DOI: 10.38146/BSZ.2022.6.11

INTERJÚ

„A kiberbiztonság jelentősége a mindennapokban”

Interjú Kovács László dandártábornokkal, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Karának egyetemi tanárával

‘The importance of cybersecurity in everyday life’ Interview with Brigadier General László Kovács, professor at the Faculty of Military Science and Military Officer Training, at the University of Public Service

Hertelendi Lajos
Dr. kooperatív szerkesztő, rendőr alezredes
Belügyminisztérium,
Belügyi Szemle Szerkesztőség
hertelendi.lajos@bmkszf.hu

Hornyik Zsuzsanna
Dr. főszerkesztő-helyettes
Belügyminisztérium,
Belügyi Szemle Szerkesztősége
zsuzsanna.hornyik@bm.gov.hu

Absztrakt

„*Infokommunikáció nélkül nehéz elképzelni az életünket a 21. században, hiszen az internet nélkül ma már fiziológiai szükségleteinket sem mindig tudjuk kielégíteni, ám az ezeket biztosító infrastruktúrák masszív támadásoknak lehetnek kitéve. A kiberbiztonság és kiberhadviselés aktuális kérdéseiről a Ludovika Szabadegyetem előadásán beszélt Kovács László dandártábornok, a Hadtudományi és Honvédtisztképző Kar egyetemi tanára és a Magyar Honvédség Parancsnokságának kibervédelmi szemlélője*." (URL1). Az előadáson olyan alapfelvetések, a mindennapi életünket átszövő, meghatározó körülmények biztonságát veszélyeztető jelenségek merültek fel, amellyel jobb, ha minél szélesebb körben tisztában vagyunk. Tábornok úr az előadását azzal a kérdéssel kezdte, hogy el tudjuk-e képzelni az életünket félóra áramkimaradással. Azt a szituációt, hogy hazaérkezve nem kapcsolunk lámpát, nem nézünk tévét, nem hűtött üdítőt fogyasztunk. Vajon hányan vagyunk képesek erre? A hallgatóság az előadás kezdetétől a végéig néma csendben, megfeszült figyelemmel hallgatta tábornok urat. Arról, hogy mi is az a kiberhadviselés, mióta beszélhetünk róla, mekkora jelentősége van a kiberbiztonságnak a hétköznapi életünkben, kérdeztük Kovács László dandártábornok urat.

Kulcsszavak: interjú, kiberbiztonság, kiberhadviselés

Abstract

"Without infocommunication, it is difficult to imagine our lives in the 21st century, as without the Internet we cannot always meet our physiological needs today, but the infrastructures that provide them can be subject to massive attacks. The current issues of cybersecurity and cyberwarfare were discussed at the Ludovika Free University by Brigadier General László Kovács, professor of the Faculty of Military Science and Military Officer Training and cyber defence observer of the Hungarian Defence Forces Command." (URL1) The presentation raised fundamental issues, phenomena that endanger the security of the determining conditions that interweave our daily lives, which we should be as widely aware of as possible. The General began his presentation by asking whether we can imagine our lives with a half-hour power cut. The situation of not turning on the lights, not watching TV, not having a chilled soft drink when we get home. How many of us are capable of this? From the beginning to the end of the lecture, the audience listened to the General in silence and with rapt attention. We asked Brigadier General László Kovács about what cyberwarfare is, since when we can talk about it, and how important cyber security is in our everyday lives.

Keywords: interview, cybersecurity, cyberwarfare

Mi is az a kiberhadviselés? Mikor volt az első kibertámadás?

A kiberhadviselésnek a szó szoros értelmében véve nincs hivatalos definíciója, a kiberműveleteknek van. Egyrészt az Európai Unióban, másrészt a NATO-ban. Ez utóbbi 2020-ban egy saját doktrínát is alkotott a kiberműveletekről. A kiberhadviselést a kiberműveletek sorozataként szoktuk jellemezni. Gyakorlatilag a kibertér adja magát, ez az egyik markáns színtere a kiberműveleteknek, de ma már ennél lényegesen többet jelent a kiberhadviselés, hiszen a fizikai térre, az információs térre, valamint a kognitív térre is hatással vannak a kiberműveletek. A kiberműveletek fajtáit tekintve léteznek védelmi, illetve támadó jellegűek. Paradox módon azért hajtunk végre kibertámadásokat, hogy védekezzünk. Egy megelőző kibertámadással – védekező céllal – megfoszthatjuk a szemben álló felet a kibertámadó képességétől. Kiberhadviselésről akkor beszélünk, amikor egy ország, egy ország által támogatott csoport vagy csoportok egy másik ország infokommunikációs rendszereibe támadó, ártó szándékkal hatolnak be.

Nehéz időben pontosan meghatározni, hogy mikor volt az első olyan kibertámadás, amelyre a legtöbb szakértő, biztonságpolitikai szakember felkapta a fejét. 2007 április-májusában Észtországot nagyon masszív kibertámadások érték. Ez az a klasszikus időpont, amikor ráébredt a szövetség, a NATO, hogy egy országot úgy is meg lehet támadni, hogy fizikailag nem lépjük át a határát. Észtország 2007-ben már NATO-tagország volt, így természetesen felmerült a szövetségben is az a kérdés, hogy hogyan kell ezt kezelni, hogyan kell védekezni technikai, humánerőforrás tervezéssel és jogi háttérrel. Itt a nemzetközi jogi háttér az, ami azóta is nagyon sokszor szóba kerül. Sőt az elmúlt időben a kiberhadviselés nemzetközi jogi háttere is felerősödött. Számos olyan egyéb támadás is bekövetkezett, amelyek másik országból, országokból érkeztek alapvetően kritikus infrastruktúra, államigazgatás, nemzetbiztonsági szolgálatok, hadseregek, egyszerű szolgáltatók, gazdasági társaságok ellen, amelyek felvetik a kiberhadviselés kezelésének nemzetközi jogi kérdéseit. 2007-től 2022-ig a technikai kérdéseken kívül a jogi, nemzetközi jogi háttér tisztázása lenne a fő feladata nemcsak a kutatóknak, de az ezt gyakorlóknak is. Mind a NATO, mind az Európai Unió államai és az államok jelentős része a nemzetközi jogot alkalmazhatónak és alkalmazandónak tartja a kiberműveletekre, ugyanakkor ez meglehetősen nehézkes, mert az esetek döntő többségében nem nagyon tudjuk megmondani, hogy ki a támadó egyáltalán. Sok esetben – érdekes módon – nem tudjuk a támadás tényét sem, hiszen nagyon sokára jutunk birtokába az erre utaló információknak. Ilyen támadások például az APT (advanced persistance threats – rendkívül tartós fenyegetések) támadások, amelyek nagyon sokáig fennálló támadások, egyben különböző támadási formák, és fő céljuk az

információszerzés. Nyilvánvalóan ebben benne lehet az információszerzés, de akár a rombolás, a kritikus infrastruktúra pusztítása, és nagyon sok minden más is. Az igazi probléma az, hogy nem mindig tudjuk magát a támadás tényét detektálni, vagy csak később, annak bekövetkezése után. Sok esetben az a kérdés is felmerül, hogy meg tudjuk-e, meg merjük-e nevezni a támadókat. Ezt nevezzük attribúciónak. Sok esetben már a technikai attribúció sem teljes, hiszen nem mindig lehet 100%-osan megmondani, hogy ki a támadó. Ezt nagyon sok esetben több éves technikai bizonyító munkával lehet csak megtenni, ezért nehéz teljes bizonyossággal kijelenteni például, hogy 2007-ben Oroszország támadta meg Észtországot, hiszen nagyon sok helyről érkeztek a támadások. A másik attribúciós feltétel, hogy politikai szempontokat figyelembe véve lehetséges-e a támadók politikai megjelölése, beazonosítása, érdekünkben áll-e kinyilvánítani, hogy ők a támadók, akik egyébként gazdasági, politikai vagy más módon befolyást gyakorolhatnak az adott országra. Ez bármilyen ország esetében igaz, nagyon sok ország nem is használja az attribúciót, még akkor sem, ha az EU kiberdiplomáciai eszköztára felsorolja az attribúciót mint lehetséges eszközt. Az attribúció lényege, hogy ha megvannak a technikai bizonyítékaink, akkor jelenítsük meg, nevezzük meg a támadót abban az esetben, ha ez politikai értelemben nem jelent konfrontációt az adott országgal szemben. A szabályozott lehetőség ellenére sem él ezzel minden ország.

Összefoglalva a kiberhadviselés rendkívül komplex tevékenységeket takar, a közéletben ismert kibertámadások ennek csak egy része. Ráadásul a kiberhadviselés nagyon sokszor összefügg a hibrid hadviseléssel, hiszen a hibrid műveletek, hagyományos katonai műveletek, kiegészítve kiberműveletekkel és egyéb más műveletekkel (például média műveletekkel), amelyeknek célja a befolyásolás akár politikai, akár kulturális területen, nagyon régóta, közel tíz éve a mindennapjaink része. Érdekes megfigyelni, hogy egy fizikai konfliktussal, egy háborúval párhuzamosan nem szűnnek meg a kiberműveletek, tovább folynak, s felerősíthetik az egyes fizikai műveletek, katonai konfliktusok egyes eredményeit, vagy hozzájárulhatnak az ottlévő előnyökhöz, hátrányokhoz.

Milyen választ adtak az országok a jelenségre és milyen gyorsan reagáltak rá?

Általánosságban elmondható, hogy az országok lassan reagáltak. Az elmúlt néhány évben azonban mindenki felébredt, mindenki rájött, hogy a kiberhadviselés egy valós veszély, ugyanakkor egy valós képesség és egy valós lehetőség is egyben. A nyugati országok jelentős része építi azokat az erőket, kibererőket, amelyekkel kiberhadviselésre alkalmas műveleteket tudnak végrehajtani. Nyilván az olyan országok, mint az Egyesült Királyság, Franciaország, Németország

vagy Izrael – 2010–2011 óta – hatalmas lendülettel építik ezen képességeiket. A NATO szövetségi szinten is keresi a választ a kiberhadviselésre. Ennek több megnyilvánulása van. Erre a legjobb példa a tallini Kiberkiválósági Központ 2008-as felállítása, amely kutatásokkal, tanácsadással, doktrína-kidolgozással, minden kiberhadviselési aspektust körüljáró tevékenységével rendkívüli mértékben hozzájárul ahhoz, hogy az országok felépítsék saját képességeiket. Több mint húsz ország vesz részt a központ munkájában. Ettől függetlenül a NATO számos felső és középszintű szervezetet hozott létre, amelyek a kiberműveletek, a kibertér biztonságát hivatottak javítani, illetve felépíteni. A NATO-nak nincsenek kibertámadó képességei, a tagországoknak vannak, de politikai szinten működik az a szervezet, amely összefogja, menedzseli a kibertérbeli tevékenységeket. A szövetség stratégiát alkotott a kibervédelemre, védelmi célú szövetségként egy olyan doktrínát is kiadott 2020-ban, amely hatékonyan szolgálja a tagországok felkészülését a kiberműveletekre. A tagországok építik a saját képességeiket, és ezek összességében hozzájárulnak a NATO kiberbiztonságához, ebből következően egységes elvek mentén kell építkezni. Az egyes ország felajánlja a saját képességét a szövetségnek. Németország például indirekt módon ajánlotta fel kiberképességeit a NATO-nak. Az országok eltérő szervezeteket építenek, melyek fejlődésük során egyre több hasonlóságot mutatnak mind technikai, mind humánerőforrás, mind a kutatásfejlesztés, mind a jogi háttér megteremtése terén. A NATO-tagországok viszonylag egységes elvek mentén építkeznek, természetesen mindenki a saját nemzeti érdekei, hadserege saját szabályzóinak megfelelően. Nem mindenki a hadseregen belül képzeli el a kibererőket. Vannak országok, ahol például a belügyi tárcához tartozó nemzetbiztonsági szolgálatok égisze alatt működnek. Ugyanakkor látszik, hogy minden ország ráeszmélt arra, hogy ez egy nagyon fontos terület nemcsak katonai, hanem politikai, gazdasági téren is. A mi oldalunkról hatalmas védekezési potenciál jön létre, amellyel befolyásolni lehet akár egy másik országot. Az egyes államok esélyegyenlőségét tekintve elmondható, hogy az anyagi feltételek csak egy részét jelentik ennek a területnek. Óriási előny, hogy Magyarország a NATO és az Európai Unió tagjai is, így ugyanis ezek az esélyek javarészt kiegyenlítődnek. Nyilván nem tudunk akkora gazdasági potenciált a kibervédelem és a kiberműveletek fejlesztése mögé tenni, mint például az Egyesült Államok, az Egyesült Királyság vagy Németország, de a NATO-n és az EU-n keresztül hozzáférünk az eljárásokhoz, képzésekhez, a kutatásfejlesztés eredményeihez. Az EU-nak sok közös kutatásfejlesztési programja van, így a tagállamok egy szintre kerülhetnek. Az anyagi erőforrások nem egyenlők, de nem minden a technika, tudniillik a jól képzett humánerőforrás az egyik kulcskérdés. Ez lehet, hogy unalmasan hangzik, de nem tizenéves hackerek

háborúznak a kibertérben, hanem több évtizedes tapasztalattal rendelkező komoly szakemberek, akik nem ad hoc módon tanultak, hanem nagyon sok szakmai tapasztalattal, egyetemi végzettséggel rendelkeznek. Ennek létezik az intézményi háttere, amely megadja az ő további felkészítésük ívét, vonalát, hiszen itt már specialistákról beszélünk, akár kiberfelderítésről, akár veszélyek felismeréséről, akár valamely forenzikus tevékenységről vagy akár a támadó képességek kialakításáról legyen szó. Egy szakértő 45-50 éves korára jut annak a tudásnak a birtokába, amellyel kiberműveletet tud végrehajtani úgy, hogy ezt megelőzően 20-25 évet ebben a szakmában töltött különböző tevékenységeket végezve. A humánerőforrás építése tart a legtovább. Az ebbe való befektetés nem biztos, hogy ugyanannyi erőforrást igényel, mint a technikai fejlesztés, de persze ez is pénzbe kerül. Óriási felelőssége van az adott ország egységének abban, hogy milyen akadémiai, kutatásfejlesztési kapacitással, kis- és közepes vállalkozói kapacitással rendelkezik, olyanokkal, akik tudnak és hajlandók is együttműködni a humánerőforrás fejlesztésében. Ugyanakkor a humánerőforrással kapcsolatosan nem lehet eltagadni azt a tényt, hogy a versenyszféra nyilvánvalóan több pénzt, azaz fizetést tud biztosítani, mint a közszféra, de nem minden a fizetés, sok szakember a kihívás miatt kevesebb fizetésért is kész a hazáját szolgálni.

Van-e jelentősége a felnővő generáció gyakoribb számítógépes játékkokal kapcsolatos szokásainak a potenciális utánpótlás tekintetében?

Személyes tapasztalatom szerint ez nem számottevő. A számítógépes játékok egyfajta készséget, sok esetben zseniális készségeket alakítanak ki, és nehéz is lenne sok készség tekintetében felvenni ezekkel a fiatalokkal a versenyt, de a játékokban szerzett gyakorlat nem jelenti azt, hogy ezeknek a srácoknak a gondolkodása vagy kibertechnikai tudása kiugróan magas lenne. Vissza kell nyúlni ugyanis a mérnöki, műszaki képzésekig, történelmi képzésekig, a gondolkodni tanításig. Nem csak technikai szakembereket képzünk, a mi kollégáink szaktudása a matematika, a fizika, a programozás, az infotechnológia területén is kiemelkedő kell legyen, mert ez a feltétele a hosszú szakmai tapasztalat kialakulásának.

Szakembereink nagy hányada elemző, akik trendeket elemeznek, sok nyelvet beszélnek. Két-három nyelv ismerete sokszor alapfeltétel. A kollégák biztonságpolitikai ismeretekkel, történelmi, eltérő kultúrák ismeretével rendelkeznek. Ezért is igyekszünk az információs műveleteket összevonni egy helyre, egy szervezetbe a kiberműveleteket végzőkkel, mert ez a kettő terület együtt adja azt, hogy olyan képességeink legyenek, amelyek valódi védelmet vagy akár a későbbiekben támadóképességet jelentenek. Összefoglalva: nagyon masszív

matek, fizika, villamosságtan, programozás, infotechnológia ismerettel rendelkező mérnökökre van szükség, de senki nem lehet polihisztor, mert olyan sok területet kell felölelni, amire egy ember biztosan nem képes. Nagyon sok alapismeret után az egyetemek specialistákat képeznek a hálózati, szoftveres mérnökön át a biztonságmérnökig sok különböző területre. Emellett nagyon sokszor kellenek az elemzőképességek, amelyekről már beszéltem. Itt viszont a stratégiai játékok jelenthetnek olyan hozzáadott értéket, amely nem a mérnöki precizitásban, hanem egy kicsit a társadalomtudományok oldaláról megközelített kreativitásban jelentkezhetnek. Hagyjuk játszani a gyerekeket, de el kell mondani nekik, hogy ne féljenek a matektól, mert a matek ugyanolyan gondolkodást, kreativitást tanít, mint egyébként a problémamegoldás a későbbiekben vagy az arra való felkészítés, még akkor is, hogyha ezeket szoftverek tervezésére vagy védelmi eljárás tervezésére fogják használni. Elengedhetetlen, hogy mind a természettudományok, mind a társadalomtudományok olyan képzést nyújtsanak már az általános és középiskolában, amelyre tudunk építeni. Közhelynek számít, de enélkül nehéz elképzelni akár egy rendőrt, akár civilt, akár egy katonát, aki ezen a területen szeretne dolgozni.

Hogyan állunk Magyarországon a kiberbiztonság területét illetően?

Hazánkban a kiberbiztonság jó állapotban van. Bátran merem mondani, hogy bár 100%-os kiberbiztonságról soha nem merünk beszélni, ilyet senki sem tud biztosítani, de országunkban ez egy nagyon jól szabályozott terület. Magyarország 2013-ban – az Európai Unióban elsők között – alkotta meg Nemzeti Kiberbiztonsági Stratégiáját. A jogszabályi háttér is rendelkezésre áll, hiszen 2013-tól az illetékes szervezetek java egyrészt a Belügyminisztérium fennhatósága alatt felel a 2013. évi L. törvény (az állami és önkormányzati szervek elektronikus információbiztonságáról) betartásáért. Mindemellett a honvédelmi ágazatban a kiberbiztonságért és kiberműveletekért felelős szervezetek is közreműködnek, ezen szervezetek együtt felelősek a területért, és nyugodt szívvel mondhatjuk, hogy az együttműködés remek. 2021-ben felgyorsult a Nemzeti Kiberbiztonsági Koordinációs Tanács munkája, és a tanács elkezdett egy új kiberbiztonsági stratégiát megfogalmazni, amely nyilván hosszú távon meghatározhatja Magyarország még magasabb szintű kiberbiztonságát. Az egyetemi képzések nagyon fontosak, az, hogy a Nemzeti Közszolgálati Egyetemen van kiberbiztonsági mesterképzés unikumnak számít az Európai Unióban. Más egyetemeken is folyik hasonló, mint például az Óbudai Egyetemen is előremutató oktatás- és kutatásfejlesztés zajlik, másfél évtizede működnek kutatóintézetek, műhelyek, és ezek világszínvonalúak. Ezen kívül vannak azok a kis- és középvállalkozások,

amelyek Magyarországon a kiberbiztonság különböző területeit fedik le, ezek együttműködése egyre jobb. Egy ilyen kis ország esetében nem is működhet másként, csak úgy, ha a közigazgatás, az akadémiai szféra és a gazdasági szféra együttműködik. Az egyik motorja ennek a nemzeti kiberbiztonsági koordinációs tanács. A tanács mellett nagyon fontos, hogy hazánkban kiberkoordinátor működik, akinek pont az a feladata, hogy ezeket az együttműködéseket segítse. Összefoglalva: Magyarországon jó a kiberbiztonság, de sosem lehetünk nyugodtak, kiberbiztonsági képességeinket tovább kell fejleszteni, és harmonizálni kell az EU és NATO képességeivel és céljaival.

Milyen hazánk kritikus infrastruktúráinak kiberbiztonsága? Mennyire biztonságtudatosak az átlagemberek, a gazdasági élet szereplői?

A fentiek elmondhatók a kritikus infrastruktúrák védelméről is. Megfelelő szintű, de nem lehetünk 100%-os biztonságban. Itt is megvan a jogszabályi háttér, megvannak a felkészült szakemberek, akik nemcsak az adott infrastruktúra üzemeltetői, hanem azok a szervezetek is, amelyek felelősek a kritikus infrastruktúrákon belüli kiberbiztonságért, mint például a Nemzeti Kibervédelmi Intézet. Itt az együttműködés a különböző ágazatokon belül nagyon jó, abból is lehet erre következtetni, hogy óriási kritikus infrastruktúra leállások nincsenek, kiegyensúlyozottan működnek, mondhatni stabilan működik minden ágazat. A 2012-ben megszületett kritikus infrastruktúra törvény (2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről) dinamikusan fejlődik. A 2018-ban születetett nemzeti hálózati- és információbiztonsági stratégia összhangban van az Európai Unió hálózat és információbiztonsági stratégiájával. A kormány és az érintett szereplők komplex módon kezelik a területet. Látni kell, hogy nagyon sok magántulajdonban lévő vállalat érintett, de az összefogás és az együttműködés – véleményem szerint – jól működik. Természetesen további fejlesztések indokoltak, mert egyre korszerűbb és újabb elemekkel bővül az infrastruktúra, az IoT (Internet of Things, azaz dolgok internete) eszközök megjelenése elengedhetetlen. A régebbi rendszerek újabb rendszerekkel való összeköttetése kritikus kockázatot rejthet magában, továbbá a jogszabályi háttér fejlesztésére is szükség van. Nem felejthetjük, hogy a kiberműveletek célpontjai pont a kritikus infrastruktúrák lesznek.

A biztonságtudatosság egyre inkább megfelelő szintű. Ez a mi felelősségünk is. Ebben a munkában az oktatók, munkatársak kiemelkedő jelentőségű feladattal bírnak. Az általános iskolákban, vagy inkább még korábban, már az óvodában a pedagógusokat fel kell készíteni a legalapvetőbb kérdésekre, megtanítani a saját, személyes infokommunikációs eszközük használatára, amelybe

beletartozik többek között a közösségi médiához való biztonságos hozzáférés elsajátítása is. Minden a tudatos felkészítésen múlik. Bár óriási előrelépés figyelhető meg ezen a területen is, sok szervezet tevékenykedik a területen, de ezek nem minden esetben jelentenek összehangolt tevékenységet. Egyre nagyobb azon szervezetek száma, amelyek tevékenységükkel egyirányba mutatnak. A közoktatásból még részben hiányzik ez a fajta biztonságtudatosítás, ezért elengedhetetlen bevinni oda, ugyanis saját elemi érdekünk a gyerekek felkészítése. A fiatalabb generációval egyidőben a társadalom idősebb részére is fókuszálni kell. A fejlesztők továbbképzése is elengedhetetlen, sok szoftvereket, hardvereket fejlesztő cég van a piacon, az ő biztonságtudatosításuk is nélkülözhetetlen. Ez utóbbira megvannak az eljárások, nemzetközi ajánlások, élő nemzetközi kapcsolatok azokkal, akik ezt hivatásszerűen végzik. A gazdasági élet szereplői előrébb járnak, de elég vegyes a kép. A nagyvállalatok nagyobb erőforrással, szervezeti kultúrával rendelkeznek, ehhez képest a kis- és középvállalkozások kicsit le vannak maradva. Sokan nincsenek tudatában, hogy ez milyen jelentős kérdés. Érdekes módon a közigazgatás előrébb jár, mert törvényi kötelezettség a kötelező jellegű továbbképzés minden állami szervnek, minden intézménynek van elektronikus információbiztonsági vezetője, akinek törvényi kötelezettség révén iskolaszerű továbbképzésen kell részt venni. Ez a Nemzeti Közszolgálati Egyetemen akkreditált képzéseket jelent, amelyek egy része e-learning formában is könnyen elérhető. A közigazgatás területét, a gazdasági szférát és az állampolgárok biztonságtudatosítását össze kell kapcsolni. Meg kell értetni mindenkivel, hogy ez miért fontos.

Evidencia, hogy a gyerekeknek a közlekedési szabályokat elmondjuk, a biztonságos közlekedést elvárjuk tőlük, azonban az okoseszközök használata esetén ez bizony sokszor elmarad, pedig nagyon korán el kell kezdeni, kötelező jelleggel felépíteni a prevenciós tájékoztató rendszert, s fel kell hívni a veszélyekre a figyelmet, akár már az általános iskola második, harmadik osztályában. Ebben a korban már felfogják, tudják például, hogy mi az a bullying. A gyerekeknek tisztában kell lenniük azzal, hogy lehet ezeket elkerülni, vagy kinek kell jelezni, ha észlelnek, tapasztalnak hasonlót. Amikor a telefon a kezében, azzal a zsebében a világ, de akkor is csak egy magányos kisgyerek, szüksége van a felvilágosításra és adott esetben a segítségre ezen a területen is. Az információforrás elsősorban a család és az iskola. Az iskola esetében a pedagógusok szerepe is komolyan felmerül. Amikor bekövetkezik egy incidens meg kell vizsgálni az összes körülményt, amelynek során általában több probléma kerül felszínre. Szülőként azonban a mi felelősségünk, hogy mekkora szabadságot biztosítunk a gyerekeinknek a kibertérben. Ennek ellenőrzésében vagy felügyeletében kell az egészséges egyensúlyt megtalálni. A kiskorú gyerek internetes

tevékenységének ellenőrzése, annak megbeszélése bűncselekményeket előzhet meg. A gyerek érzelmi stabilitását lehet javítani, ha tudja, hogy a szülőben megbízhat. Lehetséges megoldás az egyéb alternatíva, az értelmes elfoglaltság biztosítása. Az internet világa magányosabbá teszi a gyerekeket, felbátorítja a bántalmazásra az arra hajlamosakat. Rendkívül sok behatás éri a gyerekeket, ezért a legfontosabb a bizalmi kapcsolat fenntartása ebben a tekintetben is.

Hogyan építik be a vonatkozó ismeretanyagot a honvédtisztképzésbe? Mennyire felkészültek a hallgatók a témát illetően?

A hadtudományi karon régóta végzünk kutatásokat, fejlesztéseket a témát illetően. Ezeknek a kutatási projekteknek az eredményei megjelennek az alap- és mesterképzésben. Van védelmi infokommunikációs rendszertervező mesterszakunk is, amely információbiztonsági specializációt is tartalmaz. Az említett eredmények az alapképzésbe is beépülnek, minden honvédtiszt rendelkezik kiberbiztonsági, elektronikai hadviselési, információs műveleti ismeretekkel, de persze ez nem korlátozódik csak a honvédtisztképzésre. Az NKE Nemzetbiztonsági Intézet képzéseiben ugyanígy megjelennek ezek az ismeretek. A biztonságtudatosítás nemcsak az oktatás során, hanem különböző publikációkban, médiamegjelenésben, workshopokban is megjelenik. A szakkollégiumok rendezvényein rendszeresen van ilyen tagozat. Az utóbbi időben felpezsdült egyetemi közélet is kimondottan hozzájárul a hagyományos értelemben vett oktatáshoz, az ismeretek átadásához. A szabadegyetemi előadások mind jóval széleseb kört érnek el. Azt is látni kell, hogy egyre több hallgatót érdekel a téma. Végtelenül nagy öröm, amikor egy-egy előadás után érdeklődnek a hallgatók soraiból, hogy milyen munkalehetőségek vannak a Magyar Honvédségben a kibervédelem területén.

Kijelenthető, hogy a világon jelenleg van olyan hibrid fenyegetettség, amely több összetevős és a kibertérben is intenzíven zajlik?

Igen, de ez nem újkeletű dolog, elég régóta jelenlévő kérdés. Ha leegyszerűsítjük, akkor a hibrid fenyegetésekről, illetve a hibrid műveletekről elmondható, hogy ezek többtényezős hagyományos katonai és nem katonai eszközöket, tevékenységeket magába foglaló, a háborús küszöb alatt tartandó konfliktus és annak műveleteinek végrehajtását jelenti. A hibrid műveleteknek az egyik legfontosabb dimenziója a kibertér, ahol sokszor sokáig nem is tudjuk, hogy ki az elkövető, csak feltételezések vannak. A hibridtámadás nem ad hoc módon létrejött műveletek összessége, hanem előre jól megtervezett cél vagy célok érdekében tervszerűen felépített műveletek együttese. Mindezek egyik legfontosabb

jellemzője sokáig az volt, hogy a fegyveres konfliktus szintjét még ne érjék el, de gazdasági, politikai, kulturális befolyást gyakoroljanak. Ennek megfelelően a hibrid műveletek végrehajtói valamilyen befolyást akarnak elérni. Ugyanakkor a háború kitörésével, az ott zajló események alapos, tudományos igényű vizsgálatával a fenti – hibrid műveletekre vonatkozó – kitételek is változhatnak.

A cikkben található online hivatkozás

URL1: *Net(védelem) nélkül semmi sincs*. https://www.uni-nke.hu/hirek/2022/03/09/netvedelem-nelkul-semmi-sincs

A cikk APA szabály szerinti hivatkozása

Hertelendi L. & Hornyik Zs. (2022). „A kiberbiztonság jelentősége a mindennapokban". Interjú Kovács László dandártábornokkal, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Karának egyetemi tanárával. *Belügyi Szemle*, *70*(6), 1327–1337. https://doi.org/10.38146/BSZ.2022.6.11