HADMÉRNÖK

XII. Évfolyam 2. szám – 2017. június

A HAZAI CISCO HÁLÓZATI AKADÉMIAI KÉPZÉS – NETACAD PROGRAM KAPCSOLATA AZ IT SZAKTERÜLETEN FOLYÓ SZAKMAI KÉPZÉSEK RENDSZERÉVEL

CONNECTION BETWEEN THE LOCAL CISCO NETWORKING ACADEMY TRAINING – NETACAD PROGRAM AND THE EXISTING SYSTEM OF EXPERT IT PROGRAMS

JOBBÁGY Szabolcs

(ORCID: 0000-0002-2104-4665)

jobbagy.szabolcs@uni-nke.hu

Absztrakt

Jelen közleményben egy cikksorozat újabb elemeként bemutatásra kerül a hazai CISCO Hálózati Akadémiai Képzés – NetAcad Program kapcsolata az IT szakterületen folyó szakmai képzések rendszerével. Továbbá megvizsgálom a kihívásoknak, követelményeknek, szabályzói háttérnek való megfeleltethetőségét hazai és nemzetközi szinten.

Kulcsszavak: *OKJ, kibertér, varsói csúcs, kiberbiztonsági stratégia, lisszaboni csúcs, infokommunikációs stratégia*

Abstract

In this publication, as a further element of an article series, I would like to draw attention to the connection between the local CISCO Networking Academy Training – NetAcad Program and the existing system of expert IT programs. Furthermore, I would like to make a research regarding the challenges, requirements, regulation background on the local and international level.

Keywords: *OKJ, cyberspace, Warsaw summit, cybersecurity strategy, Lisbon summit, infocommunication strategy*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.22.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.05.05..

BEVEZETÉS

Jelen közleményben a „CISCO Hálózati Akadémiai Képzés – NetAcad[1] Program" cikksorozat egy újabb elemeként, a korábbi cikkek CISCO Hálózati Akadémia – NetAcad rendszerének, valamint a képzés, program keretében a különböző képzési szinteken elérhető képzések, kurzusok, vizsgák, minősítések és képesítések általános ismertetését követően, megvizsgálom és bemutatom, hogy ez a fajta „e – learning" képzés hogyan illeszkedik, hogyan helyezhető el a hazai IT szakterületen folyó szakmai képzések rendszerében, hogyan feleltethető meg az ott támasztott követelményeknek. Ezért alapul véve az Országos Képzési Jegyzék releváns részeit megpróbálok párhuzamot vonni, és beazonosítani azokat a képzési formákat, módokat és szinteket, ahol a CISCO Hálózati Akadémiai Képzés – NetAcad Program keretében elérhető képzések és kurzusok kiválthatják a hagyományos képzéseket, kurzusokat, a minősítő vizsgák pedig megfeleltethetőek az elvárt, támasztott követelményeknek.

Kutatásaim szempontjából kiemelt hangsúlyt szükséges helyeznem a képzés védelmi szféra számára történő hozzáférhetőségének, hatásának vizsgálatára is figyelembe véve az információs társadalom vívmányainak, a negyedik generációs hadviselés új típusú kihívásainak, a hazai és nemzetközi szabályozói háttérnek, valamint a különböző szövetségesi tagságunkból adódó elvárásoknak való megfelelés kritériumát is.[2] Ezen okból kifolyólag megvizsgáltam a téma szempontjából jelentőséggel bíró, érdekességre számot tartó néhány NATO csúcstalálkozót, az ott született releváns döntéseket, valamint a hazai és nemzetközi szabályozás néhány fontosabb momentumát, dokumentumát is.

A CISCO HÁLÓZAT AKADÉMIAI KÉPZÉS – NETACAD PROGRAM KAPCSOLATA AZ IT SZAKTERÜLETEN FOLYÓ SZAKMAI KÉPZÉSEK RENDSZERÉVEL

Publikációm első felében szeretném megvizsgálni és bemutatni, hogy a CISCO Hálózati Akadémiai Képzés - NetAcad Program, az elérhető e - learning oktatási anyagok hogyan is kapcsolódnak az IT szegmensben folyó, különböző szintű hazai képzések rendszerébe, hogyan is feleltethetőek meg az ottani elvárásoknak és követelményeknek, valamint milyen kapcsolatban állnak az Országos Képzési Jegyzékben (OKJ[3]) szereplő releváns szakmákkal.

Az OKJ törvényi hátterét és alapját a szakképzésről szóló 1993. évi LXXIV törvény teremtette meg, mely azóta természetesen számtalan esetben módosult. Ennek, valamint a folyamatosan kiadott új törvényeknek köszönhetően az OKJ is egy állandó átalakuláson, változáson ment keresztül, mígnem eljutott mai formájáig. A legutóbbi meghatározó jelentőségű változás 2012 - ben következett be, amikor is megtörtént annak kormányzati koncepciónak megfelelő átstrukturálása, összhangban a nemzeti köznevelésről szóló 2011. évi CXC törvénnyel, valamint a szakképzésről szóló ugyancsak 2011. évi CLXXXVII törvény megjelenésével. Az OKJ különböző bontásban és csoportosításban taglalja a Magyarországon elérhető, megszerezhető szakképesítéseket, szakmacsoportokat, melyeknek természetesen részét képezi az IT szegmens, a különböző informatikai szakmák tárháza is. [3] Ennek a módosított OKJ - nak megfelelően indult meg a képzés 2013 - ban a különböző szakképző intézményekben, amelynek inkább pozitívumai, mintsem negatívumai vannak a CISCO

[1] Networking Academy
[2] Fontos továbbá kiemelni, hogy mind a hadtudományi, mind a műszaki tudományok jelentős kutatási feladatai közözött szerepelnek ezen területek vizsgálata mind a civil, mind a védelmi szférában.[1]; [2]
[3] Országos Képzési Jegyzék

Hálózati Akadémiai Képzés - NetAcad Program létjogosultságát, indokoltságát, integrálhatóságát illetően. A HTTP[4] alapítvány hosszas megfeszített munkájának köszönhetően, valamint a képzés harmonizációjának, integrálhatóságának vizsgálata alapján elmondhatjuk azt, hogy OKJ - ban megfogalmazódott követelmények összeegyeztethetőek, megfeleltethetőek a képzésben, programban megszerezhető különböző szintű iparági minősítésekkel, képesítésekkel, melynek köszönhetően az elérhető e - learning tananyagok is maradéktalanul lefedhetik azokat az oktatási kérdéseket, átadandó ismeretanyagokat, melyek elsajátítása szükséges lehet egy adott szakképesítés megszerzése érdekében. Ennek eredményeként az oktató tanárok kezébe is egy hatékony oktatási eszköz kerülhet, hiszen sok esetben a rendelkezésre nem álló tankönyvek, hiányzó tananyagok, nem megfelelő oktatási anyagok problematikáját is az e - learning tananyag nagyon könnyen áthidalhatja. Nem beszélve arról, hogy a tananyagfejlesztés időigényes és fárasztó terhétől is megkímélhetjük őket. Mivel az online anyagok több nyelven is elérhetőek, így a nyelvismerettel nem rendelkező vagy tanulmányaikat éppen idegen nyelven folytatni kívánó diákok elvárásainak is eleget tehet.

A HTTP Alapítvány, mint a hazai CISCO Hálózati Akadémiai Képzés - NetAcad Program kiemelt és legfőbb gondozója, az OKJ - ban meghatározott követelményeknek megfelelően, alapvetően három különböző képzési szintet és az ott elérhető képzéseket, kurzusokat és iparági minősítéseket ajánlja az egyes szakképző intézmények figyelmébe, melyet a lentebb látható ábra szemléltet.

1. ábra A hazai CISCO Hálózati Akadémiai Képzés - NetAacad Program egyes képzéseinek, kurzusainak integrálhatósága a szakképzés rendszerébe [4]

Mint az a mellékelt ábrából is látható egészen középiskolai szinttől elindulva, a felsőfokú képzéssel bezárólag, a közbülső képzési szinteket lefedve kínál képzéseket, kurzusokat, minősítéseket és képesítéseket a CISCO Hálózati Akadémiai Képzés - NetAcad Program. Ennek megfelelően középiskolai szinten alapvetően a CISCO IT[5] Essentials PC Hardware and Software, az alap- és középfokú szakképzés szintjén az CISCO IT Essentials PC Hardware and Software, valamint a CCNA[6] Routing & Switching, a felsőfokú szakképzés szintjén a

[4] Hálózati Tudás Terjesztésért Programiroda Alapítvány
[5] Information Technology
[6] CISCO Certified Network Associate

CCNA Routing & Switching, valamint a CCNA Security, BSc[7] szinten pedig a CCNA Routing & Switching, a CCNA Security és a CCNP[8] képzések, kurzusok integrálhatóságának, megfeleltethetőségének lehetőségét látja.

Hogyan is kapcsolódhat ez az általam vizsgált témához, a Magyar Honvédségben folyó képzés, oktatás rendszeréhez? Egyrészt a 2016. évi Országos Képzési Jegyzékben szerepelnek a Magyar Honvédséghez köthető szakképesítések és szakirányok is, amelyek az alábbiak [5]:
Honvéd Altiszt szakképesítés:

- *híradó ágazat;*
- átvitel- és kapcsolástechnikai;
- eszközüzemeltető;
- rádióállomás - üzemeltető;
- *katonai informatikai - rendszer üzemeltető ágazat;*
- légi vezetés ágazat;
- műszerész ágazat;
- fegyverműszerész;
- páncéltörő rakétaműszerész;
- parancsnoki ágazat,
- ABV védelmi;
- légvédelmi rakéta és tüzér;
- repülésbiztosító ágazat;
- repülőműszaki ágazat;
- avionika szerelő;
- sárkány - hajtóműszerelő;
- speciális felderítő ágazat;
- elektronikai hadviselés;
- rádióelektronikai felderítő;
- szerelő ágazat;
- műszakigép - szerelő;
- valamint páncélos és gépjárműszerelő szakirányok.

Honvéd Zászlós szakképesítés:

- biztonsági ágazat;
- katonai felderítő;
- nemzetbiztonsági;
- rádióelektronikai felderítő;
- *híradó és informatikai ágazat;*
- légi vezetés ágazat;
- valamint speciális felderítő ágazat.

Ezen szakképesítések és szakirányok sorából a számunkra relevánsakat emeltem ki. Láthatjuk tehát, hogy a CISCO Hálózati Akadémiai Képzés - NetAcad Program egyrészt olyan korszerű ismereteket nyújt az annak keretében tanulmányaikat folytató hallgatóknak, amely szakmai vonalon integrálható a személyi állomány, az infokommunikációs erő oktatási és képzési rendszerébe[9], másrészt az érintett területeknek, e - learning oktatási anyagoknak, képzéseknek, kurzusoknak, minősítéseknek és képesítéseknek köszönhetően mindez

[7] Bachelor of Science
[8] CISCO Certified Network Professional
[9] Az NKE HHK szakirányú képzésén szintén kiemelt szerepet játszik a CISCO Hálózati Akadémiai Képzés.[6]; [7]

összeegyeztethető az Országos Képzési Jegyzékben megfogalmazott elvárásokkal és követelményekkel.

Mindezeken túlmenően a szakmai állomány szemszögéből olyan pozitív hozadékokkal is bírhat e korszerű ismeretek oktatási, képzési, felkészítési rendszerbe történő integrációja, így akár a CISCO Hálózati Akadémiai Képzés - NetAcad Program elérhetőségének, hozzáférhetőségének részükre is történő biztosítása, hogy egy lehetséges alternatívát, a civil szférában is elfogadott minősítést, képesítést biztosíthatunk számukra a Magyar Honvédségből történő esetleges kiválásuk esetére. Szükség lehet erre azon okból kifolyólag is, mert megítélésem szerint a megváltozott életpályamodellnek következtében az állomány tagja könnyen kikerülhet a Magyar Honvédség szervezetéből valamely elvárásnak, követelménynek objektív, rajta kívülálló okból történő nem megfelelésnek következtében. Ezért őt, miközben a szervezet számára hasznos és kiváló szakembernek készítjük fel, képezzük ki, a civil munkaerőpiacon is versenyképes szereplőként tüntethetjük fel, könnyen átültethető, korszerű ismeretekkel vértezhetjük fel, a civil szférában is elfogadott, az ott megszerezhető végzettségekkel egyenértékű szakképesítést adva kezükbe, mely egy esélyt biztosít számukra a szervezetből történő problémamentes kiválásra, beilleszkedésre, a közszolgálat kapcsolódó területein történő elhelyezkedésre. Bárkiben jogosan felmerülhet a kérdés a versenyképes és kevésbé versenyképes jövedelmekkel, a szellemi tőke egyirányú kiáramlásával kapcsolatban. Erre a legfrappánsabb választ talán egy Szent-Györgyi Alberttól származó idézettel tudnám megadni, miszerint *„Az iskola arra való, hogy az ember megtanuljon tanulni, hogy felébredjen tudásvágya, megismerje a jól végzett munka örömét, megízlelje az alkotás izgalmát, és megtalálja azt a munkát, amit szeretni fog.”* A tudásvágy, a motiváció, az iránymutatás, az érdeklődés felkeltése, a jól végzett munka, a magas szakmai képzettség elismerése és a tudás megszerzésének lehetővé tétele talán sok mindenért kárpótolhat.

KIHÍVÁSOKNAK, KÖVETELMÉNYEKNEK, SZABÁLYZÓI HÁTTÉRNEK VALÓ MEGFELELTETHETŐSÉG HAZAI ÉS NEMZETKÖZI SZINTEN

Mindezen gondolatok ellenére az elsődleges cél nem a személyi állomány, az infokommunikációs erő rendszerből történő kiválási lehetőségének biztosítása, mindenáron történő támogatása, a civil szférába történő be- illetve visszailleszkedésük lehetővé tétele, szakmai kompetenciájuk munkaerő piaci értékének növelése és vonzóvá tétele kell, hogy legyen, hanem a megtartás. Az előbbi inkább egy opció, egy alternatíva kell, hogy maradjon a humán erőforrás gazdálkodás eszköztárában, a személyi állományt érintő gondoskodás vonatkozásában. Szükség van erre mindazon okból kifolyólag, hogy az információs társadalom hatásai által is érintett, a negyedik generációs hadviselés elveinek, a szövetségesi tagságból adódó követelményeknek, a szabályzói háttérnek megfelelni akaró Magyar Honvédség egy korszerű ismeretekkel és megfelelő szakmai kompetenciával bíró személyi állománnyal rendelkezzen. Az új típusú hadviseléshez szorosan kötődnek olyan fogalmak, mint az információs műveletek, a számítógép - hálózati vagy más néven kiberhadviselés, a hálózatközpontú hadviselés korszaka, a kiberháborúk megvívásának időszaka, a hálózat nyújtotta képesség, mint a negyedik generációs hadviselés legjellemzőbb momentumai. Ezen újszerű hadviselési elveknek való megfelelés szükségessége mindenki számára vitathatatlan kell, hogy legyen, mely viszont egy jól felkészített, kiképzett személyi állomány nélkül nem

valósítható meg, ennek hiányában ugyanis a biztonságos kibertér[10] [8] állapotának megteremtése elképzelhetetlen. Ezt támasztja alá többek között a legutóbbi, 2016. július 08 - 09. között Lengyelországban, Varsóban megtartott NATO tagországok állam és kormányfőinek csúcstalálkozója is, hogy csak egyet említsünk a meghatározó jelentőségű egyeztetések közül a teljesség igénye nélkül. Ezen a csúcsértekezleten nagyon sok más fontos, a katonai- és politikai szövetség megújulását, védelmi képességei hitelességének alátámasztását, védelmi és elrettentő képességeinek megerősítését célzó döntés mellett döntöttek arról is, hogy az úgynevezett operatív hadviselés területét kiterjesztik a kibertérre is. Ennek egyenes ágú következménye lett, hogy a NATO alapokmánya 5. cikkelyének egykori kollektív védelemre vonatkozó elgondolását újragondolva, kiterjesztették azt a kibervédelmre is, melyet az Észak - Atlanti Szerződés Szervezetének kollektív védelmi feladatai közé soroltak, új feladatként jelenítve meg azt ennek eredményeképpen az egyes tagországok kollektív védelmet megtestesítő feladatai között. Ezeken túlmenően, a teljesség igénye nélkül, még egy részünkre érdeklődésre számot tartó döntést kell figyelembe vennünk, mely történelmi jelentőséggel bír a csúcstalálkozók sorában. Mégpedig azt, hogy a korábban egymással folyamatosan rivalizáló két nagy nemzetközi szervezet, a NATO és az EU közötti együttműködés elmélyítése, elősegítése érdekében egy stratégiai szintű megállapodást kötöttek a szervezetek vezető képviselői úgy, mint Jens Soltenberg NATO - főtitkár, Donald Tusk az Európai Tanács elnöke, valamint Jean - Claude Juncker az Európai Bizottság elnöke. Az aláírt nyilatkozat értelmében különböző együttműködési területeket jelöltek meg, melyek közül számunkra meghatározó jelentőséggel bíró szegmens a „*kiterjesztett és koordináltabb együttműködés (gyakorlatok, oktatás - képzés) a kibervédelem területén.*” [9; 3. o.]

A szövetségesi tagságból adódó katonai kötelezettségek teljesítése mellett az állam is mindent meg kell, hogy tegyen és megtesz annak érdekében, hogy a különböző kiberkihívásokra, veszélyekre, fenyegetésekre hatékony és korszerű eszközökkel állami szinten is reagálni lehessen. Ehhez viszont nélkülözhetetlen és szükséges különböző szintű intézkedések meghozatala, hiszen az információs társdalom, az infokommunikáció robbanásszerű technológiai- és technikai fejlődésének, az IoE[11], a smart world időszakát éljük, melyben soha ennyire könnyű még nem volt az elektronikus szupersztrádához, az Internethez és annak alapját képező számtalan eltérő méretű globális hálózathoz, erőforrásokhoz, szolgáltatásokhoz történő csatlakozás, mely magában hordozza a különböző veszélyek, fenyegetések, biztonsági kockázatok és kihívások megjelenését is. Napjainkban a különböző elektronikus és nyomtatott médiafelületek a digitális állam megteremtésének koncepcióját hangsúlyozzák, melyben egyik legnagyobb kihívást jelentő feladat, megoldandó probléma a felhasználói biztonságtudatosság kialakítása és megteremtése, a digitális analfabetizmus mérséklése, felszámolása, a digitális lábnyom hatásának csökkentése, melynek egyik legkiválóbb eszköze az oktatás, képzés. A felelősség nem hárítható egyértelműen az információs társadalom szereplőinek egyikére sem, hiszen egy közös együtt cselekvés a legkiválóbb alternatíva ezen célkitűzések reális, belátható időn belül történő elérésére érdekében. A számtalan nagy jelentőséggel bíró állami szintű intézkedés közül meg kell, hogy említsük a 1139/2013 (III.21.) Kormányhatározatot Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. A stratégia egyik legfontosabb célkitűzése többek között, hogy „*az Alaptörvény elveivel összhangban, az értékek és érdekek számbavétele, valamint a kibertér biztonsági környezetének elemzése alapján meghatározza azon nemzeti célokat, stratégiai irányokat,*

[10] *„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.”*

[11] Internet of Everything

feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is. A stratégia célja a szabad és biztonságos kibertér kialakítása és a nemzeti szuverenitás védelme a XXI. század meghatározóvá vált új közege, a kibertér létrejöttének következtében megváltozott nemzeti és nemzetközi környezetben. ... Jelen stratégia jelzi, hogy Magyarország a kibertér védelemével összefüggő feladatok ellátását felelősséggel vállalja és a magyar kiberteret, mint a gazdasági és társadalmi élet meghatározó pillérét szabad, biztonságos és innovatív környezetté kívánja alakítani. A megelőzésre épülő hatékony védelmi intézkedések útján elsődleges cél a kibertérben jelentkező és a kibertérből érkező fenyegetések és az ezzel járó kockázatok kezelése, az ehhez szükséges kormányzati koordináció és eszköztár erősítése." [8] A kormányhatározat egyik fontos momentuma az oktatás fontosságának kiemelése, hangsúlyozása, mely megjelenik egyrészt a kiberbiztonság fogalmának értelmezésében. Másrészt ennek a biztonságos kibertérnek a használata érdekében megvalósítandó célként határozzák meg többek között azt, hogy „*a kiberbiztonsági oktatás, képzés, valamint a kutatás és fejlesztés színvonala megfeleljen a legjobb nemzetközi gyakorlatoknak, hozzájárulva egy világszínvonalú hazai tudásbázis kialakításához.*" [8] Mindezeken túlmenően az oktatás a kutatás - fejlesztéssel karöltve, mint alapvető eszköz, terület jelenik meg ebben a kibertérben értelmezett kiberbiztonságnak a megfelelő szinten tartása érdekében, melynek értelmében „*Magyarország kiemelt figyelmet fordít arra, hogy az általános, a közép- és felsőoktatásban, a kormányzati tisztviselők képzésében és a szakmai továbbképzéseken a kiberbiztonság szakterülete integrálódjon az informatikai oktatásba. Magyarország stratégiai együttműködés kialakítására törekszik azon egyetemi és tudományos kutatóhelyekkel, melyek a kiberbiztonsági kutatás-fejlesztésben kiemelkedő és nemzetközileg is elismert eredményeket mutatnak fel, és segítik a kiberbiztonsági kiválósági központok kialakulását.*" [8]

Azt tehát láthattuk már, hogy a NATO kiemelten foglalkozik az új típusú kihívások kezelésével, és ehhez együttműködő kezet nyújt az Európai Uniónak. Azonban az EU önmagában sem tétlen ezen a területen, ugyanis neki is megvannak azok a stratégiai elképzelései, direktívái, szabályzói, melyek természetesen többek között az oktatást és képzést is, mint egy alapvető eszköznek a fontosságát hangsúlyozzák az ezzel kapcsolatban felmerülő kérdések megválaszolása során. A XXI. század társadalma, az információs társadalom. Az információs társadalom a tudást intenzíven felhasználó, új technológiai-, technikai és informatikai termelési világkorszak terméke. Az információs társadalom egy tudásalapú társadalom, a tudás társadalma. A tudás megszerzésének pedig már közhelyszerűen hangoztatott legalapvetőbb eszköze az oktatás, a képzés, mely magában hordozza egyrészt az élethosszig tartó tanulás elképzelését is, mint egyfajta iránymutatását ebben az újkori társadalmi létben, másrészt, pedig mint az oktatást és képzést leghatékonyabban támogató megoldás, az információs és kommunikációs technológiák (IKT[12]) minél szélesebb körben történő elterjedését, mindenki számára hozzáférhetővé tételét. Az EU tulajdonképpen e gondolatok köré építi fel az oktatással, képzéssel kapcsolatos politikáját, ennek szellemében hoz döntéseket az információs társadalom alapvető értékeinek megteremtése és megőrzése érdekében, és természetesen ezzel párhuzamosan nagy hangsúlyt helyez a kibertérrel összefüggésben felmerülő kérdések megválaszolására is. Mi sem bizonyítja ezt jobban, mint például az Európai Unió 2000. március 23 - 24. között Portugáliában, Lisszabonban megtartott csúcsértekezlete, ahol nagyon sok egyéb más kiemelkedő jelentőséggel bíró döntés mellett, elhatározták, hogy Európát 2010 végére a világ legversenyképesebb és legdinamikusabban fejlődő tudásalapú térségévé alakítják. Ennek szellemében született meg

[12] Információs és kommunikációs technológiák

az „*Oktatás és Képzés 2010*” elnevezésű program, kiemelkedő szerepet tulajdonítva az oktatásnak és képzésnek konkrét elvárások megfogalmazása és egyéb más munkaprogramok kidolgozása által, mely az egységesség elvét szem előtt tartva kellő fokú önállóságot biztosított az egyes tagállamoknak az adottságaiknak és szükségleteiknek megfelelő kidolgozás és megvalósítás érdekében, közös munkacsoportok felállítása által. Ennek köszönhetően akkor az oktatási és képzési rendszerek jövőbeni céljai között és az ezekhez kapcsolódó munkaprogramban olyan stratégiai célokat és célkitűzéseket fektettek le, mint például az Európai Uniós oktatási és képzési rendszerek minőségének és hatékonyságának javítása többek között az információs és kommunikációs technológiák (IKT) mindenki számára való hozzáférésének biztosítása által. [10] Az információs társadalom mindennapjainak előrehaladtával természetesen ezek a korábban lefektetett alapelvek, még ha átértékelődve, újragondolva is, de megamaradtak, korszerűsödtek, új szintre léptek. Egyrészt gondoljunk csak arra, hogy reagálva az új kor új típusú kihívásaira és fenyegetéseire, az EU is kidolgozta a saját kibervédelmi stratégiáját azon egyszerű felismerés eredményeképpen, hogy az európai államoknak is ebben a speciális, új típusú térben kell létezniük, ez határozza meg mindennapjaikat, és a társadalom, a gazdaság, a politika és persze a védelmi szféra működése is alapvetően a modern, korszerű infokommunikációs technológiák- és technikák meglététől, és azok alkalmazásától függ jelentős mértékben. Az EU is felismerte azt, hogy a digitális állami lét mekkora pozitív hozadékkal bír Európa fejlődését illetően. Ugyanakkor felmérte annak súlyosságát is, hogy milyen kockázatokkal és következményekkel jár ennek a digitális világnak a sebezhetősége akár az egyénre, akár az egyes nemzetállamokra kivetítve, és milyen intézkedéseket kell megtenni ezek kiküszöbölése érdekében. Ezen folyamatok eredményeképpen válik értelmezhetővé az Európai Unió szintjén is a biztonságos kibertér megteremtésének momentuma olyan stratégiai célkitűzések és intézkedések keretében, mint például a kibertámadásokkal szembeni ellenálló képesség elérése, a számítástechnikai bűnözés drasztikus csökkentése, a kibervédelmi politika és képességek fejlesztése a közös biztonság- és védelempolitika (KBVP[13]) keretében, a kiberbiztonsági ipari és technológiai erőforrások kifejlesztése, valamint egy összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára, valamint az EU alapértékeinek támogatása. [11] Ezen a ponton kapcsolódik össze az Európai Unió szabályozási hátterével a már korábban említett 1139/2013 (III.21.) Kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, de megemlíthetnénk akár a 2014 - 2020 közötti időszakra szóló Nemzeti Infokommunikációs Stratégia (NIS[14]) kialakításának szükségességét is. Ez utóbbinak legfontosabb célja „*hogy koherens képet adjon a magyar információs társadalom jelenlegi viszonyairól, és ez alapján a 2014-20-as uniós tervezési ciklussal egybeeső időtávra meghatározza az infokommunikációs területre vonatkozó fejlesztési irányokat, közpolitikai, szabályozási és támogatási teendőket, és számba vegye az ezek megvalósításához szükséges eszközöket/erőforrásokat.”* [12; 11. o.] Ez a stratégia rengeteg területet érint, ideértve többek között a teljesség igénye nélkül olyan fontos építőelemeket, mint például a digitális infrastruktúra, kompetenciák, gazdaság, vagy magának a digitális államnak az alappillérét. Természetesen ennek egyenes irányú következménye az infokommunikációs technológiáknak- és technikáknak az állam szinte minden területére történő alkalmazásának kiterjesztése, az alap-, közép- és felsőfokú képzésben az informatikai képzés színvonalának emelése, de ugyan úgy érinti ez a stratégia a kiberbiztonság kérdését, és ennek eredményeképpen a nemzeti kiberbiztonsági stratégiát is.

[13] Közös Biztonság és Védelempolitika
[14] Nemzeti Infokommunikációs Stratégia

KÖVETKEZTETÉSEK

Mindezek alapján láthatjuk tehát, hogy egy olyan hazai és nemzetközi új típusú kihívásokkal áttűzdelt környezet, követelmény és elvárás rendszer, szabályzói háttér alakult ki, melyben a CISCO Hálózati Akadémiai Képzés - NetAcad Program és annak a Magyar Honvédségen belül folyó oktatás, képzés rendszerébe történő szerves integrációja kínálhat egy jó megoldást, egy járható útvonalat a siker elérése, a követelményeknek, elvárásoknak való megfelelés, a kihívásokra történő hatékony válaszadás érdekében. Érvként sorakoztathatnánk fel olyan tényezőket többek között, mint például, a képzés, program keretében elérhető „Cybersecurity operations" kurzus Associate szinten a számtalanszor emlegetett kiberbiztonság és kibertér vonatkozásában. Ennél egyszerűbb érv lehet azonban az, hogy bármilyen környezetről, kihívásról, szabályzói háttérről legyen is szó az információs társadalom, a digitális állam, a kibertér, az infokommunikációs technológiák vonatkozásában, mindegyiknek alapja egy modern infokommunikációs hálózati infrastruktúra, abban jelenlévő korszerű technológiák- és technikák, fejlett szolgáltatások, melyek ismerete alapvető és nélkülözhetetlen feltétel. Mindezeknek megfelelően, a Magyar Honvédségben több mint tizenöt éve megkezdett, és folyamatosan végbemenő technikai fejlesztések is ezt támasztják alá. [13], [14] Ezen ismeretek megszerzésének legkézenfekvőbb megoldása pedig az oktatás, képzés biztosítása, melynek eredményeképpen egy megfelelő szakmai kompetenciával felvértezett infokommunikációs humán erő jelenhet meg.

FELHASZNÁLT IRODALOM

[1] BLESZITY J. [et al.]: *Műszaki kutatások és hatékony kormányzás*; Hadmérnök 10. évf. 3. szám (2016. szeptember), pp. 221-242.

[2] BODA J. [et al.]: *Fókusz és együttműködés. A hadtudomány kutatási feladatai*; Honvédségi Szemle 144. évf. 3. szám (2016/3.), pp.3-19.

[3] https://www.nive.hu/index.php/index.php?option=com_content&view=article&id=297 (letöltve: 2017.02.15.)

[4] http://netacad.hu/okj (letöltve: 2017.02.15.)

[5] https://www.nive.hu/index.php/index.php?option=com_content&view=article&id=297 (letöltve: 2017.02.15.)

[6] FARKAS T.: *Signal Officer Training at the National University of Public Service (Budapest, Hungary)* In.: MIKULÁŠ Š. [et.al], (szerk.) New Trends in Signal Processing 2014: Proceedings of the International Conference, Armed Forces Academy of General Milan Rastislav Štefánik, 2014. pp. 37-43.

[7] FARKAS T.: *CIS officer training at the National University of Public Service: capabilities and requirements* In: Miroslav H. (szerk.) Distance Learning, Simulation and Communication (DLSC) Conference. University of Defence, Faculty of Military Technology, Brno, 2015. pp. 84-90.

[8] http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845 (letöltve: 2017.02.15.)

[9] TÁLAS P.: *A varsói NATO – csúcs legfontosabb döntéseiről*; http://netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2016-10-a-nato-varsoi-csucstalalkozojanak-don.original.pdf (letöltve: 2017.02.15.)

[10] KOVÁCS I. V.: *A lisszaboni folyamat és az oktatás;* http://epa.oszk.hu/00000/00035/00083/2004-07-Vt-Kovacs-Lisszaboni.html (letöltve: 2017.02.15.)

[11] http://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52013JC0001 (letöltve: 2017.02.15.)

[12] http://www.kormany.hu/download/a/f7/30000/NIS_v%C3%A9gleges.pdf (letöltve: 2017.02.15.)

[13] FARKAS T.: *A honvédség tervezett kommunikációs hálózata*; Kard és Toll: Válogatás a hadtudomány doktoranduszainak tanulmányaiból 1:(1) pp. 53-57. (2006)

[14] FARKAS T.; SÁNDOR M.: *A honvédség állandó hírhálózatának fejlesztési kérdései* Kard és Toll: Válogatás a hadtudomány doktoranduszainak tanulmányaiból 1:(2) pp. 158-164. (2006)