgálati életpálya, különös tekintettel a munkaköralapú rendszer bevezetése irányába tett hazai kísérletekre, *Polgári Szemle: Gazdasági és Társadalmi Folyóirat,* 10. évf. 2014/3–6, 369–389. o.

Sági Gábor: Megvédhetőek-e a kritikus információs infrastruktúrák?, *Hadmérnök,* 11. évf. 2016/2, 154–169. o.

Som Zoltán – Papp Gergely Zoltán: Tudásfejlesztés a kiberbűnüldözésben – Lehetőségek és kihívások, *Hadmérnök,* 11. évf. 2016/2, 170–182. o.

Urbanovics Anna: *Az Egyesült Királyságban működő kiberbiztonsági képzések elemzése,* TDK-dolgozat, Nemzeti Közszolgálati Egyetem, Nemzetközi és Európai Tanulmányok Kar, 2017