HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 3. szám 213–224.
DOI: 10.32567/hm.2024.3.13

Pozderka Gábor[1]

A Magyar Honvédség kiberképzési rendszerének evolúciója

The Evolution of the Hungarian Defence Forces's Cyber Training System

Absztrakt

A katonai képességek kialakítása során a kibertér mint külön műveleti tér jelenik meg, azonban hatását kifejti minden haderőnem vonatkozásában. A kibervédelmi és kiberműveleti oktatási tematikák esetében ezen keresztfunkció megjelenése elengedhetetlen az összhaderőnemi gondolkodás és művelettervezés megteremtése érdekében. Az elmúlt években a Magyar Honvédség működésében is egyre hangsúlyosabb szerepet kaptak az infokommunikációs szolgáltatások, valamint az ezek védelmét biztosító elektronikus információvédelmi, ebből továbbfejlődve kibervédelmi képességek és a felhasználói tudatosság növelésére irányuló képzések, gyakorlatok. A Magyar Honvédség 2019-ben megalakította a Kiberakadémiát, amely platformot biztosít ezen feladatok végrehajtására mind az ügyintézői, mind a vezetői, mind az üzemeltető állomány részére. A kialakított oktatási tematikát a felmerült igények figyelembevételével rendszeresen aktualizálják, az oktatói állomány folyamatosan nyomon követi a kiberbiztonsági trendek alakulását.

Kulcsszavak: kiber, kiberakadémia, tudatosítás, oktatás, kiképzés

Abstract

During the development of military capabilities, cyberspace appears as a separate domain of war, however, it impacts all other domains. In the case of cyber defence and cyber operations education topics, the emergence of this cross-function (between domains) is

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: pozderka.gabor@hm.gov.hu

essential to joint military thinking and operations planning. In recent years, communications and information systems (CIS) as well as CIS protection services have played an increasingly prominent role in Hungarian Defence Forces operations, further developing cyber defence capabilities, training and exercises aimed at raising user awareness. In 2019, the Hungarian Defence Forces established the Military Cyber Academy, which provides an appropriate platform for the implementation of these tasks for the administrator, management and operating staff. Cyber education topics are regularly updated considering emerging needs and the teaching staff continuously monitors (ever-evolving) cybersecurity trends.

Keywords: cyber, cyber academy, awareness, education, training

Bevezetés

A NATO 2016-os varsói csúcstalálkozóján az országok vezetői egyetértettek abban, hogy a kibertér önálló hadszíntér *(domain),* és a védelme részét képezi a NATO kollektív védelmi feladatainak, és ebben a tekintetben a Szövetségnek ugyanúgy képesnek kell lennie megvédeni a tagállamokat, mint a hagyományos hadszíntereken vívott harcok során.[2]

Magyarország Kormánya és a Magyar Honvédség vezetése érzékelve és megértve az új hadszíntérben rejlő veszélyeket, kihívásokat és lehetőségeket, 2019-ben elrendelte a Kibervédelmi Haderőnemi Szemlélőség (KIBSZ) mint stratégiai szintű vezetési és képességfejlesztési szervezeti elem megalakítását. 2022-ben a KIBSZ feladatrendszere kiegészült a nem kinetikus képességi elemekkel, ennek eredményeként megalakult az MH Kiberműveleti Parancsnokság (KIBP). A KIBSZ a kezdeti képességfelmérést követően, az azonosított hiányosságok mihamarabbi felszámolása érdekében javasolta és kezdeményezte a honvédelmi miniszter részére olyan kibervédelmi képző- és oktatóhely létrehozását, amely a kiberbiztonság, a kibervédelem, valamint az elektronikus információbiztonsági és az elektronikus eseménykezelő beosztásokban feladatot ellátók képzését és továbbképzését biztosítani képes a Magyar Honvédség számára. Ezen javaslat eredményeként a Magyar Honvédség 2019-ben megalakította Szentendre székhellyel a Kiber Képzési Központot, ismertebb nevén a Kiberakadémiát.[3] A Kiberakadémia megalakulásával a Magyar Honvédség képességkatalógusa egy szervezetszerű képzéseket nyújtani képes, korszerű infrastruktúrával rendelkező, az MH egész állományát kiszolgálni hivatott képzőhellyel bővült, amely megfelelő alapot teremtett a kibervédelmi és kiberműveleti képességek kialakításához szükséges képzések folyamatos nyomon követéséhez, továbbfejlesztéséhez. Már a kezdeti célok között szerepelt a honvédtiszti, valamint honvédaltiszti képzésben részt vevők általános, illetve a speciálisan kibervédelmi beosztásokba tervezett állomány tanfolyami rendszerű, illetve képzési tervükbe illesztett felkészítése.

Az oktatási portfolió evolúciójának vizsgálata logikai kapcsolatot teremt a képességfejlesztési célok megvalósulása és kiberműveleti feladatok végrehajtása között. Célom olyan képzési javaslatcsomag megfogalmazása, amely az evolúció következő

[2] NATO 2016.
[3] Draveczki-Ury 2019.

szakaszában elősegíti majd ezen folyamatok sikerességét. A kitűzött cél eléréséhez a korábban kialakított oktatási tematika többütemű vizsgálatán keresztül kívánok eljutni, megértve annak logikáját a továbblépéshez szükséges javaslatok megfogalmazásával. Hipotézisem szerint a Magyar Honvédség feladatrendszeréhez kapcsolódó kiberszakterületi képzéseket a kibervédelmi és kiberműveleti feladatok végrehajtásának érdekében, az arra történő felkészülés jegyében alakították ki, összhangban az érvényben lévő jogszabályi hátérrel, felhasználva a civil szektor tapasztalatait. A hipotézisnek való megfelelést az alábbi feltételek teljesülésén keresztül kívánom vizsgálni és igazolni, valamint szükség esetén kiegészítő javaslatokat megfogalmazni:

- Tudatosság növelése: a kibervédelmi oktatások célja, hogy növeljék a felhasználók tudatosságát a kiberfenyegetésekkel szemben.
- Gyakorlati ismeretek: az elméleti tudás mellett fontos, hogy a résztvevők gyakorlati tapasztalatokat is szerezzenek.
- Biztonsági protokollok: a képzések során bemutatják a legjobb biztonsági protokollokat és gyakorlatokat.
- Rendszeres frissítés: a kibervédelmi oktatásoknak folyamatosan frissülniük kell az új fenyegetések és technológiák ismeretében.
- Szabályozási ismeretek: fontos, hogy a résztvevők tisztában legyenek a vonatkozó jogszabályokkal és szabályozásokkal.

Az evolúció kezdeti szakasza

A Magyar Honvédség feladatrendszere törvényi szinten szabályozott, amelyben a kor követelményeinek megfelelően értelemszerűen megjelennek a kibervédelmi és kiberműveleti hadszintérrel kapcsolatos feladatok is.[4] Magyarország Nemzeti Katonai Stratégiája szintén megerősíti ezen feladatok szükségességét, kiemeli, hogy a kiberfenyegetésnek a hagyományos fenyegetésektől eltérő jellemzői szükségessé teszik a háborúval kapcsolatos fogalmaink átfogó felülvizsgálatát és adott esetben módosítását, a kiberhadviselés anyagi kár okozásában és a közrend megzavarásában potenciálját tekintve egyre kevésbé marad el a hagyományos fegyverektől.[5] Ez a hatás folyamatosan gyorsuló tendenciát mutat a kibertér sajátosságából adódóan, az adott eseményekre adható válaszidők pedig folyamatosan rövidülnek, a siker érdekében olyan kidolgozott eljárásrendekkel kell rendelkezni a vezető és üzemeltető állománynak is, amelyet készségszinten már a felkészülési időszakban elsajátítanak.

Mivel az oktatás és képzés minden esetben hosszú távú „befektetés", az oktatás megkezdése előtt az oktatói állományt kellett kiválasztani, akik megfelelő szakmai háttér birtokában, a szükséges kiegészítő felkészítéseket követően alkalmasnak bizonyultak a speciális képzési tematika kialakítására, a tanfolyami rendszer elindítására. A Kiberakadémia működésének kezdeti fázisában az első körös tanfolyamok tematikájának részleteit alakítottuk ki, figyelembe véve a nemzeti és nemzetközi trendeket,[6]

[4] 2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről.
[5] A Kormány 1393/2021 (VI. 24.) határozata Magyarország Nemzeti Katonai Stratégiájáról.
[6] *Cybersecurity Education… 2022.*

valamint a Magyar Honvédség működéséből adódó sajátosságokat. A tervezés során egyértelművé vált, hogy azon eljárások, amelyek egy civil környezetben működőképesek, nem minden esetben elégítik ki a sajátos feladatrendszerből adódó igényeket, azok biztosítására elkülönült eljárásrendet kell kidolgozni és alkalmazni.

A hiteles, teljes spektrumot átölelő és széles körű oktatási tematika kialakításának céljából, a Magyar Honvédség által üzemeltetett hálózaton és hálózati elemeken azonosított biztonsági események összegzése és megfelelő kiértékelése érdekében a Kiberakadémia oktatói állománya mellett a tervezésbe már a kezdeti szakaszban bekapcsolódtak az MH Elektronikus Eseménykezelő Főközpont (EEFK) szakemberei, akik a hálózatvédelem szempontjából nélkülözhetetlen feladatukat a nap 24 órájában látják el. Ennek a sikeres együttműködésnek folytatásaként 2022-ben megalakult az MH Kiber- és Információs Műveleti Központ (KIMK), amely már egységes képességként integrálta a korábban külön szervezeteknél kialakított információs műveleti elemeket (Kiber Képzési Központ, EEFK, Civil-Katonai Együttműködési és Lélektani Műveleti Központ).

Figyelembe véve és priorizálva a rendelkezésre álló erőforrásokat és igényeket, kezdeti képességként az alábbi képzési portfólió alakult ki:

- Kiberbiztonsági tudatosság tanfolyam (Cyber Security Awareness Course): 1 hét
  - Tartalom: a mindennapi munkavégzés során jelentkező kiberbiztonsági kihívások és a védelem komplex ismeretei.
  - Célközönség: MH teljes állománya.
- Kiberbiztonság – katonai döntéshozók számára tanfolyam (Cyber Security for Military Decision Makers): 2 nap
  - Tartalom: általános kiberbiztonsággal kapcsolatos ismeretek átadása, amely tartalmazza a kibertér meghatározását, a kibertéri kihívásokat, a kibertér védelmével kapcsolatos tervezési eljárások ismereteit.
  - Célközönség: katonai/honvédelmi alkalmazott közép- és felső vezetők.
- Kiberbiztonsági szervezés tanfolyam (Cyber Management Course): 3 hónap
  - Tartalom: magasabb szintű kiberbiztonsági stratégiai, technikai és szervezési ismeretek a kiberbiztonság és az információbiztonság területeken.
  - Célközönség: a kiberbiztonság, az információbiztonság és az elektronikus információbiztonság területén középvezetői feladatokat ellátók.
- Kiberbiztonsági üzemeltetés tanfolyam (Advanced Operators Course): 3,5 hónap
  - Tartalom: magasabb szintű kiberbiztonsági szervezői és tervezői ismeretek átadása, amely kiegészül a CISSP (Certified Information Systems Security Professional, azaz minősített információs rendszer biztonsági szakértő) képzéssel.
  - Célközönség: informatikai üzemeltetésben dolgozó szakemberek.
- Digitális helyszínelő és eseménykezelő tanfolyam (Advanced Analyst Course): 6 hónap
  - Tartalom: kiberbiztonsági incidensek kivizsgálásának technikai ismeretei.
  - Célközönség: informatikai üzemeltetésben és incidenskezelésben dolgozó szakemberek.

A portfolió kialakításakor fontos szempont volt a hatékonyság mellett, hogy melyek lehetnek azok a képzések, amelyek már a kezdeti fázisban megvalósíthatók saját erőforrásokból, és melyek azok, amelyek nemzetközi vagy szövetségesi képzéseken megszerzett tapasztalatokból integrálhatók sikeresen az elkövetkező években a fokozatosság elvét követve. A hatékony jövőbeni feladat-végrehajtás érdekében a KIBSZ állandó szakértőt delegált a tallinni székhelyű Cooperative Cyber Defence Centre of Excellence kutatási és képzési központba (CCD COE), így az ott kialakított új megoldásokat már párhuzamosan alkalmazták a Kiberakadémia portfóliójában is, ennek egyik látványos példája a katonai döntéshozók felkészítése a *kiberdomain* vonatkozásában. A NATO és EU oktatási intézményei is folyamatosan fejlesztik saját specifikált képzéseiket, ennek részeként megjelentek többek között a kiberműveleti tervezői, kommunikációs és jogi szakértői állomány felkészítésére szolgáló tanfolyamok. A kiber- és elektronikus információvédelmi szakterület vonatkozásában meghatározónak tekinthető az NCI Academy Oeiras, valamint a NATO School Oberammergau képzési rendszere, a képességfejlesztés érdekében ezek a tanfolyamok *train-the-trainer* rendszerben működtek. A NATO oktatási rendszerébe visszacsatolásként kerültek a Kiberakadémia oktatói állományának tapasztalatai is a kölcsönös információmegosztás részeként. Nemzetközi téren fontos elemét képezik a képzési tematika kialakításának a hardver- és szoftvergyártó cégek specifikált kurzusai, ennek a tudásnak a bevonzása kezdetben vendégelőadókon keresztül valósult meg, később részben integrálódtak a tanfolyamokba.

A kezdeti szakaszban a képzések elindításával párhuzamosan, a KIBSZ végrehajtotta azon nemzetközi gyakorlatok feltérképezését, amelyek a Magyar Honvédség feladatrendszeréhez kapcsolódóan (beleértve nemcsak a saját hálózatok védelmét, hanem az országvédelmi feladatokat is) valós képességnövekedést eredményezhettek, amelyek tapasztalatai hatékonyan felhasználhatók voltak a hasonló jellegű nemzeti gyakorlatok és képzések kialakítása során. Az MH szervezeti elemei már korábban is részt vettek szakterületi gyakorlatokon, amelyek közül a kiberterület vonatkozásában kiemelkedtek a Cyber Coalition,[7] Locked Shield[8] és CMX[9] gyakorlatok, ezeket beillesztették a kiberszakterület stratégiai tervezési folyamatába. Ebben az időszakban kijelenthető volt a fenti gyakorlatok esetében, hogy bár azok hasonló területhez kapcsolódtak, a végrehajtás során megjelenő feladatok fókuszterületei eltértek egymástól, míg az LS alapvetően a technikai megoldásokra, addig a CC inkább a folyamatokra fókuszált, a CMX pedig egy komplex krízismenedzsmentet modellezni hivatott gyakorlatként jelent meg. A gyakorlatok profilja az évek során kiegészült, átalakult, ma már inkább az intenzitás, kompetitivitás és az együttműködési feladatrendszer mélysége, ami megkülönbözteti őket.

[7] Cyber Coalition – a NATO egyik legnagyobb és legösszetettebb kibervédelmi gyakorlata.
[8] Locked Shields – a NATO Cooperative Cyber Defence Centre of Excellence által rendezett kibervédelmi gyakorlat.
[9] Crisis Management Exercise – a NATO válságkezelési gyakorlata.

Az evolúció jelenlegi szakasza

A tanfolyami tematika hatékonyságának vizsgálatára a KIBSZ és Kiberakadémia szakállománya olyan eljárásrendet dolgozott ki, amely egyszerre biztosítja a tanfolyamok finomhangolását, valamint az újonnan meghatározott követelmények képzésekbe történő beépítését. A 2020–2024 közötti időszakban az alábbi főbb tényezők azok, amelyek jelentős befolyást gyakoroltak a képzések tematikájának átalakítására:

A Kiberbiztonsági tudatosság tanfolyamok esetében kiemelt feladat azok felkészítése, akik jelentős mértékben találkoznak érzékeny adatokkal, vagy munkakörükből adódóan nagy és koncentrált adatmennyiséggel dolgoznak. A felkészítési sorrend priorizálásánál kiemelt figyelmet kapott az ügyviteli pontok üzemeltetéséért felelős, valamint a szervezetek és felső vezetők adminisztratív állománya. Feladatrendszerükből adódóan hosszabb időre kiszakítani őket a napi munkavégzésből igen körülményes, így esetükben egyedi tematika kidolgozása vált szükségessé.

Tartós nemzetközi beosztásokat megelőzően a beosztás függvényében szükségessé válhat az adott helyőrségben, szervezetnél alkalmazott eljárásrendek kibervédelemmel kapcsolatos kiegészítése, aktualizálása oktatás keretében. Egyes speciális célcsoportok számára a jövőbeni feladatrendszerük miatt speciális célképzések szükségesek.

A nemzeti és nemzetközi kiber- és hibrid gyakorlatokra történő felkészüléshez a Kiberakadémia megfelelő platformot képes biztosítani mind elméleti, mind technikai vonatkozású feladatok esetén. Az információs műveletek különböző elemei nem függetleníthetők egymástól,[10] azok folyamatos hatást gyakorolnak egymásra, ahogyan az a KIMK megalakulásakor is alapvetés volt.

A képzéseknek minden esetben az aktuális információkat kell tartalmazni, ennek érdekében az oktatói állomány folyamatos továbbképzése, civil környezetben történő felkészítése is szükséges. Az erőforrás-menedzsment szempontjából számolni kell azzal a ténnyel, hogy nem minden erőforrás használható azonos időintervallumban.

Az online képzések kialakítása erősíti az információbiztonságot, ezzel a módszerrel gyorsabban és nagyobb tömegek megszólíthatók egy időben, azonban a személyes képzések, konzultációk hatékonysága túlmutat ezeken a képzéseken. A képzések megindítását megelőzően minden esetben ki kell alakítani a szükséges technikai hátteret, létre kell hozni a kiértékeléshez szükséges platformot, és minden esetben megfelelően kell méretezni a rendszer keresztmetszetét.

A mélyebb technikai tudást igénylő tanfolyamok esetében fontos a szükséges bemeneteli feltételek megléte, ennek érdekében egymásra épülő tanfolyamok kialakítása.

Figyelembe véve a fent megfogalmazott és csoportosított igényeket, a korábbi portfóliót az alábbi képzésekkel kell kiegészíteni:

- Kiberbiztonsági tudatosság tanfolyam (Cyber Security Awareness Course): 2 nap
  - Tartalom: a mindennapi munkavégzés során jelentkező kiberbiztonsági kihívások és a védelem komplex ismeretei, kiemelt figyelemmel a szervezet feladatrendszerére.
  - Célközönség: szervezetek és felső vezetők adminisztratív-ügyviteli állománya.

[10] Kovács 2023.

- Kiberbiztonsági tudatosság zászlósállomány számára tanfolyam (Cyber Security Awareness): Modulelem
  - Tartalom: a mindennapi munkavégzés során jelentkező kiberbiztonsági kihívások és a védelem komplex ismeretei.
  - Célközönség: zászlós, tanfolyamon részt vevő állomány.
- Kiberbiztonsági tudatosság ÖVAT-[11] állomány számára tanfolyam (Cyber Security Awareness): Modulelem
  - Tartalom: a mindennapi munkavégzés során jelentkező kiberbiztonsági kihívások és a védelem komplex ismeretei altiszti vezető feladatok viszonylatában.
  - Célközönség: ÖVAT tanfolyamon részt vevő állomány.
- Biztonsági tesztelő tanfolyam (Etikus hacker/Ethical Hacker Course): 10 nap
  - Tartalom: a mindennapi munkavégzés során jelentkező kiberbiztonsági kihívások és a védelem komplex ismeretei, tesztelői alapok megszerzése.
  - Célközönség: kibervédelmi beosztásban és incidenskezelésben dolgozó szakemberek.
- Python programozás alapjai tanfolyam: 10 nap
  - Tartalom: programozás alapjainak ismertetése.
  - Célközönség: kibervédelmi beosztásban és incidenskezelésben dolgozó szakemberek.
- Kiberművelet-tervezői képzés (Cyber Operational Planer Training): Online
  - Tartalom: kiberművelet-tervezés alapjai.
  - Célközönség: műveletttervező állomány.
- Forgatókönyvszerű kiképzések (szituációs felkészítések, technikai gyakorlatok):
  - Cyber Range alkalmazása;
  - felkészülés nemzetközi gyakorlatokra (Locked Shields, Cyber Coalition, CMX, MIC);
  - nemzeti és saját szervezésű gyakorlatok (Digitális Csapás, Adaptive Hussars);
  - Kiberműveleti Parancsnokság és KIMK állományának felkészítése, megszerzett tudás szinten tartása;
  - nemzetközi beosztásokat megelőző felkészítések.

Jövőbeni igények és lehetőségek

A Kiberakadémia megalakulásától 5 év telt el, amely elégséges időintervallum ahhoz, hogy értékelni tudjuk az eddig végrehajtott feladatokat, és azonosítani tudjuk a jövőbenieket. Fontos megjegyezni, hogy a kibertérben, így a kiberműveletekben, valamint az azokat végrehajtó állomány tevékenységének esetében is az elsődleges tényező az időfaktor. A 21. század biztonsági kihívásai között első helyen szerepel a hibrid tevékenységekkel és műveletekkel szembeni fellépés, amelynek elemei között megtalálhatók többek között a kibertérben vagy azon keresztül megvalósított információs

[11] Az Acélkocka Altisztképzési Rendszer legmagasabb szintű tanfolyama – Összhaderőnemi Vezető Altiszti Tanfolyam (ÖVAT).

műveletek. A nem katonai környezetben sikeresen alkalmazott technikai eljárások nem minden esetben elégítik ki maradéktalanul a speciális katonai igényeket, azokat megfelelően kialakított katonai biztonsági környezetben a kiberműveleti tervező állomány részére speciális tematika alapján szükséges oktatni. A kiberhaderőnem, ahogyan a fenti összegzésből is tisztán látszik, nem csak technikai szakemberekre épül, a feladatok végrehajtása során bekapcsolódnak a műveleti tervező, kommunikációs, jogi és más szakterületek képviselői is, értelemszerűen ezen feladatoknak az oktatásban is meg kell jelenniük.[12]

A kibertér a számítógépes eszközök világméretű információcsere-hálózatával kapcsolódik össze. A digitális forradalom és az adatfeldolgozó eszközök fejlődése kétségkívül megváltoztatta életmódunkat, a korábban különálló eszközök rendszerbe integrálása fokozatosan történt, ma már a rendszerek más rendszerekkel történő folyamatos adatcsere-lehetőségének megteremtése alapkövetelmény. A dolgok internete (*internet of things,* IoT)[13] lényegében olyan különböző, egyértelműen azonosítható elektronikai eszközöket jelent, amelyek képesek felismerni valamilyen lényegi információt, és azt egy internetalapú hálózaton egy másik eszközzel kommunikálni. A fogalom más szavakkal hálózatba kötött „intelligens" eszközöket takar, amelyek a beépített érzékelőknek és szenzoroknak köszönhetően képesek adatokat gyűjteni. Ez a technológia és az 5G gyorsuló ütemben fejlődik, illetve terjed. A mesterséges intelligencia *(Artificial Intelligence)* jelenleg kiszámíthatatlan fejlődése szintén új távlatokat nyit meg és egyszerre veszélyeket is jelent a szakterületek számára, ennek az oktatásban is meg kell jelennie.[14]

A fegyverrendszerek teljes mértében nem függetleníthetők a fenti folyamatoktól, bár a hardver- és szoftvereszközök specifikáltak, azok alap kommunikációs folyamatai nem térnek el jelentősen. A rendszereket kezelő állomány kibervédelmi felkészítését kiemelt figyelemmel kell végrehajtani, az oktatási tematikák folyamatos felülvizsgálata elengedhetetlen. A komplex gyakorlatok megfelelő platformot teremtenek a kritikusinfrastruktúra-védelmi képességek védelméhez szükséges folyamatok begyakorlásához, a honvédelmi és más ágazatok együttműködésének modellezéséhez. A feladatok sikeres végrehajtása érdekében a kapcsolati és együttműködési rendszer kialakításának már korábban meg kell történnie mind a képzések, mind valós időben történő feladat-végrehajtás érdekében.[15]

Mivel a kibertérben végrehajtott feladatok részben más logikai felépítést követnek, mint a fizikai tér műveleti feladatai,[16] ezért azok megjelenése a katonai oktatási tematikákban kiemelt fontosságú, ennek érdekében a KIBP szoros kapcsolati rendszert alakított ki a Nemzeti Közszolgálati Egyetemmel, az Óbudai Egyetemmel és más oktatási intézményekkel. A szövetségi rendszerekben (NATO, EU, V4, bilaterális) végrehajtott feladatok érdekében rendkívül fontos a nemzetközi kapcsolati rendszer

[12] CCD COE 2017.
[13] *Internet of Things* [é. n.].
[14] Németh–Virágh 2022.
[15] NATO 2020.
[16] Clapson 2023.

kiépítése[17] és folyamatos aktualizálása, ennek megvalósításához kiváló platformot biztosítanak a nemzetközi gyakorlatok és konferenciák.

A Covid–19 a kiberszakterület vonatkozásában is sok változást hozott, a személyes érintkezések számának csökkenésével exponenciálisan nőt a kibertérben történő kapcsolatfelvételek száma, így az alkalmazott rendszerek kitettsége is. Bár a honvédségi rendszerek túlnyomó többségben zártak, az otthonról dolgozás lehetősége ebben a szektorban is megjelent. Ennek a változásnak is betudható, hogy a kibertámadások számában drámai növekedés mutatkozott ezen időszakban, jellemzően a támadók e-mailes adathalászati módszerekre és az ellátási láncot érintő támadásokra helyezték a hangsúlyt. Az oktatási tematikák kialakítása során ezen tapasztalatok felhasználása elengedhetetlen, folyamatos továbbfejlesztésük szükséges.[18]

Figyelembe véve a nemzeti-nemzetközi trendeket és felmerült igényeket, a jelenlegi portfóliót tervezetten az alábbi irányokkal szükséges kiegészíteni (folyamatos utánkövetéssel):

- Online képzési katalógus bővítése, hatékonyságának vizsgálata: folyamatos feladat, amely jelentősen elősegíti a felhasználói tudatosság erősítését a részt vevő állomány létszámának növelésével. A folyamatnak szerves részét kell hogy képezze a visszacsatolások kiértékelése, ellenkező esetben a színvonal szinten tartása nem garantálható.
- Lehetőség biztosítása a részvételre más közigazgatási szervezetek számára a kiberbiztonsági képzéseken: a megszerzett tapasztalatok átadása más közigazgatási szervezetek részére – figyelembe véve az erőforrások rendelkezésre állását – fontos részét kell hogy képezze az egységes országvédelem és az együttműködési rendszer kialakításának. Természetesen ez a folyamat, ahogyan a NATO esetében is láttuk, nem szükségszerűen egyirányú, a más szervezetek által kialakított képzések modulelemként, vendégoktatókon keresztül is megvalósulhatnak.
- Mobil oktatási képességek erősítése, műveleti területen történő képzések technikai hátterének megteremtése: amennyiben csak a jelenlegi oktatási képességekre és infrastrukturális lehetőségekre összpontosítunk, elveszítjük a fejlődés lehetőségét, ütemét és dinamikáját. Olyan megoldásokban szükséges gondolkozni, amelyek biztosítják a mobilitást az oktatói állomány részére, így gyorsabban, nagyobb létszámú felhasználó felkészítése válik lehetségessé, akár műveleti területen is. Fontos a haderőnemek közötti együttműködés az igények meghatározásakor.
- Felhőszolgáltatások és mobilalkalmazások használatának vizsgálata: összhangban a vezető nemzetközi trendekkel a jövőbeni feladat-végrehajtás hatékonyságnövelése érdekében fókuszpontban kell szerepelni ezen alkalmazások használati lehetőségeinek, így erősítve a katonai és nem katonai szolgáltatások közötti interoperabilitás megvalósulását.

[17] Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.

[18] Magas 2022.

- Nemzetközi kiajánlású (ki)képzések (NATO, EU, V4, bilaterális): Magyarország és a Magyar Honvédség nemzetközi pozíciójának, reputációjának, tapasztalatszerzésének, feladat-végrehajtásának erősítése érdekében a nemzetközi képzések kialakítása kiemelt célként kezelendő mind rövid, mind hosszú távon.
- Nemzetközi kibergyakorlatok helyszínének biztosítása (NATO, EU, V4, bilaterális): a kibertér jellegéből adódóan a nemzeti és nemzetközi szolgáltatások és az azokat biztosító infrastruktúra nem minden esteben szegmentálható teljes mértékben, ennek megfelelően a felkészüléseknek, gyakorlatoknak is ezt a logikát kell követniük. A sikeres gyakorlati feladat-végrehajtás egyik alapfeltétele a szükséges platformok kialakítása, ezek a valós műveleti feladatok során is kiemelt szerepet fognak kapni.
- A kiberfizikai rendszerekre való hatásainak vizsgálata: a valós folyamatok oktatása, üzemeltetett rendszerek sérülékenységeinek felderítése (fegyverrendszerek, vezérlőszoftverek, irányítás)[19] olyan kiemelt feladat, amely elemi részét kell hogy képezze a katonai kibertérműveleti erők felkészítésének.
- Más nem kinetikus képzések erősítése, egységes rendszerbe integrálása: az információs műveleti elemek egymásra kifejtett hatásai nagymértékben befolyásolják a kibertérben a feladat-végrehajtás hatékonyságát, a korábban kialakított, nem kinetikus tematikák és képzések (PSYOPS, CIMIC) hangsúlyosabb megjelenése a Kiberakadémia portfóliójában erősítik és gyorsítják a valós műveleti feladatvégrehajtást.
- StratCom-[20] együttműködés erősítése: a gyakorlatokra és valós műveleti feladat-végrehajtásra történő felkészülés érdekében, az információs műveletek teljes életciklusának modellezésében és a hatások elemzésében, szükséges az információs műveleti platform elemei hatékony együttműködésének megteremtése. Ezen modellek kialakításához a Kiberakadémia ideális helyszínt képes biztosítani.

Összegzés

Megállapítható, hogy a Magyar Honvédség megfelelő ütemben alakította ki hiánypótló kiberoktatási központját, ez a szervezeti elem kiváló alapot teremtett a kibervédelmi és információbiztonsági képzések megkezdéséhez.[21] A szervezet és szakterület jelenlegi fejlődési állapota garantálja a továbblépést és a folyamatos fejlődést.

A bevezetésben megfogalmazott hipotézis valósnak bizonyult, a meghatározott feltételek alapján az oktatási tematikák megfelelők, felülvizsgálatuk folyamatosan megtörténik. A jövőbeni képességeket az alábbi irányok figyelembevételével javasolt kialakítani:

[19] Kovács 2021.
[20] Stratégiai kommunikáció: a StratCom kifejezés a stratégiai kommunikációval kapcsolatos tevékenységeket takarja. Magában foglalja a kommunikációs tervek kidolgozását, az üzenetek célzott terjesztését és a hatékony kommunikációs stratégiák kidolgozását.
[21] Országgyűlés Hivatala 2019.

- Kockázatelemzés: a képzések során a kockázatelemzés módszertanát is bemutatják, hogy a résztvevők képesek legyenek azonosítani és kezelni a kockázatokat.
- Interaktív tanulás: az interaktív előadások és szimulációk hatékonyabbá teszik a tanulási folyamatot.
- Kritikus ágazatok védelme: kiemelten fontos a kritikus ágazatokban és rendszerekkel dolgozók képzése, mivel ezek a területek különösen érzékenyek a kiberfenyegetésekre.[22]
- Kiberpszichológia: a kiberpszichológia ismerete segít megérteni a támadók motivációit és módszereit.

A Magyar Honvédség állománya nemcsak elfogadta a kiberképzések rendszerbe illesztését, hanem igényli is azokat, a tanfolyamokra jelentkezők száma minden esetben meghaladja a kiajánlott létszámkeretet. A sikeres evolúciós folyamat következményeként az oktatások mennyisége, színvonala és az oktatók száma folyamatosan növekvő tendenciát mutat, ezzel összhangban hajtja végre az MH Kiberműveleti Parancsnokság a Kiberakadémia jövőképének kialakítását és fejlesztését.

A felmerült igények kielégítése érdekében az oktatáson részt vett állomány visszajelzései alapján az MH kijelölt állománya folyamatosan felülvizsgálja az oktatási tematikák időszerűségét és tartalmát. Az új tanfolyamok véglegesítését megelőzően azokat tesztelik a KIBP- és KIMK-állomány részvételével (speciális tanfolyamok a jövőbeni célközönség bevonásával), azokat a finomhangolást követően ajánlják ki az MH-állomány részére. Az így kialakuló szervezeti ellenálló képesség *(reziliencia)* megfelelő alapot teremt a nemzeti ellenálló képesség erősítéséhez, a megszerzett tapasztalatok átadásához.

A kibertér sajátosságából adódóan a nemzetközi és civil szervezetekkel történő kapcsolattartás nagyon fontos, a kritikus infrastruktúrákat üzemeltető civil szolgáltatókkal közös feladatok végrehajtását a gyakorlatok felhasználásával készségszintre kell fejleszteni.

Felhasznált irodalom

CCD COE (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched.* Online: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

Clapson, Colin (2023): Microsoft Belgian Scrutinises International Digital Battlefield for Western Governments. *VRT NWS,* 2023. február 18. Online: www.vrt.be/vrtnws/en/2023/02/13/microsoft-belgian-scrutinises-international-digital-battlefield/

Cybersecurity Education Initiatives In The EU Member States (2022). [h. n.]: ENISA. Online: www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states

[22] European Union 2016.

Draveczki-Ury Ádám (2019): Átadták a Magyar Honvédség Kiber Képzési Központját. *Honvédelem.hu,* 2019. június 13. Online: https://honvedelem.hu/media/aktualis-videok/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat.html

European Union (2016): *Protecting critical infrastructure.* Online: https://eur-lex.europa.eu/EN/legal-content/summary/protecting-critical-infrastructure.html

Internet of Things [é. n.]. Online: https://www.britannica.com/science/Internet-of-Things

Kovács László (2021): Offenzív kiberműveletek II. Kibererők és képességeik. *Hadmérnök,* 16(3), 119–137. Online: https://doi.org/10.32567/hm.2021.3.7

Kovács László (2023): *Hadviselés a 21. században: kiberműveletek.* Budapest: Ludovika.

Magas Bianka (2022): Kiberhigiéniai kisokos – 1. rész. *Ludovika.hu,* 2022. június 30. Online: www.ludovika.hu/blogok/cyberblog/2022/06/30/kiberhigieniai-kisokos-1-resz/

NATO (2016): *Warsaw Summit Communiqué. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8–9 July 2016.* Online: www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO (2020): *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations.* Online. https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Németh András – Virágh Krisztián (2022): Mesterséges intelligencia és haderő – A mesterséges intelligencia területei. *Haditechnika,* 56(1), 17–22. Online: https://doi.org/10.23713/HT.56.1.03

Országgyűlés Hivatala (2019): *Kiberhadviselés és katonai kibervédelem.* Online: www.parlament.hu/documents/10181/1789217/Infojegyzet_2019_49_Kiberhadviseles.pdf

Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration Text with EEA relevance. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011R0580