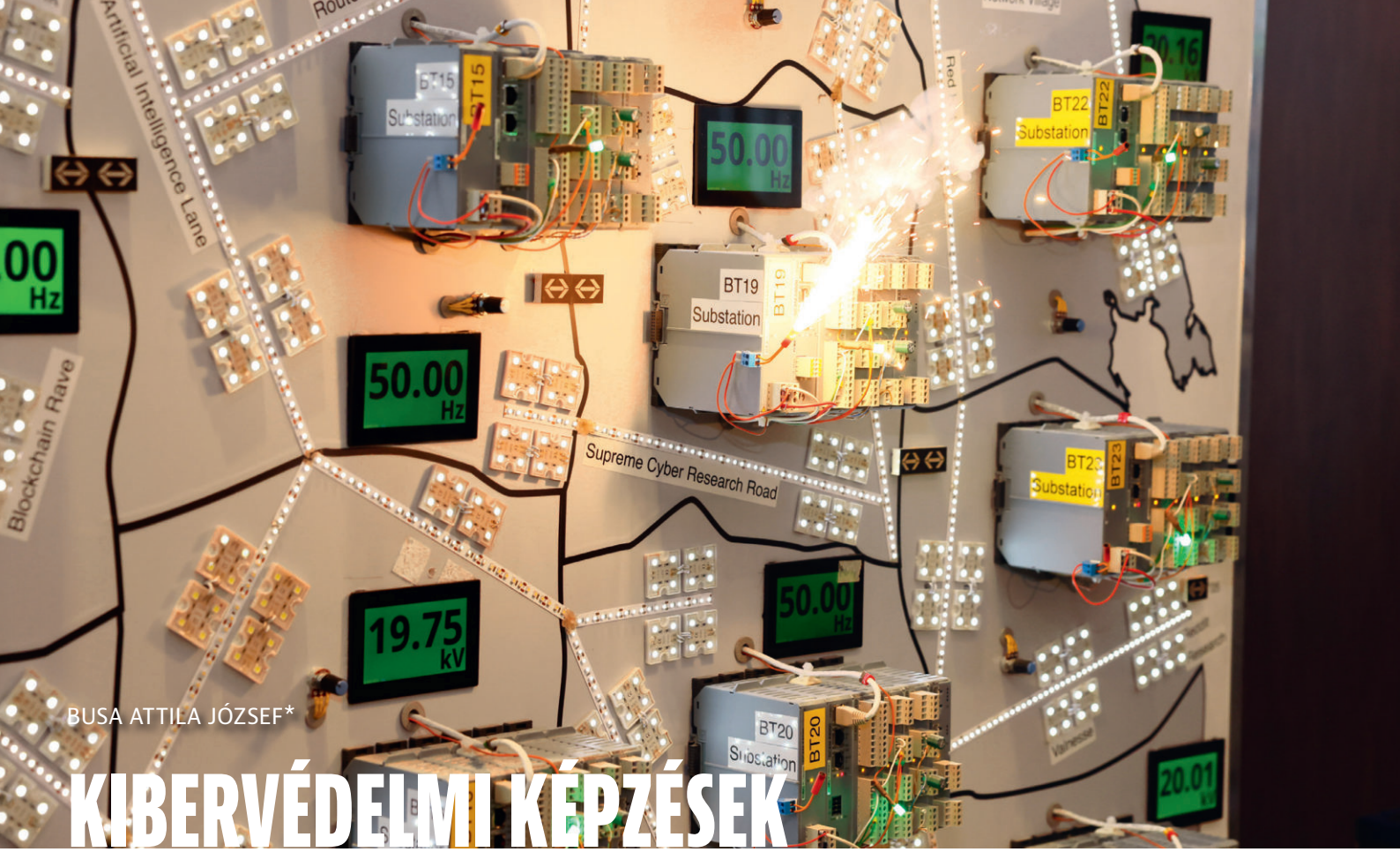


BUSA ATTILA JÓZSEF*

KIBERVÉDELMI KÉPZÉSEK A HONVÉDELEMBEN – EURÓPAI ÉS HAZAI VISZONYLATBAN

Összefoglalás: *A digitális kor kihívásai miatt a kibervédelem egyre fontosabb szerepet játszik a honvédelemben. A cikk célja, hogy megvizsgálja a NATO-n belül akkreditált európai és a Magyarországon létrehozott kibervédelmi képzési központokat, emellett egy lehetséges fejlődési irányt mutasson. Az egyes kiberképzési központok képzési formáinak összehasonlítása a cél egy előre meghatározott szempontrendszer alapján, szem előtt tartva, hogy a magyarországi kiberképzéseknek is helye van a palettán. A cikk röviden ismerteti a hazánkban is elengedhetetlen kibervédelmi oktatási központ létrehozásának okait. Kitér a kibervédelmi feladatok és gyakorlatok komplexitására, a technológiai fejlődés hatásaira és a szervezeti képességek fontosságára mind hazai, mind a NATO szempontjából.*

Kulcsszavak: *kibervédelem, kibervédelmi képzések, Kooperatív Kibervédelmi Kiválósági Központ, Locked Shields, Crossed Swords, kibervédelmi gyakorlatok, Kiber Akadémia.*

Abstract: *The challenges of the digital age make cyber defence an increasingly important part of defence. The aim of the article is to examine the European and Hungarian cyber defence training centres accredited within NATO and to point to a possible direction of development. The aim is to compare the types of training offered by each cyber training centre on the basis of a predefined set of criteria, bearing in mind that there is a place for cyber training in Hungary. I will briefly describe the events that have led to the emergence of a cyber defence training centre in the Hungarian Defence Forces. I will discuss the complexity of cyber defence tasks and exercises, the impact of technological development and the importance of organisational capabilities from both a domestic and NATO perspective.*

Keywords: *cyber defence, cyber defence training, Cooperative Cyber Defence Centre of Excellence, Locked Shields, Crossed Swords, cyber defence exercises, Cyber Academy.*

KIBERTÖRTÉNETI ÁTTEKINTÉS

2007-ben Tallinnban, az észt fővárosban komoly kibertámadás történt, amely az első komoly kiberhadműveletként vált ismertté. A válság középpontjában az Észtországot ért számítógépes támadások álltak, amelyek a kormányzati és gazdasági célpontokra mért sikeres offenzívával teljesen megbénították az ország működését. Az események hátterében az állt, hogy az észt kormány bejelentette: a Vörös Hadsereg Bronzkatona-emlékművét Tallinn központjából a város szélén található katonai temetőbe helyezi át. Ezt követően, vélelmezhetően az orosz Killnet hekkercsoport megindította az észtek elleni összevont kibertámadást. A támadások során számos kormányzati és üzleti weboldal, valamint az online banki rendszerek is teljesen megbénultak. A kibervédelmi incidenst követően a NATO-nemzetek összefogtak, és közös erővel segítettek a digitális középkorba taszított Észtországon.

* Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola. ORCID: 0009-0009-6167-2154

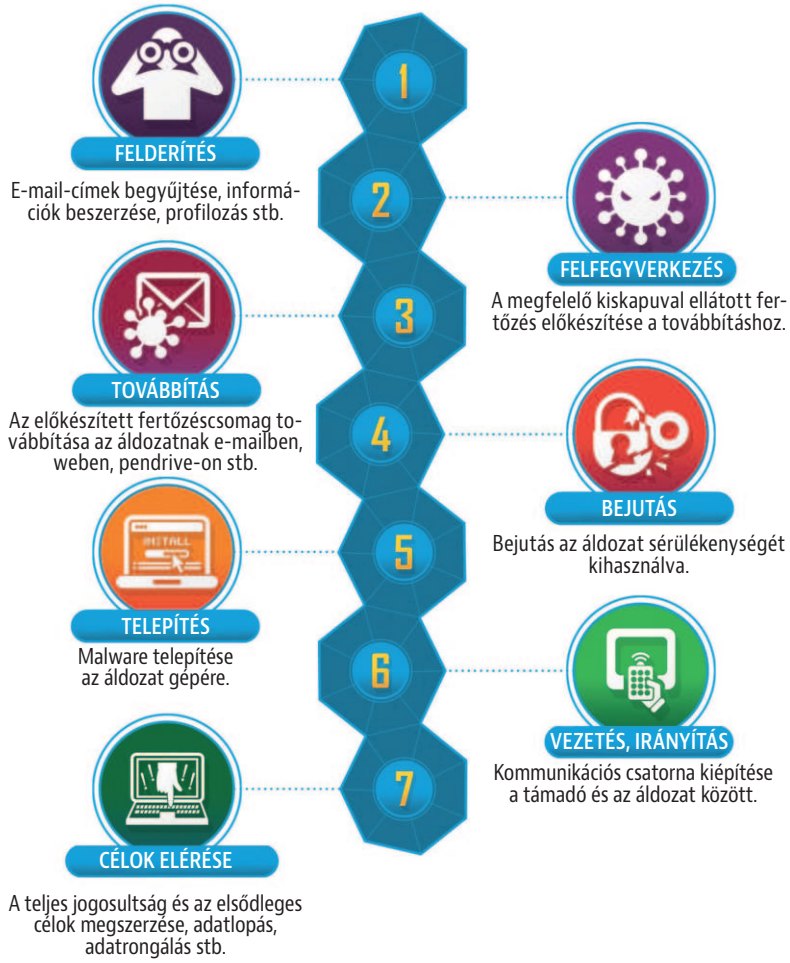
DOI: 10.23713/HT.59.1.08

Ennek köszönhetően két generációnyi digitális fejlődést sikerült megugrania az országnak. A kibervédelem szerepe felértékelődött az eseménynek köszönhetően, ezért 2008-ban megalapították a NATO Kooperatív Kibervédelmi Kiválósági Központot Tallinnban, ahol elkezdődött a specifikus kibervédelmi képzések kidolgozása és oktatása a Szövetségen belül. Kezdetben nagy segítséget nyújtott a központnak az Egyesült Államok és Izrael, később pedig még 32 állam csatlakozott a támogatók köréhez.

A következő mérföldkő a 2010-ben felbukkanó Stuxnet, amely egy számítógépes féreg volt. Ez a kibertámadás az iráni nukleáris program ellen irányult, és kifejezetten a Siemens által használt ipari rendszereket vette célkeresztbe. A vírus célja az iráni urándúsító centrifugák irányítórendszereinek megzavarása és károsítása volt. A Stuxnet rendkívül fejlett volt, és számos különleges technikát alkalmazott, például a folyamatosan változó, robusztus önvédelmi mechanizmusokat, illetve a felfedezés elkerülését szolgáló stratégiákat. Ez az eset felhívta a figyelmet arra, hogy a kibertér már nemcsak kiberbűnözők és hekkerek részéről jelenthet fenyegetést, hanem állami szereplők is használhatják a kibertérben zajló tevékenységeket politikai és katonai célok elérésére. A Stuxnet [1] az egyik első ismert esete volt egy olyan kibertámadásnak, amely valós fizikai rendszerekre irányult, és komoly hatással volt az érintett ipari folyamatokra.

A 2010-es évek utolsó negyedévében a kiberbűnözés professzionális szintre lépett. A kiberbűnözők a rosszindulatú szoftvereket kezdték elrejteni, és egyre jobban megszervezték csoportjaikat. Komoly programozói tapasztalattal rendelkeztek, ami sokkal jobb minőségű malware[1]-eket eredményezett. A támadók többnyire saját maguk módosították egyedivé a payloadot[2], pontosan tudták, hogy a támadást elősegítő programkód hogyan épül fel és hogyan működik. A bűnözők egyre motiváltabbak lettek abban, hogy nagyobb anyagi háttérrel rendelkező célpontok után nézzenek. A 2010-es évek hekkerei gyakran előre elkészített eszközöket (toolokat) használtak a kibertámadásokhoz, mivel ezek könnyen használhatók, idő- és erőforrástakarékosak, lehetővé teszik a gyors támadásokat tömeges célpontok ellen is. Az ilyen előre elkészített eszközök elterjedése és nagy hatóereje miatt a fenyegetettség jelentősen megnőtt, és ráirányította a figyelmet a számítógépes rendszerek kibertámadások elleni hatékony védelmének kiemelt fontosságára.

A 2016-os NATO-csúcstalálkozón az állam- és kormányfők egyöntetűen kinyilvánították a kibertér operatív területté válása melletti elkötelezettségüket, ennek megfelelően pedig elfogadták azt negyedik műveleti dimenziónak (a szárazföldi, a légi és a tengeri mellett). [2] A világűr csak ezek után, 2019 decemberében vált az ötödik műveleti területté. A kibervédelem megerősítése érdekében a tagállamoknak új kibervédelmi stratégiát kell kidolgozniuk, emellett erősíteniük kell a kiber ellenállóképességüket. [3] Ezt követően több nemzetnél is stratégiai szinten kezdenek foglalkozni a kibervédelmi képzések megszervezésével.



1. ÁBRA.
Lockheed Martin-féle kibertámadási lánc [5]

A KIBERVÉDELMI KÉPZÉSEKKEL SZEMBEN TÁMASZTOTT KIHÍVÁSOK

Hatékony és átfogó kiberbiztonsági képzési koncepció tervezéséhez fontosnak tartom megvizsgálni egy kibertámadás „sikeres" létrejöttének lépéseit. A kibertámadási folyamat egyes elemeihez szükséges kompetenciák felállítása az első lépés. Kutatásom kiindulási alapjaként a Lockheed Martin-féle kibertámadási láncot (cyber

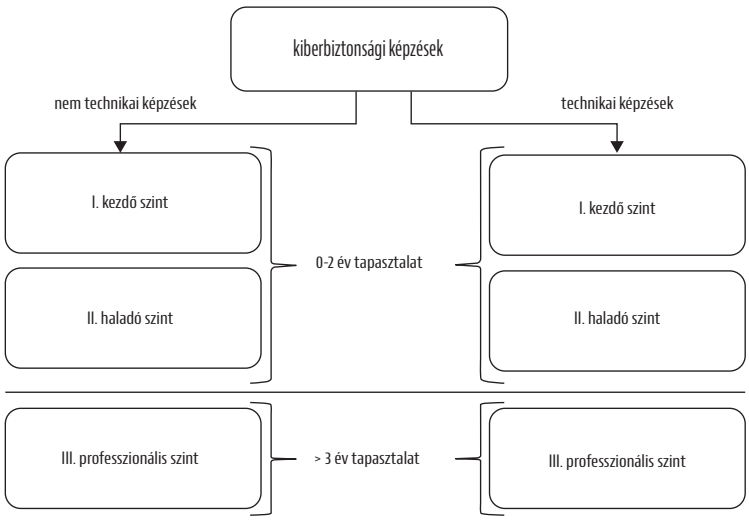
[1] Az angol malware (a malicious software rövidítése), magyarul: rosszindulatú szoftver, kártevő szoftver, kártékony szoftver, káros szoftver.
[2] A támadó által a célrendszerbe juttatott kártékony programkód vagy adat.

killchain)[3] [4] (1. ábra) vettem alapul. A támadásokra teljes egészében nem lehet egy általános sémát ráhúzni, azonban a kiberbiztonsági szakmában ez a legismertebb eljárás. Egy átgondolt kibertámadás felépítése összetett folyamat, amely a támadók részéről kitartó erőfeszítést igényel, és egyre nehezebbé válik a technológiai fejlődésnek köszönhetően.

Az első lépésnél feltüntetett felderítéshez szükséges kompetenciák halmazába tartozik a nyílt forrásokból elérhető információk megszerzésének tudománya (Open Source Intelligence – OSINT[4]), a legtöbbször előnyösebb jogosultsági szint elérésére irányuló, megtévesztésen alapuló technikák (social engineering[5]) ismerete, valamint az adathalász (phishing) taktikák. Ezekre a technikákra a továbbiakban nem technikai képességként fogok hivatkozni. A megfelelő védekezési szint eléréséhez szükséges fejlesztendő terület ezen a szinten a kibertudatosság kialakítása. Kiemelten fontos továbbá a vezetési szinten történő, illeszkedő és szükséges kiberbiztonsági szervezési folyamatok koordinálása, illetve a megfelelő szabályzók elkészítése és azok betartatása.

A felfegyverkezés és a továbbítás már kissé magasabb szintű ismereteket igényel, így a technikai képességek körébe sorolhatók. A védelem szempontjából a fejlesztendő terület ezen vonatkozásban a programozási és hálózatbiztonsági ismeretek magas szintű ismerete.

A 4-es, 5-ös, 6-os és 7-es szinten a támadás elmélyítéséhez már egy magasabb technikai szintre van szüksége a támadónak, ahol programozási, operációsrendszer-ismereti és hálózatismereti képességekkel is rendelkeznie kell, ráadásul magas szinten. A biztonság növelése érdekében a felsorolt technikai képességeket egy magasabb szinten kell fejleszteni a megfelelő tudás elérése érdekében. Ezen képességek fejlesztésére kiválóak a nemzetközi kibervédelmi gyakorlatok, ahol a valósághoz nagyon hasonló környezetben tudják szimulálni a kibertámadásokat, ezáltal fejleszthetők a szükséges védekezési technikák, praktikák.



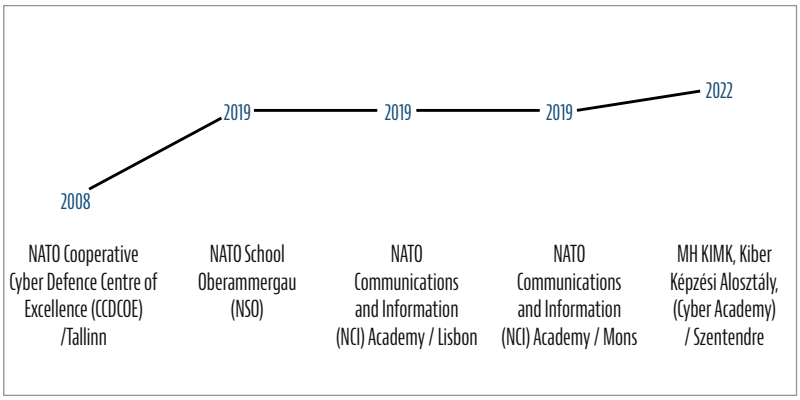
2. ÁBRA. **A kiberbiztonsági képzések szakmai tapasztalati szintjei** (A szerző szerkesztése)

A KIBERBIZTONSÁGI KÉPZÉSEK VIZSGÁLATÁHOZ FELÁLLÍTOTT SZEMPONTRENDSZER

A kiberbiztonsági szakterületek az egyes képzési területeken belül is meglehetősen szerteágazók lehetnek, ezért szükség van egy közös szempontrendszer felállítására, amely a későbbiekben segít besorolni az egyes kiberképző intézeteket az általuk szervezett tréningek alapján, legyen szó technikai vagy nem technikai képességekről. Ezek tovább bonthatók elért, szakmai tapasztalati szintekre. (2. ábra) Megkülönböztethetünk tehát az egyes képességcsoportokhoz tartozó minimális szakmai tapasztalatot igénylő (kevesebb, mint 2 év) I. kezdő, II. haladó szinteket, valamint a már releváns szakmai tapasztalati szintet igénylő (több, mint 3 év) III. professzionális szintű képzéseket.

A 2. ábra lépéseinek vizsgálata segítséget nyújt abban, hogy egy képzés vizsgálata során milyen kompetenciák fejlesztésének szükségessége merül fel. Így egyes képzéseket tovább bonthatjuk a kibervédelmi folyamatban fejlesztendő kompetenciájuk alapján. Megkülönböztethetjük az alábbi szakterületeket:

- információgyűjtési szakterület: phishing, osint, social engineering stb.;
- hálózatbiztonsági szakterület;
- Windows szerverismereti szakterület;
- Linux szerverismereti szakterület;
- kliensoldali Windows ismereti szakterület;
- kliensoldali Unix alapú rendszerismereti szakterület;
- kiberbiztonsági csapatirányítói szakterület;



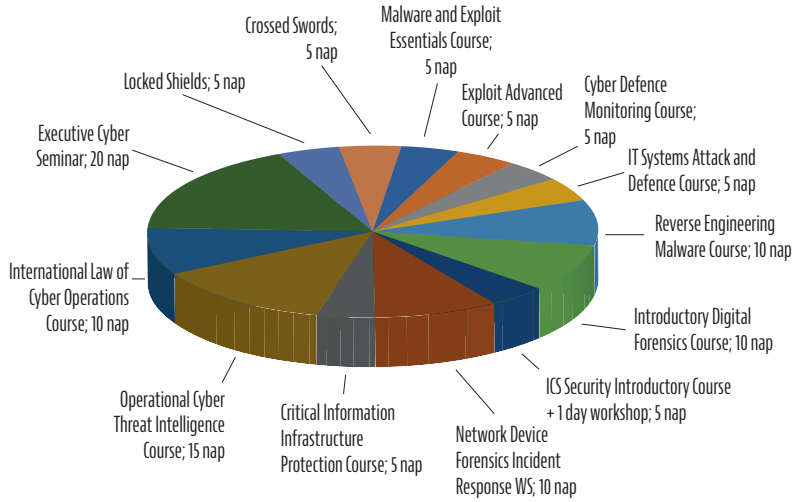
3. ÁBRA. **Főbb kibervédelmi oktatóközpontok alapítási dátumai a NATO/EU-ban** (A szerző szerkesztése)

[3] A cyber killchaint mint fogalmat nagyon ritkán használják magyarul. Kibertámadási láncot jelent, és a kibertámadások különböző fázisait írja le, amelyeket egy támadó követhet a támadás végrehajtása során.

[4] A globális információs robbanás a 20. század végén, a 21. század elején gyökeresen átformálta a hírszerzés feladatrendszerét, mert a nyílt információk tömegében kell megtalálnia az ellenfél igazi titkait.

[5] A social engineering pszichológiai manipuláció, amely az áldozat megtévesztésén alapul.

4. ÁBRA. **A NATO CCDCOE kibervédelmi képzései és gyakorlatai** (A szerző szerkesztése)



- kiberbiztonsági szervezői, vezetői szakterület.

A fent kialakított szempontrendszer alapján a képzés elvárt szakmai tapasztalati szintjének és a fejlesztendő kompetenciaterületnek köszönhetően a különböző kiberbiztonsági képzések beazonosíthatóak. Ennek eredményeként a későbbiekben vizsgált oktatóhelyeknél a futó képzések tekintetében beazonosítható, hogy az egyes intézményeknek melyek az erősségei, és melyek azok a területek, amelyek fejleszthetők a jövőben.

KIBERVÉDELMI OKTATÓKÖZPONTOK FELÁLLÍTÁSA

Jelen fejezet célja a főbb, nem iskolarendszerű, katonai kiberképző intézetek bemutatása, különös tekintettel a Tallinnban, Oeirasban, Monsban, Oberammergauban, valamint Vardóban felállított kibervédelmi intézetek fontosságára. A kutatásom a fent felsorolt intézmények NATO-tagok által igénybe vehető tanfolyamaira terjedt ki. Majd ezt követően a Magyarországon folyó tanfolyamrendszerű képzéseket állítom párhuzamba a nemzetközi tanfolyamokkal.

Alapítási idejüket tekintve mindenképpen a tallinni iskola tekinthető a NATO-ban a legelsőnek, még akkor is, ha az újdonsült kiberbiztonsági (hálózatbiztonsági) képzések megjelennek a nagy múltú oberammergaui NATO-iskolában is, melyet 1953-ban alapítottak, és a nemzetközi tiszthelyettesképzés egyik kiemelkedő alappilléreként vált ismertté. A német alma máterben 2019-ben jelentek meg először online képzési formában a kiberbiztonságot érintő kurzusok. Szintén ebben az évben nyitotta meg kapuit a NATO Communications and Information Agency által patronált NCI Academy. A több székhelyű képzési intézmény Monsban és Oeirasban tartja a kibervédelemmel kapcsolatos oktatást. A fent felsorolt intézmények közül mind hirdet a NATO-tagállamok katonái számára elérhető kurzusokat. A magyarországi kiberképzőhely, a Magyar Honvédség Kiber és Információs Műveleti Központ, Kiber Képzési Alosztály 2022. január 1-től működik a jelenlegi formájában, amelynek tanfolyamai nemzetközi viszonylatban egyelőre nem elérhetőek. Az egyes iskolák alapítási dátumait a 3. ábra szemlélteti.

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, TALLINN

A NATO Cooperative Cyber Defence Centre of Excellence-et (CCDCOE) 2008-ban hozták létre, amely az Észt Kiberbiztonsági Stratégia részeként a kibervédelmi, -biztonsági és -hadviselési területeken nyújt szakértelmet és támogatást.

A központ fő feladatai közé tartozik a kibertérrel kapcsolatos kihívások elemzése, kutatása és oktatása, valamint a kibertérrel kapcsolatos nemzetközi együttműködés elősegítése. A CCDCOE együttműködik más nemzetekkel, intézményekkel és szakértőkkel, hogy javítsa a globális kibervédelmi képességet. [6] Rendszeresen szerveznek kibervédelmi gyakorlatokat és konferenciákat, segítve az országokat és szervezeteket a kibervédelmi képességeik fejlesztésében és tesztelésében. A nemzetközi kibervédelmi gyakorlatok rendkívül fontosak az informatikai biztonság és az online védelem szempontjából. Az információs technológiák robbanásszerű fejlődése miatt egyre több személyes és üzleti adatot kezelünk az interneten, így a kibertámadások által okozott kár is egyre nagyobb. A gyakorlatokon szimulálni tudják a különböző kibertámadásokat, a vírusok, férgek, trójaik, illetve adathalász támadások hatásait a teljes infrastruktúrára. Az ilyen támadások következményei súlyosak lehetnek, például adatvesztés, személyazonosság-lopás, pénzügyi csalás, de akár egy egész szervezet megbénulását is okozhatják. A nemzetközi kibervédelmi gyakorlatok és együttműködések különböző országok, iparágak, vállalkozások és intézmények között segíthetnek az ilyen támadások elhárításában és a károk minimalizálásában. A gyakorlatok általában magukban foglalják a biztonsági szabályok és eljárások kidolgozását és betartását, a biztonsági eszközök telepítését és frissítését, valamint a személyzet oktatását és felkészítését. Az online világ globális jellegét tekintve a kibervédelmi kihívások nem ismernek határokat, ezért a nemzetközi együttműködés lehetővé teszi az információk és a szakértelem megosztását, valamint a különböző országok és szervezetek közötti erőforrások hatékony felhasználását. Számos éles helyzetet szimuláló nemzetközi kibervédelmi gyakorlat elérhető, amelyek segítenek felkészülni egy esetleges kibertámadásra mind védekezési (blue team: kék csoport), mind támadási (red team: vörös csoport) oldalról. Az évente megrendezésre kerülő védelmi gyakorlatok a *Locked Shields* és a *Cyber Coalition*. Az offenzív oldalon történő tapasztalatszerzést a *Crossed Swords* gyakorlat teszi lehe-

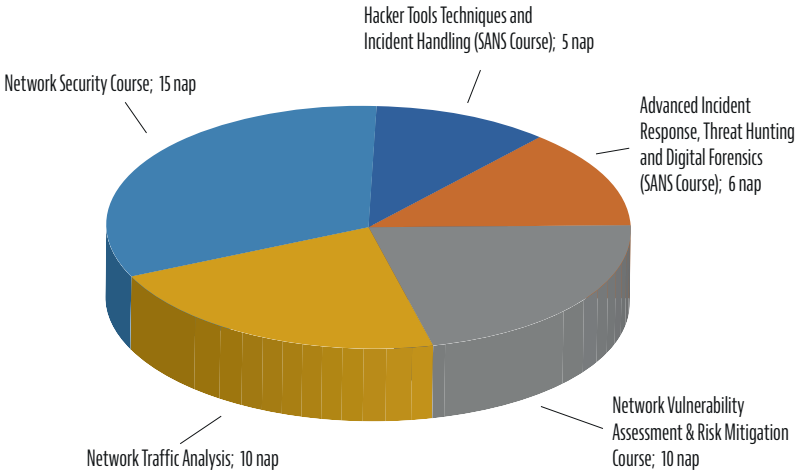
tővé, amelyet minden év végén szerveznek meg a tallinni CR14[6]-es cyber range platformon.

Kutatásom során feltérképeztem, hogy az egyes képzési intézmények milyen kiberbiztonsági témájú céltanfolyamokat szerveznek. A felmérésem alapját csupán a NATO számára is felajánlott képzések adják. Az összegyűjtött adatokból egyértelműen látszik, hogy a CCDCOE igyekszik a kibervédelem teljes spektrumát lefedni. Az ötnapostól a húsznapos tanfolyamig találhatók kurzusok a képzési palettájukon, amelyeket zömében jelenléti oktatási formában tartanak, de van számos online képzésük is. (4. ábra)

Az iskola a NATO-ban egyedülálló módon felvállalja, hogy kiemelkedően fontos a támadói (red) oldal specifikus képzése, amelyet a Malware and Exploit Essentials Course, Exploit Advanced Course, valamint az IT Systems Attack and Defence Course tanfolyamain hajt végre. Továbbá minden évben szervez egy „red teaming" kibergyakorlatot is, a *Crossed Swords*-ot.

Természetesen itt is ki kell hangsúlyozni azt, hogy nem csak a támadó oldal erősítése a fő spektruma az iskolának, de mindenképpen szükséges a megfelelő védelmi intézkedések előkészítéséhez. A védelmi oldal erősítése érdekében léteznek jogi, stratégiai, valamint információbiztonsági képzések mind IT (Information Technology), mind OT (Operational Technology) területen. A megszerzett ismeretek kamatoztatására minden évben több lehetőség nyílik a CCDCOE által szervezett számos kisebb-nagyobb nemzetközi kibervédelmi gyakorlaton, amelyek közül a két legnagyobb a *Locked Shields*[7] és a *Cyber Coalition*[8].

A vizsgálat során alkalmazott szempontrendszer alapján a tallinni iskola képzései széles spektrumban lefedik a nem technikai és technikai képzések valamennyi ágazatát. A NATO-s kiberbiztonsági képzések tekintetében az etalonként ismert képzőintézmény

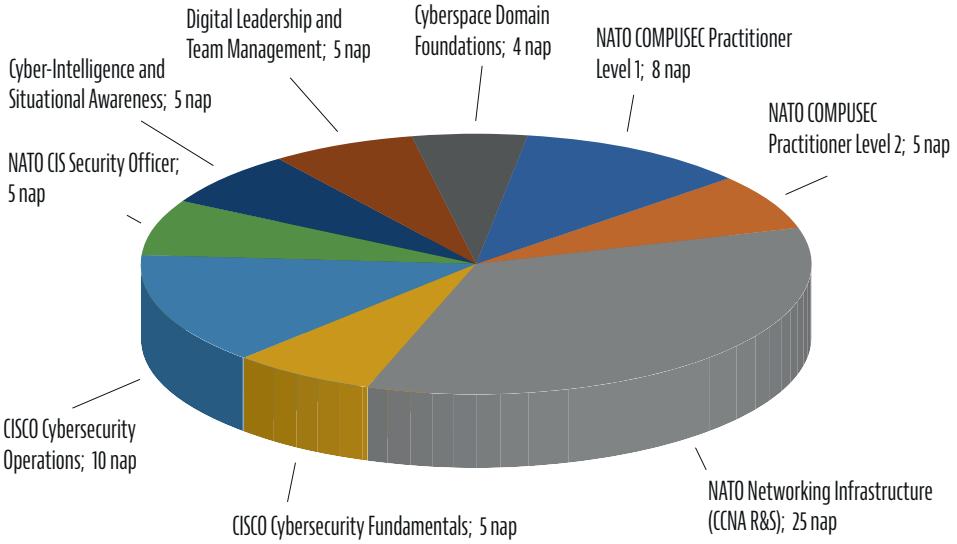


5. ÁBRA.
Az NSO kibervédelmi képzései (A szerző szerkesztése)

egész évben várja a tanulni vágyókat. Fejlődni, fejleszteni mindig lehetséges és szükséges is. Véleményem szerint a támadó oldali felkészítésekből lehetne több a professzionális szintű technikai képzések palettáján.

NATO SCHOOL OBERAMMERGAU

A NATO School Oberammergau (NSO) egy képzési intézmény, amely a NATO tagállamainak, partnerszervezeteinek és más érdekelt feleknek kínál katonai és civileknek szóló oktatási programokat. Az iskola a bajorországi Oberammergauban található. Célja az észak-atlanti térségben és azon túlmutató területeken a nemzetközi biztonság és védelem terén dolgozó szakemberek képzése és továbbképzése. Az intézmény különböző kurzusokat és tréningeket kínál, amelyek a NATO védelmi stratégiájára és műveleti képességeire fókuszálnak. (3. ábra) Az 1953-ban alapított intézmény 2019 óta indít főleg hálózatvédelemre specializálódott kibervédelmi felkészítéseket. 2023-tól online formában teljes NATO-finanszírozással kiszervezi a SANS Technology Institute[9] egyes kurzusait is a jelentkezők számára. A SANS világszerte elismert képzésein az alapok-



6. ÁBRA.
Az NCI Academy lisszaboni kibervédelmi képzései (A szerző szerkesztése)

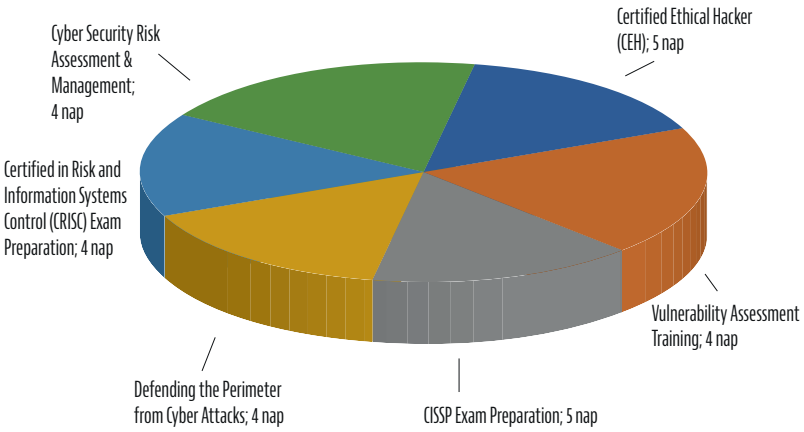
[6] A NATO CR14 egy olyan platform és adatközpont, amely lehetővé teszi a NATO számára a legnagyobb kibervédelmi gyakorlatok és kiképzések lebonyolítását.

[7] A *Locked Shields* egy éves, rendszeres kibervédelmi gyakorlat, amelyet a tallinni Kooperatív Kibervédelmi Kiválósági Központ (CCDCOE) szervez. A gyakorlat során nemzetközi csapatoknak kell számos kibertámadás elleni védelem kiépítésére és fenntartására törekedniük.

[8] A *Cyber Coalition* egy éves, rendszeres nemzetközi kibervédelmi gyakorlat, amelyet a NATO szervez. A gyakorlat célja a tagállamok, partnerországok és szervezetek közötti együttműködés elősegítése a kibertér védelme terén.

[9] A SANS Technology Institute egy nemzetközileg elismert oktatási intézmény, amelynek fő célja magas színvonalú információbiztonság terén jártas szakemberek képzése és továbbképzése.

7. ÁBRA.
Az NCI Academy monsi kibervédelmi képzései
(A szerző szerkesztése)



tól ismerkedhetünk meg a különböző támadási taktikákkal és technikákkal, továbbá elsajátíthatjuk a hackerek által is használt és elterjedt rootkiteket, kártékony szoftvereket, amelyek célja az, hogy a hekkerek jelenlétét elrejtsék a számítógép rendszerében vagy hálózatában. A „root" a rendszergazda (adminisztrátor) jogosultságaira utal, a „kit" szó pedig egy gyűjteményt vagy eszközöket jelent. Tehát a rootkitet arra tervezték, hogy hozzáférjen a számítógéphez, és ezzel teljes ellenőrzést szerezzen a rendszer felett.

Az oberammergaui iskola kibervédelmi területén közel 25 szakképzett oktató dolgozik, és éves szinten hozzávetőlegesen 300-an kaphatják kézhez az okleveleiket a sikeres vizsgákat követően.

A képzések között kizárólag technikai jellegű, alapfokú kurzusok találhatók meg, ahol a 15 napos Network Security Course már egy kellő belépő szintű tudást biztosít a professzionális szintű képzésekhez. A fejlődési irány a nem technikai jellegű képzési lehetőségekben rejlik, még akkor is, ha ezek nagy részét a lisszaboni NCI Academy biztosítja a szakmabelieknek.

NCI ACADEMY, LISSZABON

A NATO Communications and Information Agency (NATO Kommunikációs és Információs Ügynökség) legkiemelkedőbb, információbiztonsággal foglalkozó oktatási intézménye, az NCI Academy (NATO Kommunikációs és Információs Akadémia) a portugáliai Lisszabonban található. [7]

2019 szeptemberében történt megalakulása óta világszínvonalú képzési képességet biztosít a NATO számára technológiai előnyének megőrzése érdekében. Az NCI Academy a NATO kommunikációs és információs rendszerek (Communications and Information Systems – CIS), a légi irányítás és ellenőrzés (Air Command and Control – AirC2), a kiberbiztonság és a kibervédelem terén nyújt képzést. Ezen túlmenően a képzési igények alapos elemzésével és a legújabb tanulási technológiák felhasználásával kulcsszerepet játszik a tagállamok számára új tanulási megoldások megtervezésében és kidolgozásában.

A stratégiai, kiberbiztonsági üzemeltetési, kibertudatossági ismeretek mellett kiemelt szerepet kap a képzések között a hálózatvédelem, amelyet a Cisco Systems, Inc.-del közösen kidolgozott tanmenetre építenek fel. (4. ábra)

Az alap kiberbiztonsági tudatossági képzésen fontosnak tartják az alap kiberfogalmak tisztázását, amelyet a két alapozó tanfolyamuk, a Cyberspace Domain Foundations és a CISCO Cybersecurity Fundamentals biztosítanak a jelentkezők számára 4 és 5 nap időtartamban.

Egyedülállóként jelenik meg a vezetőket célzó kurzus, a Digital Leadership and Team Management, amelyen a kiberbiztonsági szervezési és vezetési ismereteket sajátíthatják el a résztvevők online vagy jelenléti formában.

Az intézmény kiemelt helyen szerepel a NATO információvédelmi képzései között, ugyanis a közel 3000 oktató több mint 8000 főt képez egy évben az online és a jelenléti képzésein együttvéve.

Az NCI Academy képzési palettáján szerepelnek még a nem technikai jellegű képzések kezdő, haladó és professzionális szintű tanfolyamai. A lisszaboni iskola a technikai jellegű képzésekből a haladó szintű ismereti hátteret kiválóan biztosítja. Moduljaival az iskola zseniálisan fogja meg a kibervédelem stratégiai szintjeinek egymásra épülését, és példaértékűen implementálja a biztonsági direktívákat a hálózatbiztonság alapjaiban. Fejlődési irányként a támadó oldali képzéseket lehetne megjelölni, hogy a jövő kiberkihívásainak továbbra is maradéktalanul eleget tudjon tenni az egyik legjobb infrastruktúrával ellátott kiberképzési intézet.

NCI ACADEMY, MONS

Az NCI Ügynökség vezetése alatt működik az NCI Academy monsi intézménye is. A kiberbiztonsági képzések szempontjából azért fontos, mert itt kiemelt szerepet kap a kiberbiztonsági döntéshozatal előkészítése, vagyis a kiberbiztonsági kockázatelemzés és kockázatkezelés. (5. ábra) A belgiumi kurzusok többségében ötnaposak, aminek nagy előnye, hogy a tanfolyam csupán egy munkahétre szakítja ki feladatai közül a munkavállalót.

A nemzetközi kiberbiztonsági képzőintézetek közül itt a legalacsonyabb az oktatók létszáma. A mintegy 25 főből álló, többnemzetiségű, professzionális gárda évente 200 hallgatót képes fogadni, illetve a képzéseket megtartani online és jelenléti formában, hiszen minden képzésük elérhető a speciális oktatóportáljukon is.

A többségében egy munkahetet kitevő szakmai tanfolyamok haladó szintűek és technikai jellegűek, azonban kiváló alapot adnak a későbbi professzionális szintű tudásbázis megszerzéséhez. A kis számú oktatói gárda ellenére a professzionális szintű támadóoldali felkészítések az aktuális kiberfenyegetettségi trendeknek köszönhetően nagyban növelnék a képzési paletta sokszínűségét.

CYBERSECURITY TRAINING CENTRE OF EXCELLENCE, VARSÓ

Az egyre növekvő kiberfenyegetettség és a világszerte tapasztalható hibrid hadviselésére reagálva 2020-ban Lengyelország létrehozta a saját Kiberbiztonsági Képzési Kiválósá-

gi Központját (Cybersecurity Training Centre of Excellence – CSTCoE) Varsóban. A Központ a lengyel Honvédelmi Minisztérium egyik vezető szakmai szervezeti egysége, amely a kiberbiztonság, a rejtjelzés és az információs technológiák területén a fejlesztési irányokat és a szakképzési rendszert alakítja. A Központ a katonák és civilek kiberképességeit növelve fejleszti a Lengyel Fegyveres Erők és a NATO kompetenciáit a kibertérben végzett tevékenységek kapcsán, valamint a szakértői potenciált megszilárdító egységként is működik, és támogatja a Nemzetvédelmi Minisztériumot a nemzeti és nemzetközi kiberképzési együttműködések fejlesztésében.

A Központ a képzéseit integrálta az altiszti és tiszti oktatási rendszerbe olyan módon, hogy a már említett képzési szinteken a már meglévő szakok mellé indított kibervédelmi szakokat is. Így biztosítani tudja az utánpótlást, és nem szorul kizárólag a civil szférából bevonzott szakemberekre. Ez a példa követendő lehet a magyar képzésben is.

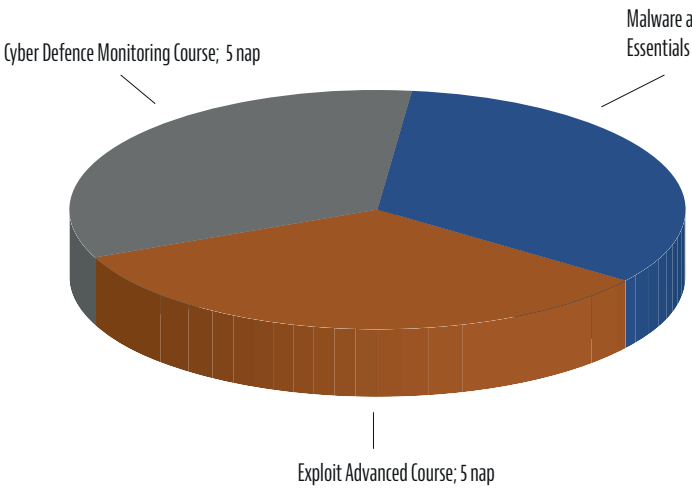
Az említett komplett iskolarendszerű szakokon kívül természetesen szervez specifikus kiberbiztonsági tanfolyamokat is, melyeket 2023 novembere óta NATO-tagállamoknak is felajánl. (6. ábra) Egyelőre három ötnapos, gyakorlatközpontú képzés érhető el csak jelenléti formában.

A varsói Központban 150 oktató dolgozik, és bár még nincs statisztikájuk a NATO-s képzéseikkel kapcsolatban, az iskolarendszerű képzésükön évente 1800 hallgatót képesek oktatni.

A NATO egyik legfiatalabb oktatóközpontjaként még az útkeresés az egyik legfontosabb feladata véleményem szerint. El kell határozniuk, hogy maradnak a néhánynapos kezdő szintű képzéseknél, amelyeket egy évben többször is megtartanak majd, vagy felosztják az évet akár több, egymásra épülő, nagyobb technikai tudást igénylő képzésre.

MAGYAR HONVÉDSÉG KIBER- ÉS INFORMÁCIÓS MŰVELETI KÖZPONT, KIBER KÉPZÉSI ALOSZTÁLY (CYBER ACADEMY), SZENTENDRE

Az összehasonlító és elemző felmérésemből semmiképpen nem hagyható ki a magyarországi képzőintézmény,



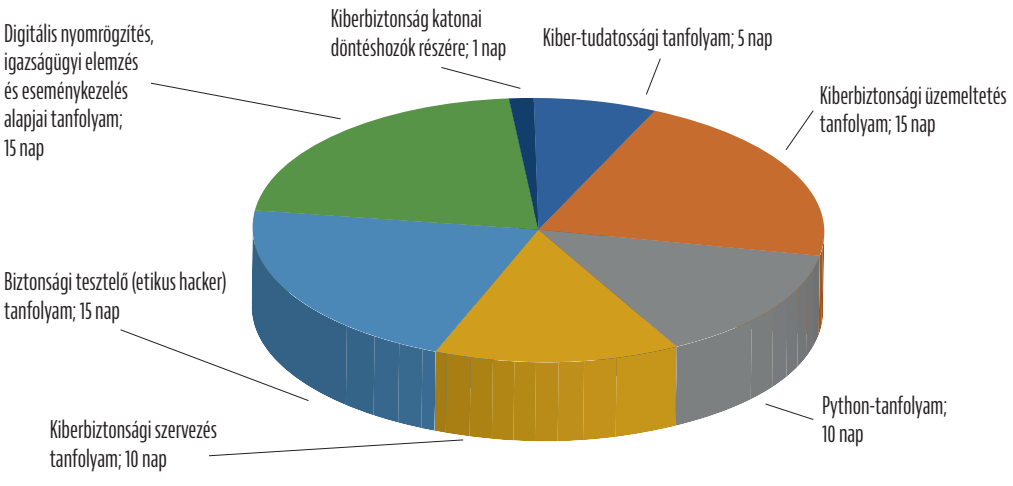
8. ÁBRA. **A CSTCoE kibervédelmi képzései** (A szerző szerkesztése)

amelynek létrehozása a 2016-os varsói NATO-csúcsot követően elengedhetetlenné vált. A környező európai államokban létrehozott honvédelmi kibervédelmi képzési intézményeket alapul véve 2018-ban elkezdődtek a szervezési feladatok. [8]

A 2020-ban megjelent Nemzeti Biztonsági Stratégia is a kiberképességek erősítését sürgette, majd a 2021-es Nemzeti Katonai Stratégia is alátámasztotta egy új Kiber- és Információs Műveleti Központ létrehozását. [9]

A Magyar Honvédség Kiber- és Információs Műveleti Központja (MH KIMK) – alkalmazkodva a biztonsági kihívásokhoz – 2022 elején alakult meg a Magyar Honvédség Katonai Kibertér Műveleti Központ, a Civil-katonai Együttműködési és Lélektani Műveleti Központ, valamint a Budapest Helyőrségdandár Elektronikus Eseménykezelő Főközpont összevonásával. A honvédség nem kinetikus műveleti lehetőségeinek egy szervezetbe történő integrációjával egy olyan új képességet hoztak létre, amellyel gyorsabban és nagyobb eredményességgel kezelhetők a Magyar Honvédség feladatai, egy napjainkra jellemző, bonyolult, hibrid környezetben. A honvédség ezen alakulatának katonái az év minden napján a honvédelmi tárca KCEHH nyílt hálózatrészeinek kiberbiztonságáért felelnek, feladatukat az eseménykezelő központon keresztül látják el. A számítógépes kártevők, zsarolólevelek, rosszindulatú kódok elhárítása napi 24 órában jelent feladatot a központ állományának. Bár 100 százalékos védelem soha nincs, de a 21. századi technikai megoldások értő kezekben vannak, és megbízhatóan biztosítják a megfelelő szintű védelmet. [4]

A megalapult Központban a kiberképzési feladatokat a Kiber Képzési Alosztály látja el. A korábban felsorolt nemzetközi iskolákkal ellentétben a cikk megírásának időpontjában még egyelőre kizárólag hazai viszonylatban szervez képzéseket, kimondot-



9. ÁBRA. **Az MH KIMK kibervédelmi képzései** (A szerző szerkesztése)

tan a védelmi szférában. A nemzetközi képzéseknél megfigyelhettük, hogy teljes spektrumukban nem fedik le képzéseikkel a kibervédelem minden szakterületét, csupán egyes szakterületekre igyekeznek ráerősíteni az egyes iskolákban. A magyarországi tanfolyamok kialakításánál törekedtek arra, hogy a kiberbiztonsági kurzusok egymásra épülő modulrendszerben legyenek elérhetőek, és az összes kiberbiztonsági szakterületet igyekeznek lefedni a védekezési oldalon. (7. ábra)

A kiberképességek megalapozását a megfelelő szintű kibertudatosság jelenti. Ez a képzés különösebb előképzettséget nem igényel. A komolyabb gyakorlati ismereteket követelő képzések mindegyikéhez beugró szintű képzés a Kiberbiztonsági üzemeltetés tanfolyam, amelyre épülnek az Etikus Hacker és a Digitális nyomrögzítés, igazságügyi elemzés és eseménykezelés alapjai elnevezésű tanfolyamok. A jelenlegi formában 4 oktató évente kb. 800 hallgatót képez ki a fent említett kurzusokon.

A korábban felsorolt képzőintézmények közül a magyar iskola a második a CCDCOE után, amelyik igyekszik a nem technikai jellegű és technikai jellegű képzésekből is mind a kezdő, mind a haladó, mind a professzionális szintű kurzusokból is ízelítőt adni az intézménybe látogatóknak. A professzionális szintű támadó oldali felkészítések kidolgozása és a NATO-országoknak való felajánlása lehet a várható fejlődési irány a jövő kihívásainak történő megfelelés érdekében.

A Központ technikai fejlesztése és a szakállomány feltöltése folyamatos. A Magyar Honvédség kiemelkedő fejlődési lehetőségekkel igyekszik bevonzani a munkaerőt. Az intézmény jövőbeni céljai között szerepel az e-learning alapú online képzések fejlesztése, valamint a NATO irányába felajánlható angol nyelvű szakképzések megszervezése.

ÖSSZEGZÉS

Cikkemben kiemeltem néhány fontosabb kiberképző intézményt, amelyeket az általuk nyújtott képzési szakterületek irányából a szakmai kompetenciaszintek segítségével meghatározott szempontrendszer alapján vizsgáltam. A kutatásom alapján kiemelkedően alacsony számú azonos témájú képzés folyik a szóban forgó iskoláknál. Az intézmények között szétoszlanak az egyes kibervédelmi szakterületek, mint például a kibertudatossági, kibervédelmi üzemeltetési, hálózatbiztonsági, stratégiai szintű, jogi, valamint forenzikus ismeretek. Ez a megközelítés tükröződik a NATO alapvető szemléletében is, miszerint az erőforrásokat igyekszik megosztani a tagállamok között. Úgy gondolom, hogy nem lehet vagy nagyon nehéz minden képességet egyenlő mértékben kiemelten fejleszteni egy intézményben. Mi lehet ennek az oka? Talán a legnagyobb problémát a kiberbiztonsági szakemberek hiánya okozza, amely nem koncentráltan csak a hadi ágazatot érinti, hanem az egész világra jellemző. Továbbá nem elég, ha valaki kiváló szakember, a tudását át is kell tudnia adni a hallgatóság felé. A kiberbiztonsági szakterületen belül dolgozók sem érthetnek a legmagasabb szinten mindenhez. Itt arra gondolok, hogy kötelező szegmentálni a tudásfókuszokat is, miszerint külön kell tárgyalni hálózati, szerveroldali, felhasználóoldali, operációsrendszer-specifikus védelmi területekről. Ezeket a területeket felosztva, különböző szintű tudást adva alakították ki az európai NATO kiképzőközpontokban az egyes felkészítéseket, ezért is nehéz egy homogén viszonyrendszert kialakítani az iskolák képzései között. Tanulmányomban éppen ezért választottam szempontrendszerként azt, hogy milyen képzettségi szintet adnak a vizsgált kibervédelmi kurzusok.

A közös együttműködés elkerülhetetlen a nemzetek között a sikeres védelmi szint elérése érdekében. Erre kiváló lehetőséget nyújtanak az összevont kiberbiztonsági gyakorlatok, ahol lehetőség nyílik a nemzeteknek önállóan és csapatban is bizonyítani a rátermettségüket. A 2020-as évek eleje óta hazánk is egyre sikeresebben vesz részt ezeken a gyakorlatokon. A legutóbbi, 2024 tavaszán megrendezésre került *Locked Shields* gyakorlaton Magyarország a szlovák csapattal közös együttműködésben a negyedik helyet érte el a közel 40 induló közül.

Véleményem szerint a magyarországi kiberképző intézmény, vagyis a Magyar Honvédség Kiber- és Információs Műveleti Központ kiemelt helyen szerepelhet a jövőben, amennyiben sikerül a képzéseit meghirdetnie a NATO képzési palettáján. Az online tanfolyami lehetőségek bővítése is segíthet abban, hogy a fontos ismeretanyag minél több emberhez eljusson. Elgondolkodtató példával állt elő a varsói központ, ahol a kibervédelmi képzéseket bevonták a meglévő katonai iskolarendszerű képzések körébe, így biztosítva az állandó, felnövekvő szakember-gárdát. Kikerülhetetlen az oktatói létszám bővítése, amely jelenleg jelentősen elmarad a nemzetközi intézményekéhez képest.

A fentiek alapján látható, hogy a NATO-n belüli kibervédelmi képzési intézmények szerepe kulcsfontosságú a modern kiberbiztonsági kihívásokra való hatékony válaszadásban. Ezek a képzési intézmények segítik a szövetségeseket a kibertérrel kapcsolatos készségeik fejlesztésében, a fenyegetésekkel szembeni gyors alkalmazkodásban, valamint az együttműködés és információcsere javításában, elősegítve ezzel a NATO egészének biztonságát és ellenálló képességét a kibertérben. ■

HIVATKOZÁSOK

[1] Kovács L. és Sipos M. A STUXNET és ami mögötte van: tények és a cyberháború hajnala. Hadmérnök V. Évfolyam 4. szám, december 2010.;
[2] Tóth A. A prágai NATO csúcstalálkozót követő határozatok, megállapodások a parancsnoki rendszer-és a vezetésirendszer korszerűsítésére, valamint az együttes tevékenység képesség fejlesztésére. Hadmérnök 2016. / 3. sz., ISSN 1788-1929, pp. 214–220., 2016.;
[3] Ambrus É. A Well Planned Life, Digital Wellbeing. 05. november 2023. [Online]. Available: https://evaambrus.wordpress.com/2023/11/05/the-importance-of-cybersecurity-capacity-building-for-nations/. [Letöltve: 2023. december 21.];
[4] Busa A. J. Kibervédelmi alapismeretek. In Honvédelmi alapismeretek tankönyv, ISBN 9789633279007, Budapest, Zrínyi Kiadó, 2023., pp. 274–293.;
[5] Lockheed Martin, 1998. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Letöltve: 02. 05. 2024.];
[6] T. Tóth. A NATO Kibervédelmi Kiválósági Központ bemutatása. Nemzetbiztonsági Szemle 2018. / 4. sz., ISSN 2064-3756, pp. 48–62., 2018.;
[7] NCIA WebPage, NATO Communications and Information Agency. 21. december 2023. https://www.ncia.nato.int/about-us/our-locations.html. [Letöltve: 2023. december 21.];
[8] Kovács L. A kiberbiztonság stratégiai megközelítése, Budapest: Nemzeti Közszolgálati Egyetem, 2018., pp. 105–163.;
[9] 614/2022. (XII. 29.) Korm. rendelet a honvédelemről és a Magyar Honvédségről szóló törvény egyes rendelkezéseinek végrehajtásáról, 2023., pp. XI. Fejezet, 42§–46§.