HADMÉRNÖK

XIII. Évfolyam „KÖFOP” szám – 2018. január

AJÁNLÁS TTX GYAKORLATOK SZERVEZÉSÉHEZ

RECOMMENDATIONS FOR DESIGNING TABLE TOP EXERCISES (TTX)

SZABÓ András

(ORCID: 0000-0002-8750-8557)

szabo.andras@uni-nke.hu

Absztrakt

A 2016 évi Varsói NATO csúcson katonai műveleti területnek definiálták a kiberteret. Ennek következtében egyre nagyobb szükség van, a kibertérben zajló eseményeket átlátó, azokra reagálni tudó szakemberekre. A kiberbiztonság számos mérnöki, és nem mérnöki tudományterületet ölel át. Ez a tagoltság sokszor a szakemberek közös munkavégzését nehezíti. Az egyéni ismeretek megszerzése mellett, a szakembereknek szükségük van a közös munkavégzésre való felkészítésre is. Az összekovácsolás érdekében döntéshozatali gyakorlatokat (un. Table Top Exercise - TTX) lehet szervezni. Az ilyen típusú gyakorlatok szervezéséhez nyújt segítséget jelen cikk, bemutatva a nemzetközi trendeket, a követendő példákat.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Ludovika Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: *Kibervédelem, oktatás, gyakorlat, TTX*

Abstract

During the Warsaw Summit in 2016, NATO defined cyberspace as an operational domain. For this reason, there is an increased need for experts who are capable of understanding events in the cyberspace. Cyber security interconnects different subject matter experts, from engineering to social science. The interdisciplinary nature of this topic has an impact on the communication and cooperation between different fields.

Beside the technological skills on the individual level, experts need to learn how to work as a team. The so called tabletop exercises (~TTX) can be used for learning teamwork and other essential skills in the field of cyber security. This article presents the trends in the field of cyber education, focusing on the before mentioned tabletop exercises, and also try to help the organizer's of such an event by showing them the international trends.

The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance” in the Ludovika Workshop.

Keywords: *Cybersecurity, education, Tabletop exercise, TTX*

A kézirat benyújtásának dátuma (Date of the submission): 2017.09.30.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.10.09.

BEVEZETÉS

A hadviselés történetében a nagy áttöréseket az újszerű, ezáltal a másik fél által ismeretlen technológiák és taktikák szokatlan alkalmazása hozta. Hannibál előnyre tett szert, mert nem várt irányból, szokatlan harcmodorral támadott a Római birodalomra. Nagy Sándor első sikereit a kor szokványos görög hadviselésétől való eltérése eredményezte. A középkorban a nehéz páncélzatú keresztény seregek Szentföldön elszenvedett vereségeihez a könnyűlovas, íjász arab harcmodor vezetett. Napóleon lovasságának vesztét a sakktáblaszerű alakzatban felálló gyalogság okozta. Az I. Világháborúban a Somme folyónál a harckocsi, az yperni csata során a mustárgáz [1], mint az addig nem ismert technológia törte meg az ellenállást. A II. Világháború kezdetén a németek által alkalmazott 'Bliztkrieg' dinamizmusa a szövetséges hatalmak katonai stratégáinak "állóháború" paradigmáját döntötte meg.

A XXI. században a technológiai fejlődés hatalmas lendületet vett, a haditechnikai eszközök életciklusa ennek következtében az n*10 évről n*1 évre csökkent (a kibertérben pedig egy-egy védelmi mechanizmus hatékonysága sokszor csupán néhány hónapig tart). Így az újszerű megoldások megismerése, a technológiakövetés nélkülözhetetlenné vált napjainkban a kiberbiztonsággal foglalkozó szakemberek számára. Pusztán a legfejlettebb technológiák használata azonban nem elégséges, fel kell ismerni, hogy azokat az alkalmazó szervezet saját céljaira (pl.: egy katonai művelet támogatása érdekében) hogyan tudja leghatásosabban hasznosítani. Épp ezért vált fontossá a technológiák kifejlesztése mellett az alkalmazandó taktikák és módszerek tesztelése, az állomány felkészítése és tudásának naprakészen tartása.

A katonai felkészítésben évezredek óta használnak különféle hadijátékokat a taktikák és stratégiák kidolgozására, azok végrehajtásának begyakorlására, továbbá a parancsnokok vezetői képességeinek javítására, és a csapatok hadrafoghatóságának ellenőrzésére. Ezek a gyakorlatok a korábban elsajátított elméleti ismeretekre építenek, és a gyakorlat tervezése során előre definiált célok elérése érdekében váratlan kihívások elé állítják a résztvevőket. Jellemzően nem az egyéni kvalitásokat ellenőrzik, hanem a közösségben végzett tevékenységet. A gyakorlatok során fontos a tervezettség, annak érdekében, hogy a gyakorlat szervezői és végrehajtói számára végig egyértelműek legyenek az elérendő célok, és az elsajátítandó képességek. Ugyancsak fontos, hogy a gyakorlat során végzett munka eredményessége mérhető legyen, ezzel is elősegítve a gyakorlat-, és az azon résztvevők értékelését.

A 2016 évi Varsói NATO csúcson különálló katonai műveleti területnek definiálták a kiberteret. Sokan ebben az új dimenzióban a szárazföldi-tengeri-légi hadviselés paradigmáit akarják alkalmazni (pl.: szőnyegbombázás analógiája [2], vagy az elrettentés taktikája [3]), viszont ezek ebben a dimenzióban nem, vagy kis hatásfokkal alkalmazhatóak. Vannak azonban olyan felkészült nemzetek is, akik mind taktikai szinten (pl.: APT[1] támadások, nagy volumenű DDoS[2] támadások), mind stratégiai szinten (információs műveletek támogatása kiberhadviselési módszerekkel) komoly felkészültségről tettek tanúbizonyságot.

Ezek alapján fontossá vált a kibertér és a kapcsolódó területek (közbiztonság, nemzetbiztonság, honvédelem) összefüggéseinek megállapítása (jellemzően ezzel a kutatási feladattal a nemzetek védelmi kutatóintézeteket bíztak meg). Az összefüggések felismerése azonban önmagában nem elegendő, azokat a nemzetek kormányzati és gazdasági szervezeteinek védelmébe bele is kell építeni. Ez pedig képzést és oktatást igényel.

1 APT, Advanced Persistent Threat, hosszú lappangási idejű, professzionálisan kidolgozott, célzott támadás
2 DDoS, Distributed Denial of Service, Elosztott szolgáltatás megtagadás alapú támadás

A KIBERBIZTONSÁG OKTATÁSÁNAK KORSZERŰ MÓDSZEREI

Az oktatás tervezése egy folyamat, melynek során először meghatározzuk az elérendő képességeket, majd annak eléréséhez kiválasztjuk az ideális módszer(eke)t. Az ismeretek nagy része elméleti, melyet online tananyag, előadások, vagy szeminárium formájában lehet a leghatékonyabban átadni. Törekedni kell, hogy az elméleti ismeretek a gyakorlatban alkalmazhatóak, a későbbiekben hasznosak legyenek, illetve azok különböző gyakorlati foglalkozások során elmélyítésre is kerüljenek. Az ilyen jellegű oktatásnak a technológia ismeretek átadása mellett másik szerepe a kommunikációs készség fejlesztése lehet. Ezt jellemzően csoportos feladatok megoldásával, és a tanulók egyéni felkészülését követő, őáltaluk tartott szóbeli előadásokkal lehet elősegíteni.

Az oktatási módszerek és technikák sokat fejlődtek az elmúlt évtizedekben, elsősorban az technológiai innovációnak köszönhetően. Manapság lehetőségünk van online, un. MOOC (*Massive Open Online Courses*[3]) kurzusokon részt venni, melyeknél testre tudjuk szabni, hogy mikor[4], és milyen ütemben tudunk az anyaggal foglalkozni. A NATO [4] [5] is felismerte ezt a lehetőséget, és egyre nagyobb mértékben kívánja kiváltani ezzel a klasszikus tantermi foglalkozásokat, hiszen így gyorsabb és rugalmasabb, az igényeknek jobban megfelelő kurzusokat tudnak kialakítani (például, ha szükséges, akkor akár a műveleti területen szolgálatot teljesítőket készíthetik fel az új típusú fenyegetésekre vonatkozóan egy-egy kurzus segítségével). Az online tananyagok jellemzően az egyéni tanulásra koncentrálnak, sokszor lehetőséget adnak, hogy a felmerülő kérdéseiket az oktatókhoz eljutassák a résztvevők, de az oktatásnak nincs kommunikációs készségfejlesztő, vagy közösségformáló szerepe[5]. Ezeket tehát más módszerekkel kell megoldani.

Az ismeretek elsajátításának mértékét különböző módon tudjuk mérni. A praktikusság egyik legjobb mércéje pedig ha "csináljuk is" (használjuk az elsajátítottokat). Ennek pedig egyik, de nem egyetlen módja a gyakorlatok szervezése.

A kibertérben végzett gyakorlatok lehetnek technikai jellegűek (pl.:*Red/Blue teamgyakorlatok*[6]*,Capture The Flag*[7] *versenyek*) és nem technikai fókuszúak (pl.: vezetési törzsgyakorlatok, TTX-ek). A technikai gyakorlatok nemzetközi trendjeiről egy későbbi cikkemben értekezek részletesen.

Tudományterület-, és témafüggő, hogy a képzésben milyen az ideális arány az elmélet és gyakorlat foglalkozások között. Célszerű megvizsgálni, hogy megfelelő-e az arány ezek között, illetve, hogy egyenletesen kell-e elosztani azokat (pl. sokszor érdemes a tananyag főbb elméleti szakaszaihoz hozzákapcsolni egy-egy gyakorlati példát, esetleg a tudás elsajátítását elősegítheti önálló feladatok megoldása).

---

3 Pl. Az alábbi weblapon: https://www.mooc-list.com/

4 Pl. a klasszikus iskolai oktatás nem veszi figyelembe, hogy a hallgatók figyelme a fáradság, éhség, vagy jóllakottság, stb. okok miatt ingadozik a nap folyamán.

5 Nem valószínű, hogy a 2017-ben online tanulmányokat folytatók, 2027-ben e-osztálytalálkozót szervezzenek

6 Red/blue team gyakorlatok során a résztvevők két eltérő feladatú csapatot alkotnak: a védőket (blue team), és a támadókat (red team). A cél függvényében ezek a csapatok a gyakorlat során maradnak ennél a szerepnél, vagy akár váltogathatják is egymás közt. Vannak olyan gyakorlatok, melyeknél a résztvevőknek egyszerre kell védekezniük, és támadniuk is. Illetve több blue team és/vagy több red team is részt vehet, eltérő céllal, és feladatkörrel.

7 A Capture the flag, vagy más néven CTF versenyek célja, hogy a résztvevőknek IT biztonsági feladványokat kell megoldaniuk, jellemzően nem a szokványos gondolkodást követve. A résztvevők sokszor egymást is támadhatják, illetve mások munkáját ellehetetlenítve juthatnak előnyhöz. A "think out of box" mentalitást követve sokszor a pontozó rendszert támadják, és így próbálnak előnyre szert tenni...

1. ábra Példa az elméleti és gyakorlati oktatás arányára (saját szerkesztés)

A fent vázolt példában egy variációt láthatunk az oktatási ciklus arányaira (Lásd: 1. Ábra). Ennek során haladunk az egyéni ismeretek és képességek elsajátításától a csapatmunka, a közös problémamegoldás felé. Az oktatás témája, és a rendelkezésre álló idő függvényében az oktatás lezárásaként, vagy akár az egyes elméleti blokkok közé is szervezhetünk a tanulócsoport számára közös gyakorlatokat.

Felmerülhet a kérdés: *Miért is szervezzünk gyakorlatokat?* Több célja is lehet egy csoportos gyakorlatnak, melyeket az alábbiakban gyűjtöttem össze:

- Biztonságtechnika [9, 20.§ (1)-(3)]
- az egyének kollektív munkavégzésének, a csapatmunkának az értékelése (a gyakorlat szervezői, vagy a szervezet szempontjából),
- figyelemfelhívás (az egyének szempontjából a hiányosságok azonosítása),
- oktatás, új ismeretek átadása alternatív módszerekkel (elsősorban a csapatmunkával és a kommunikációval kapcsolatos ismeretek),
- új védelmi módszerek és eljárások kidolgozása és tesztelése[8].

A célokat nagyban meghatározza a célközönség, az ő előképzettségük, szakmai ismereteik. Ugyancsak determinálja a gyakorlatot a felkészülésre és végrehajtásra szánt idő. Egyrészt a szervezők, másrészt a résztvevők idejével is gazdálkodni kell, hiszen értelmét veszi a szervezők hosszas felkészülése, aprólékos háttér információk kidolgozása, ha a végrehajtás során a résztvevőknek nincs ideje azokat alaposan áttanulmányozni. A gyakorlatokra a valós világ eseményeinek modellezéseképpen is tekinthetünk, és itt is igaz, hogy a részletgazdagságra, és valósághűségre addig kell törekedni, amilyen mértékig az befolyásolja a gyakorlatban hozott döntéseket.

A nem technikai jellegű kiberbiztonsági gyakorlatok

Az Egyesült Államok szabványügyi hivatalának (NIST [6]) definíciója szerint: "*A Tabletop gyakorlatok*[9] *olyan csoportmunkán alapuló megbeszélések, amelyek során az informatikai biztonsági tervekben szereplő felelősségi köröket betöltő személyek egy tantermi környezetben találkoznak, hogy a vészhelyzetek során alkalmazandó lépéseket begyakorolják, a tervek alkalmazhatóságát ellenőrizzék, az esetleges hiányosságokat kijavítsák. A gyakorlatot vezető személy az előre meghatározott célok elérésére érdekében irányítja a megbeszélést."*[10]

Napjainkban ez kiegészült azzal, hogy már nem csak az informatikai biztonsági tervekben szereplő funkcionális munkakörökben dolgozók képzésére alkalmazható, hanem tágabb

8 Az ilyen gyakorlatoknál, már felkészült kiképzett végrehajtókkal teszteltetünk egy új eljárást/eszközt és az értékelés nem a végrehajtók felkészültségére, hanem az új eljárás/eszköz hatékonyságára fókuszál.
9 Tabletop exercise - TTX
10 Forrás: Tim Grance,TamaraNolan, KristinBurke, Rich Dudley, Gregory White, Travis Good - Guideto Test, Training, and ExerciseProgramsfor IT Plans and Capabilities (NIST SpecialPublication 800-84), p. 21. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

értelemben mindenkivel, aki összefüggésbe kerül a kiberbiztonsággal (döntéshozók, felhasználók, üzemeltetők, auditorok stb.).

A biztonság a naprakész védelmi *technológiák*on, az azokat tervező, fejlesztő, üzemeltető és használó *emberek*en, valamint az általuk alkalmazott *procedúrák*on múlik. Ha ezek közül a tényezők közül egy is figyelmen kívül marad, akkor nem lesz teljeskörű a védelem.

Leegyszerűsítve, az oktatás során az emberekkel ismertetjük meg az alkalmazandó technológiákat és procedúrákat.

Ugyan vannak törekvések a minél hatékonyabban működő automatizált védelmi mechanizmusokra (tanuló rendszerek, mesterséges intelligencia, stb.), a közeljövőben még megmarad az emberek központi szerepe ezen a téren.

Garry Kasparov a Defcon 2017 kiberbiztonsági konferencián nyitóbeszédében[7] a közeli 2 évtizede vívott sakkversenyéről, és annak következményeiről beszélt. 1996-ban, majd 1997-ben ismét az IBM DeepBlue szuperszámítógép ellen sakkozott, amelyet az első játszmában ugyan legyőzött, de a későbbiekben vesztett ellene. Elmondta, hogy a DeepBlue nem volt mesterséges intelligencia, csupán egy, az embernél sokkalta gyorsabb számításokra képes gép. Napjainkban sorra jelennek meg a valós, mesterséges intelligenciával bíró rendszerek. Azonban Kasparov felhívta a figyelmet arra, hogy az önállóan döntéseket hozó mesterséges intelligenciát, egy ember-gép páros meg tud verni. Példaként az olyan sakkversenyeket hozta fel, ahol emberek sakkoznak egymással, de minkét fél rendelkezik számítógépes döntéstámogatással[11]. Kasparov a jövőt ezekben, és nem az önállóan döntést hozó gépekben látja.

A hatékony kiberbiztonság sem pusztán az automatizált, esetleg mesterséges intelligenciával támogatott védelmi technológiákkal, hanem az azokat értően használó szakemberekkel valósítható meg.

Szellemes IT biztonsági mondás, hogy *"Az emberi butaságra nincs javítócsomag ("There is no patch for human stupidity"* [8]), ugyanakkor ezzel vitatkozni lehet. Hiszen oktatással és megfelelő HR[12] politikával (jutalmazással és retorzióval) a tudatlanságból vagy hanyagságból bekövetkező biztonsági incidensek száma csökkenthető (lenne).

Fontos, hogy érdekeltté tegyük a szereplőket (rendszergazda, vezető, felhasználó stb.), azért, hogy lássák mi a szerepük a szervezet egészének működésében és a biztonság fenntartásában.

Napjainkban egyre nagyobb teret nyernek az alternatív módszerek, mint például a projekt alapú tanulás (melynél egyénileg vagy kis csoportokban, önállóan végzett feladatok során gyűjtik a tanulók a szükséges háttérismereteket, illetve azokat a projekt célja érdekében egyből alkalmazzák is a gyakorlatban). A másik, az oktatásban elterjedt módszer, a feladatok játékszerűvé tétele (un. "*gamification*"), mely során az ismereteket játékos módszerek segítségével sajátítják el. Az előbb említett módszerek érdekessége, hogy alapvető emberi tulajdonságokat (tudásvágy, szabadságszeretet, kreativitásra való törekvés, játékosság) használnak fel annak érdekében, hogy az ismeretelsajátítás hatékonyabb, és a résztvevők számára élvezetesebb legyen (mivel amit élvezünk, azt nagyobb motivációval is végezzük).

A képzéseknél az életkori sajátosságokat is figyelembe kell venni. Az, ami esetleg évtizedekig hatékonyan működött, azt illeszteni kell az új generációk oktatási kihívásaihoz [9]. Az un. "Z generáció" (a 2000-es évek elején születettek) a felsőoktatás, és a munkavállalás küszöbén áll, számukra az ismeretátadás hatékonyabb ha interaktív, online és testre szabható [10] [11]. A különböző korosztályok közti kommunikációra is oda kell figyelni, hiszen nemcsak a technikai-nem technikai szakemberek közti "fordításra", hanem a generációk közti szakadékok leküzdésére is szükség lehet.

---

11 Ezt a sakk variánst Advanced Chess-nek nevezik.

12 HR (Human resource) - személyügy

Célközönség

A szervezet szintű IT biztonság újszerű megközelítést igényel, mely fókuszba helyezi a humán aspektust, és az alkalmazottak képzése, gyakoroltatása és ellenőrzése révén fokozza a védelmet[12].

Ezek alapján az alábbi csoportoknak szervezhetünk TTX-eket:

- *Informatikusok* (üzemeltetők, fejlesztők) számára például szemléletmód váltás érdekében (sokszor nem látnak túl a technikai problémákon, esetenként pedig javítani kell a kommunikációs képességeiken [13]). Az ilyen gyakorlatok lehetőséget adnak számukra, hogy ne csak technikai-technológiai válaszokat adjanak egy-egy felmerülő biztonsági kihívásra, hanem a szervezet egészére is tekintettel legyenek, szem előtt tartva annak lehetőségeit és érdekeit.
- Az *incidenskezelésben érintettek* csapatmunkája javítása érdekében. Ha a résztvevők nem ismerik egymás képességeit, az alkalmazandó incidens kezelési eljárásokat, nincsenek tisztában a szervezet prioritásaival, akkor nem tudnak egy csapatként dolgozni. Sokszor a munka hatékonyságát kommunikációs, vagy információ-megosztási problémák rontják. A TTX-ek során ezek a problémák a felszínre kerülnek, és a valós incidensek bekövetkezte előtt elháríthatóvá válnak.
- A *vezetők* számára a kibertér, az abban rejlő lehetőségek, és veszélyek ismertetésére is alkalmazható demonstrációs és tudásbővítési céllal (döntési szempontok, hatások és következmények elemzése), valamint az incidenskezelés operatív feladatait elvégző csoporttal való együttműködés, továbbá a vezetői kommunikáció is begyakorolható egy-egy TTX-en.
- A *felhasználók* számára tartott biztonságtudatosító kampány egyik eleme lehet egy felhasználó fókuszú TTX, melyben megismerhetik a fenyegetéseket, bemutathatjuk számukra a biztonságtudatos munkavégzést (megindokoljuk, hogy miért kell a biztonsági kontrollokat betartani). Itt törekedni kell arra, hogy a való életből vett eseteken, esetleg a korábbi rossz felhasználói megszokások iskolapéldáin keresztül mutassuk be a veszélyeket. Az ismeretterjesztésre kell törekedni (a túlzottan mély technikai ismeretek átadása, vagy a szakma specifikus nyelvezet használat ellentétes hatást válhat ki, így az átlag felhasználók esetén a leegyszerűsített magyarázatok hatékonyabbak, mint a részletekbe veszők).

A "*mi történt volna*" szcenáriók interaktív lejátszása növelheti a biztonságtudatosságot, de kérdőíveknél figyelték meg, hogy a kitöltők az "elvárt" helyes válaszokat adták, míg a munkájuk során sokszor nem eszerint cselekedtek.

A TTX gyakorlat az IT biztonsági képzések egyik eleme lehet, de semmiképpen sem varázsszer, mely mindenre megoldást kínál. Inkább egy hatásnövelő (katonai kifejezéssel "*force-multiplier*") eszköz. Kiegészíti, összekapcsolja az elméleti oktatást, a labor feladatokat és a technikai jellegű gyakorlatokat. Összekapcsolhatja a felhasználókat, az informatikusokat és a döntéshozókat, elősegítheti, hogy köztük egységes biztonsági kultúra, és egy közös „nyelv” alakuljon ki.

Oktatásba való integrálás lehetőségei

Ahogy korábban említettem, TTX-eket különböző célból szervezhetünk. A következőekben bemutatom, hogyan lehet a TTX gyakorlatokat felhasználni az oktatásban a tudás átadására, a megszerzett ismeretek elmélyítésére, vagy az elméleti tudás gyakorlati ismeretté történő konvertálására.

Fontos, hogy már a gyakorlat előtt tisztázzuk a résztvevőkkel a leendő feladatukat. Nagy valószínűséggel korábban ilyen jellegű oktatásban nem vettek még részt, ezért hatékony lehet,

ha néhány héttel a gyakorlat előtt kapnak felkészülési anyagokat (pl.: videókat, beszámolókat, stb.), vagy ha látnak hasonlóakat (pl.:megfigyelőként megnézhetnek egy gyakorlatot). Jelen cikk is forrása lehet egy ilyen felkészítő anyagnak, mely elolvasását követően a résztvevők látják a célt, és a gyakorlat során elsajátítandó képességeket.

Ha sikerül ezt a képzési formát a felsőoktatásba integrálni, akkor a BSc, MSc tanulmányokat folytatók a későbbi munkájuk során hasznosíthatják is azt (pl.: gyakorlat szervezése a munkatársaik, vagy a beosztottaik számára).

2015-2017 között a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Üzemeltető Intézet Informatikai tanszéke több alkalommal is tartott a BSc, az MSc oktatásban, illetve az Erasmus képzésben részt vevő hallgatói számára TTX gyakorlatokat.

Ezek az oktatott tantárgyak zárásaként, az átadott tudás összegzéseképpen, illetve az elméleti tudás "hasznosságának" demonstrálásaképpen lettek megszervezve. Ezeknek a tapasztalata volt, hogy jóval aktívabbak a résztvevők, ha a TTX-et egy többlépcsős csapatmunka végén hajtjuk végre (a lépcsőket az 1. Táblázat mutatja be).

A közösen, praktikusan egy asztal körül végzett feladatmegoldás első elemeként egy katonai válságreagáló művelet során bevetett kontingens erőit kell összeállítaniuk a felvázolt környezetben (fikcionált konfliktus, nem létező országok között, megfelelően kidolgozott geopolitikai, gazdasági, katonaföldrajzi háttér-információkkal). A következő feladat a települő erők híradó-informatikai igényeinek felmérése (információvédelmi, logisztikai és elektronikai hadviselési szempontokat is figyelembe véve), majd az informatikai szolgáltatáspalettát kell összeállítaniuk. Ezt követően a várt fenyegetéseket kell azonosítaniuk, és egy vázlatos incidenskezelési tervet kell kidolgozniuk. Végül az eddig közösen dolgozó csoporttagok egyesével kapnak egy "karaktert", aki egy, a művelet szempontjából lényeges pozíciót tölt be az alegységen belül, vagy külső szervezetnél (pl.: internetszolgáltató helpdesk-jén, hírügynökség riportereként, vagy a helyi rendvédelmi szervnél stb.).

Megfelelő létszám esetén az ellenerőt is a résztvevőkből szervezhetjük. Ekkor egy, vagy akár több "Red team" is kialakítható, akik különböző felkészültséggel, erőforrással és motivációval rendelkező támadókat játszanak (pl.: egy nagy létszámú, de alacsony technikai színvonalú hacktivista csoport, két eltérő munkamódszerű kiberbűnöző csoport, és egy államilag támogatott hackercsoport). Utóbbi megléte esetén komplexebb gyakorlatok valósíthatóak meg, és az attribúcióval, háttér információk elemzésével [14] is foglalkozhatnak.

No.	A feladat leírása	Idő	Módszer	A fejlesztett / vizsgált tudás / készség	
0	A játékszabályok, és a háttértörténet ismertetése	10’	Előadás	-	- Kommunikációs készségek & - Csapatmunka & - Katonai műveletek tervezés
1	Erők és eszközök definiálása, CONOP, RoE	20’ - 30’	Brainstorm	Művelet tervezési alapok	
2	Híradó-informatikai igényeinek felmérése - hadműveleti követelmények definiálása - műszaki követelmények definiálása	30’	Brainstorm	- Híradó - informatikai tervezői ismeretek - Kapcsolat a katonai igények és a műszaki megoldások között	
3	Fenyegetések azonosítása	20’	Brainstorm	- Kibertérbeli és fizikai fenyegetések felismerése, - kapcsolat a kiberműveletek és a fizikai térbeli műveletek között	
4	Incidenskezelési terv készítése (vázlatos)	20’	Brainstorm	Incidenskezelési lépések és *preventív*, *detektív* és korrektív kontrollok alkalmazási lehetőségei	
5	TTX	45’-60’	Szerepjáték	- Szerepkörök az incidenskezelésben - Döntési helyzetek a műveletek során - Kommunikáció a szervezeten belül és kívül	

1. táblázat Egy katonai TTX felépítése (saját szerkesztés)

A gyakorlat hangulatát és valósághűségét javíthatja, ha a résztvevők a karakterük munkája mellett néhány pozitív és negatív tulajdonságot is kapnak, amiket bele kell szőniük a játékba. Olyan emberi tulajdonságokat oszthatunk ki, mint például a "munkamániás", a "felületes", a "tudálékos", "a "titkolózó", a "fecsegő" stb. Ezzel kijátszása nagyban függ a csoport élettapasztalatától (Bsc esetén kevésbé, Msc hallgatók esetén általában jól mintázzák, feltételezhetően azért, mert munkájuk során találkoztak már ilyen karakterekkel). Ennek a "szerepjátéknak" a célja a figyelem megosztása is lehet, mivel megfigyeltük, a játékosok a helyzet fokozódásával ezekről a tulajdonságukról megfeledkeznek (mivel kizárólag a felmerülő incidensekre fókuszálnak).

Az instruktoroknak és segítőiknek több dologra is oda kell figyelniük a gyakorlat levezetése során. Az gyakorlat dinamikájára ügyelni kell, és az egyes lépcsőkre, mérföldkövekre szánt idővel jól kell gazdálkodni. Ellenkező esetben elhúzódik a gyakorlat, és a fáradás hatására többen passzivitásba temetkeznek, ezek a résztvevők pedig az egész csoport hangulatát, és produktivitását befolyásolják). A egyes résztvevők bevonása, és az aktivitásuk fenntartása is fontos a gyakorlat során, ugyanis vannak, akik nehezebben oldódnak (kapcsolódnak be a csapatmunkába), és vannak, akik túlságosan is bőbeszédűek, így nem hagyják érvényesülni a csendesebb társaikat. A két típus között kell megtalálni az egyensúlyt. Egy másik figyelmet igénylő jelenség a viták és véleményeltérések lezárása (az indokok és érvek alapján a csoportnak konszenzusra kell jutnia az adott feladatra szánt időkereten belül). Ez a vezető határozottságán múlik. Nem szabad hagyni a „túl szorgalmas”, vagy kötekedő résztvevőket, hogy átvegyék a beszélgetés irányítását.

Az oktatók számára a TTX egy mérési módszer is, egyfajta visszajelzés munkájuk eredményességéről (és a hiányosságokról), hiszen látják, hogy az elméleti ismereteiket milyen mértékben tudják "éles" helyzetekben alkalmazni a hallgatók.

Célszerű az oktatás, és a gyakorlat hatékonyságáról információt gyűjteni a résztvevőktől annak érdekében, hogy a következő TTX szervezettebb, jobb hatásfokú legyen (így azonosítható, ha egy-egy részfeladat célja nem volt egyértelmű, kevés/sok időt szántunk a különböző lépésekre stb.) .

A gyakorlatot követően ugyancsak lehetséges önálló munkaként kiadni számukra egy TTX gyakorlatnak az előkészítését (vagy részterületeknek, pl.: a háttértörténetnek, vagy az egyes eseményeknek a kidolgozását). Azzal, hogy megpróbálnak a látottak alapján újabb szcenáriókat összeállítani, felkészülni egy gyakorlatra, újabb ismereteket szerezhetnek, illetve a meglévőek jobban bevéződnek (természetesen ezeket az önálló munkákat az oktatóknak értékelni, javítani, véleményezni kell, mellyel garantálható a minőség).

TTX mint tudástranszfer

A kiberbiztonság, a kibertérben végzett műveletek folytatása újító, kreatív elméket igényelnek. Felmerülhet így a kérdés, hogy ezeknek a kvalitásoknak a megszerzése az erősen hierarchikus, szabálykövető katonai felkészítésben hova, és hogyan helyezhető el, illetve, hogy az ilyen újító egyéniségek, alternatív gondolkodók a későbbiekben hogyan illeszkednek egy hadsereg szervezeti egységébe.

Érdemes ilyen tekintetben figyelemmel kísérni más nemzetek képzési programjait. Az Egyesült Államok hadserege, és kormányzati szervei például képviselik magukat a nagyobb hacker konferenciákon (pl.:a Blackhatkonferencián a védelmi szektor szereplői álláshirdetések és ösztöndíj programokat hirdetnek, a Defcon konferencián pedig a "*Meet the Feds*" panelen lehetőség van párbeszédet folytatni a rendvédelmi szervekkel), továbbá versenyekre invitálják az érdeklődőket (hibakereső versenyeket[13], középiskolás rejtvények, un. challenge-ek[14], és felvételi puzzle-ek[15]), valamint kutatásokat támogatnak. Ezek a kapcsolódási pontok segítik a motivált, és megfelelő tudással rendelkezők megszólítását, és bevonzását a folyamatos szakemberhiánnyal rendelkező kormányzati szektorba.

Másfelől a saját, katonai felsőoktatásban részt vevő hallgatóiknak az ilyen irányú ambícióit támogatják, civil szervezésű versenyekre és konferenciákra küldik őket (így esetükben a már meglévő elhivatottság mellé szakmai tapasztalatot is gyűjtenek).

A kibertér egy új terület, mely esetén hiány van az összefüggéseket átlátó, évtizedes tapasztalatokkal rendelkező szakemberekből. Jellemző, hogy a fiatal tisztek naprakész technológiai ismeretekkel rendelkeznek, azonban nincs megfelelő tapasztalatuk a parancsnoki-, és törzsmunkában, míg az ezen a területen, évtizedes tapasztalattal rendelkezők műszaki szakemberek ismeretei, az aktuális fenyegetések, és azok kezelése terén sokszor felületes. A TTX-ek jó lehetőséget adnak arra, hogy a technológia szempontból képzett, valamint a műveleti tervezésben tapasztalattal bíró szakemberek egymással tudásukat megosszák [15].

A korosztályok közötti tudástranszfer mellett a hivatásrendek közötti (civil-katonai, vagy kormányzati szereplők közötti együttműködés) is fontos, törekedni kell rendezvények, konferenciák, és egyéb fórumokon az együttműködés erősítésére.

---

13 Un. Bug Bounty programokat, mint pl.: https://hackerone.com/hacktheairforce ; https://www.hackerone.com/resources/hack-the-pentagon ; https://hackerone.com/deptofdefense

14 Pl.: U.S. CYBER CHALLENGE Forrás:https://www.uscyberchallenge.org/frequently-asked-questions/

15 Forrás: https://www.gchq.gov.uk/puzz

FELKÉSZÜLÉS EGY TTX GYAKORLATRA

Ahogy korábban említettem, a szervezőknek és a résztvevőknek is célszerű felkészítési anyagokat összeállítani, elősegítve munkájukat. A nagyszabású gyakorlatok esetén javasolt készíteni egy központi tudástárat, másnéven wiki[16]-t [16], a szétaprózott anyagok egységes tárolása, aktualizálhatósága (központi frissíthetősége) érdekében.

A felkészülés során használható információs csomagok javasolt tartalmát alább foglalom össze:

- a törvényi szabályzókból, szervezet szintű szabályzatokból összeállított, magyarázatokkal és összefoglalókkal kiegészített segédletek,
- ellenőrző listák (un. Checklist-ek),
- dokumentum minták (un. template-ek),
- felkészítő videóanyagok[17],
- kommunikációs terv[18],
- térképek, hálózati diagrammok

A SANS által összeállított útmutató [17] segítséget nyújt az incidenskezelési terv összeállításában, és annak időszakos tesztelésének megtervezésében.

Célszerű a dokumentumban felsorolt kérdésköröket a gyakorlaton részt vevő incidenskezelő állománnyal áttanulmányoztatni, és az incidenskezelési tervükbe beépíteni.

A levezetéshez, és a gyakorlati feladatok tartalmához útmutatóul szolgálhat a Szövetségi Válságkezelési Ügynökség (*Federal Emergency Management Agency*) által összeállított minta is [18].

A gyakorlat során célszerű folyamatosan nyomon követni a résztvevők munkáját, és naplózni az elért eredményeket, valamint a pozitív és negatív tapasztalatokat. A korábban említett wiki ennek is lehet a fóruma. De csak akkor lesz ez hatékony, ha a kommunikációs csatornákat (pl.:chat), és információs forrásokat (pl.:wiki) már korábban bemutatták a résztevőknek, és nem ott és akkor kell elkezdeni elsajátítani azok használatát.

Forgatókönyv (Storyline) tervezése

A gyakorlatot vezető személy előzetesen megtervezi a biztonsági incidens(ek) körülményeit, és az események időrendjét egy forgatókönyvbe rögzíti. A gyakorlatok egyik legfontosabb kelléke ez a forgatókönyv, mely meghatározza az egyes injekt-eket (elemi eseményeket), azok időrendjét, továbbá a moderátor által megszemélyesített külső szervezetek reakcióit.

Fontos, hogy a szervezetre szabott legyen a gyakorlat története, ezért sokszor a belső munkatársak készítik azt. Ekkor a gyakorlat sikere nagyban függ az ő szakértelmüktől és felkészültségüktől (ez esetenként veszélyt is rejthet magában). Azonban ebben a megközelítésben rejlik egy újabb oktatási potenciál is: a TTX szcenáriójának tervezői is tanulhatnak munkájuk során (fenyegetéseket kutatnak, átnézik az incidenskezelési terveket,

16 A wiki szolgáltatás egy web alapú tartalomkezelő rendszer, mely lehetővé teszi eltérő dokumentumok és egyéb fájlok (képek, videók, prezentációk stb.) megosztását a közös munka segítése érdekében. Számtalan ingyenes szoftver (pl.:mediawiki, dokuwik stb.) áll rendelkezésre, melyek grafikus kialakítása jellemzően a wikipédia weboldalát mintázzák.

17 Gabriel Marzonie – How to Plan a Table-TopExercise https://www.youtube.com/watch?v=J5GwKru1Z0g United Educators - HowtoConduct a Tabletop Exercise https://www.youtube.com/watch?v=1XK_dZkb9KwJames Messer – TabletopExercises - CompTIASecurity+ SY0-401: 2.8 https://www.youtube.com/watch?v=Bz35eXNVBZM

18 Ha többhelyszínes a végrehajtás, vagy szükség van a gyakorlat előtt a résztvevőknek egyeztetniük, közösen felkészülniük

abban hibákat, hiányosságokat, nem egyértelmű részeket keresnek, a támadó fejével gondolkodva életszerű helyzeteket alakítanak ki stb.).

Annak érdekében, hogy ne veszítsen a "meglepetésszerű" jellegéből a gyakorlat, szeparáljuk az érintetteket (a tervezők, és a gyakorlat résztvevői más személyek legyenek). Egy idő után érdemes lehet cserélni (rotálni az állományt), és a korábbi résztvevőket szervezőként alkalmazni.

A forgatókönyv meghatározásánál célszerű a valós életben látható trendeket figyelembe venni, azonban az érzékeny információkat (pl. a szervezet korábbi, vagy aktuális incidensei) kerülni kell (amennyiben nélkülük is megvalósítható a gyakorlat).

Akár több kihívást is lehet a történetbe integrálni (pl.: ransomware fertőzés, mely nyomainak elemzése során egy másik, információgyűjtési céllal végzett célzott támadást is detektáltak a szakértők…)

Fontos, hogy még a végrehajtás előtt gondoljuk azt át, hogy a meghatározott végcél felé mutat-e a gyakorlat terve, van-e benne bizonytalan, vagy félreérthető rész. A gyakorlat levezetője legyen tisztában a végcéllal és a forgatókönyvvel, szükség esetén avatkozzon be, és terelje a megfelelő irányba a csapatot, de ne helyettük oldja meg a problémákat, inkább csak irányított kérdéseket tegyen fel.

A háttértörténet megfelelő előkészítése fontos egy gyakorlat szempontjából, hiszen ezek alapján fognak döntéseket hozni a résztvevők, reagálni az eseményekre. A háttértörténetnek tartalmaznia kell a résztvevők szervezetének leírását, az általuk használt IT rendszereket, korábbi incidensek leírását, CERT jelentéseket, IT biztonsági cégek figyelmeztető leveleit, újságcikkeket, sajtóközleményeket. A nemzetközi „helyzetet” is be kell mutatni, azonban a „politikai” korrektség érdekében célszerű kitalált országok közti konfliktusokat „eljátszani”, elkerülve a külpolitikai kellemetlenségeket (akár egy alternatív valóság megalkotásával, melyben kitalált szereplők és országok konfrontálódnak).

A gyakorlat komplexitása határozza meg, hogy mennyire mély, és alaposan kidolgozott háttértörténetre van szükség. A NATO gyakorlatok során alkalmazott háttér-információk (geopolitika, országok, konfliktusok stb.) egy alternatív világot írnak le. Az egyik ilyen alternatívát *Skolkan* szcenáriónak nevezték el. Ez egy "*olyan környezet, ahol nem a múlt ütközeteire készülnek fel, hanem a jövő kihívásai elé tudják a NATO erőket és parancsnokságokat állítani*"[19].

Két verziót dolgoztak ki legutóbb, a Skolkan 1.0 szcenáriót, mely egy 5. cikkely szerinti védelmi helyzetet demonstrál, és a Skolkan 2.0-át, mely egy komplex, nem 5. cikkely szerinti válsághelyzet, egy regionális krízis menedzselését követeli meg.

A bevezetőben tárgyalt sajátosságok miatt szükséges lenne egy "Cyber Skolkan" kidolgozása is, mely lehetővé tenné, hogy a különböző fegyvernemek gyakorlataiba, a kibertérből érkező fenyegetések is integrálásra kerüljenek.

TTX gyakorlat lefolytatásának menete

A felkészülésre és a végrehajtásra szánt idő, az elérendő célok, és a résztvevők háttere (tudása és munkája), alapján különböző gyakorlatokat szervezhetünk. Az alábbiakban ezek a típusok kerülnek felsorolásra:

- általános oktatási célú,
- kampányszerű ("többlépcsős"),
- epizódszerű,
- funkcionális gyakorlatok (egy-egy részterületre koncentrálnak).

A legegyszerűbb ezek közül a biztonságtudatosító kampány részét képező általános oktatásokat kiegészítő, vagy az ismeretterjesztést szolgáló gyakorlat. Ezek általában nem

összefüggő forgatókönyvek alapján évente, vagy félévente kerülnek megrendezésre, gyakran eltérő szakterületeket érintenek (és eltérő kompetenciák fejlesztését célozzák).

A kampányszerű ("többlépcsős") gyakorlatokat célszerű többnaposra szervezni, így az akciók-reakciók alaposabban kidolgozottak lesznek, mivel több idejük van a résztvevőknek a felkészülésre, a szervezőknek a reakciók értékelésére. Az epizódszerű gyakorlatok gyors, rövid lefolyásuk miatt egy-egy aktuális biztonsági kihívás kezelésére készítik fel a résztvevőket (pl.: új malware terjedésre figyelmeztet a CERT, külső helyszínen rendezvény szervezünk, melyre informatikai szolgáltatásokat is biztosítunk stb.).

A funkcionális gyakorlatok az alábbiakban felsorolt részterületek egyikére koncentrálnak, és az adott szakterületen dolgozók felkészültségének ellenőrzésére, fokozására használhatók. Célszerű kiemelni az adott csoport szerepét, feladatait és tevékenységük hatását a szervezet egészének kiberbiztonságára.

Funkcionális gyakorlatok fókuszcsoportja:

- Felsővezetők,
- Jogi részleg,
- CIMIC/PR, kommunikációs feladatokat ellátó személyek,
- Igazságügyi szakértők,
- Fizikai biztonságért felelős személyek (objektum/személyvédelem),

Szerepjáték szerepe a szervezeti folyamatok megértésében

Jó szemléltetési eszköz lehet a szerepjáték alapú gyakorlat akkor is, ha a résztvevőkkel számukra ismeretlen perspektívából szeretnénk szemléltetni egy-egy biztonsági problémát. Például az incidenskezelő csapat tagjai számára a felsőszintű vezetés munkáját, a külső kapcsolattartók szerepét, stb. mutatjuk be. Ezek a "fordított napok" hozzásegíthetik őket a hatékonyabb kommunikáció kialakításához (pl. látják, hogy milyen jellegű, és minőségű információra van szükségük a döntéshozóknak).

SZIMULÁCIÓS RENDSZEREK - COMPUTER ASSISTED EXERCISE (CAX)

Már a 60-as évektől alkalmaznak katonai célú döntéstámogató szoftvereket, illetve a kiképzést támogató szimulációs rendszereket. Ezek elsődlegesen a klasszikus katonai feladatokra vannak kifejlesztve, és a szárazföldi és légi műveletekben való részvételre készítik fel a különböző vezetési szinteket [20].

A harc szimulációja előre definiált forgatókönyvek és szimulációs modellek segítségével zajlanak. Ezek lehetnek kis felbontású "n" résztvevős, szakterület specifikus szimulációk *(pl.:logisztikai terület),* valamint nagy felbontású, részletes gyakorlatok, melyek a hadműveletek több aspektusát is szimulálják.

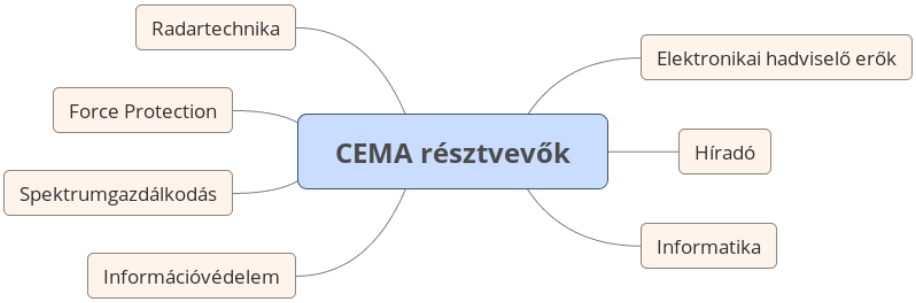
A szimulációnak több rendeltetése is van, egyrészt a döntési alternatívák elemzésére használható (ekkor kutatási eszköz a helyzetértékelés és a döntéstámogatás érdekében), valamint az alegységek, a parancsnokok és a törzsek felkészítésében is használható gyakorlattámogató eszköz (Computer assisted exercise, másnéven CAX) is lehet.

A szimulációs rendszerek használatával a TTX-ek realisztikusabbakká tehetőek, ennek érdekében a kiberműveletek, azok fizikai és egyéb hatásainak ábrázolására lenne szükség a cyberCAX-ok során.

Ugyancsak érdekes fejlesztési irány lenne a technikai kiberbiztonsági gyakorlatokban zajló események, és a CAX -ban zajló katonai műveletek összekapcsolása. Ez hasonló lenne azokhoz a hibrid gyakorlatokhoz, melyben egyes mozzanatok a szimulációs rendszereken, mások a valós gyakorlótereken kerülnek végrehajtásra.

TÖBBSZINTŰ GYAKORLATOK

A "többdimenziós" (un. *Multi &Cross level training*), több szakterület és vezetési szint együttműködését elősegítő gyakorlatok során is hatékonyan alkalmazhatóak a TTX-ek, mellyel összekapcsolhatóak a különböző szakterületek (horizontális összekapcsolás), valamint végrehajtói és a döntéshozatali szintek (vertikális összekapcsolás).



2. ábra A CEMA résztvevői (saját szerkesztés)

Az Egyesült Államok hadserege 2014-től kezdődően a korábban különálló, és más-más alegységek (LÁSD: 2. Ábra) által az elektromágneses spektrumban, és a kibertérben végzett műveleteket egységesítette, és integrálta a CEMA (*Cyber Electromagnetic Activity*) koncepcióban [21]. E mellett a doktrinális változtatás mellett az utóbbi években gyakorlati példákat is láthattunk (Ukrajna, Szíria) az egyre szorosabbra fonódó elektronikus hadviselési, és a kibertérbeli műveletekre [22].

Ezek alapján a katonai kiberműveletekre való felkészítést nem önállóan, hanem a hadsereg más fegyvernemeivel közösen kell végrehajtani. A kiberbiztonság vonatkozásában a többszintű katonai gyakorlatokra a híradó, az informatikai, az információvédelmi, a felderítő és az elektronikai hadviselés erők minél szorosabb, és hatékonyabb művelettervezése miatt lenne szükség.

A TAPASZTALAT ÖSSZEGYŰJTÉSE

A résztvevőknek a TTX gyakorlatok angol kifejezéssel a STARTEX-től az ENDEX-ig tartanak. A szervezőknek ez hosszabb, hiszen a korábban említett felkészüléstől, az eredmények és tapasztalatok kiértékeléséig tart. A gyakorlat lezárásaképpen meg kell határozniuk, hogy mi működött (ezek alapján a bevált gyakorlatokat, más néven a "best practices"-eket összegezhetjük), és hogy mi nem működött megfelelően, melyekből a későbbiekben tanulnunk kell (ezt nevezzük "lesson learned"-nek).

A gyakorlat lezárását követően egy előzetes értékelést kell tartani ("hot washup"), melyben a résztvevőktől meg kell tudni az elsődleges benyomásokat, majd egy részletes jelentést kell készíteni (un. After Action Report-ot). Célszerű a munka gyorsítása, és a könnyű átláthatóság érdekében kérdőív segítségével felmérni a résztvevők véleményét.

A NATO "ODCR" formátuma [23] ebben is segíthet, mely az alábbiakban látható 4 szempontot foglalja össze:

Észrevételek	Observation Description:	„What happened?"
Tapasztalatok leírása (indoklás)	Discussion:	„Why did it happen?"
Következtetések	Conclusion	„What can we learn from this?"
Javaslattétel	Recommendation:	„Who can do what about it?"

Felmerülhet a kérdés, hogy kitől is gyűjtsük a tapasztalatokat? A gyakorlatok során, illetve azt követően az alábbi szereplőktől érdemes:

- szervezőktől,
- résztvevőktől,
- külső megfigyelőktől (ha volt ilyen)

Nagyobb gyakorlatok esetén külön tapasztalatgyűjtő csoport is alakulhat, hogy hatékonyabb legyen az információgyűjtés.

A különböző forrásból gyűjtötteket értékelni kell, és felülvizsgálni, amennyiben valós problémát azonosítottak, akkor javaslatokat kell tenni a következő gyakorlatok hatékonyságának javítására[19]. Célszerű erre egy online felületet létrehozni (pl.: a korábban említett wiki), így akár a gyakorlat közben is tudnak jelezni a résztvevők.

Az egyes gyakorlatok során tapasztaltak mellett a hosszabbtávú statisztikák és a későbbi visszajelzések (pl.: az egy éve korábban megtartott gyakorlaton elsajátítottak hasznosak voltak-e, vagy sem) is érdekesek lehetnek.

A NATO a tapasztalat feldolgozó oldalán létrehozott egy Cyber Defence Community of Interest Lessons Learned oldalt[24], ahol a nemzetek és a szövetég tudja megosztani a gyakorlatok kibervédelmi aspektusaiból tanultakat.

TÖBBNEMZETI GYAKORLATOK

A kooperáció a kibervédelem területén (nemzetközi szinten, szövetségi rendszeren belül, és nemzeti szinten, a kormányzati rendszerek és a gazdasági - ipari szereplők között) azért fontos, mert egy-egy támadás állami infrastruktúrák ellen is irányulhat (például Észtországban 2007 tavaszán [25], vagy Ukrajnában 2015 és 2016 decemberében [26]). Illetve sokszor még a „célzott" támadások sem állnak meg a célpontjuknál (pl.: az iráni atomprogramot szabotáló Stuxnet, más rendszereket is megfertőzött [27]). Így a minket célzó támadók másokat is érinthetnek (pl. egy többnemzeti katonai művelet során). Ennek következtében az incidenskezelés egységesített, közös metodikája és az információ megosztás nélkülözhetetlen a hatékony válaszlépéshez.

Ezt a közös metodikákat legkönnyebben közös gyakorlatok szervezésével lehet elsajátíttatni. A többnemzeti gyakorlatok során gyűjtött szemléletmódok, elsajátított új módszerek ("bevált gyakorlatok, best practice-ek") növelik a szervezet felkészültségét, csökkentik az incidensek bekövetkezési valószínűségét, és azok hatásait.

A korábbiakban leírt kommunikációs készségek nemzetközi együttműködések során hatványozottan szükségesek, és amellett, hogy mi nyitottak vagyunk a felénk irányuló

19 Az értékelés szerepe és felhasználása is kettős: egyrészt a résztvevők saját magunknak is készíthetnek, hogy a következő gyakorlatra (vagy a valós helyzetre) fel tudjanak készülni, illetve a szervezők is gyűjthetnek adatokat. Mindkettő alkalmas lehet, hogy a gyakorlat szűk céljain túl a tevékenységek hatékonyságának javítására fel lehessen használni, úgy, mint új védelmi eszközök, eljárásrendek, oktatási módszerek és segédletek, doktrínák kidolgozása.

kommunikációra, ismernünk kell más nemzetek sajátosságait is (habitus, helyi szokások és szabályzók). Ezek elsajátítására kiváló lehetőséget adnak a nemzetközi TTX-ek.

Információbiztonsági szempontok

A gyakorlatok, még ha nem is használnak fel minősített információt (pl.: felderítési jelentéseket) akkor is generálhatnak érzékeny adatokat, hiszen a résztvevők felkészültsége, a valós helyzetben alkalmazandó taktikákra és stratégiákra vonatkozó információkat tartalmazhatnak. Ilyen tekintetben információvédelmi szempontból érdemes elgondolkodni a gyakorlat, és az azzal kapcsolatban készült dokumentumok minősítésén.

Sok esetben éppen ez, az információ korlátozása és meg nem osztása szab gátat az előző fejezetben leírt többnemzeti, közös gyakorlatoknak.

Véleményem szerint itt is egy egészséges egyensúlyt kell kialakítani: azonosítani kell azokat az információkat, képességeket, törekvéseket, melyeket nem kívánunk külső féllel megosztani, továbbá azonosítani kell az azok megismerésére jogosultak körét (különböző csoportosításokat alkalmazhatunk pl.: NATO, EU, V4 országok, rendvédelmi szervek stb.). Ezt követően törekedni kell az együttműködésre és az információ megosztására partnereinkkel.

KÖVETKEZTETÉSEK

2016 évi Varsói NATO csúcson amellett, hogy a kiberteret műveleti térnek definiálták, a tagállamok ígéretet tettek a saját kibervédelmi képességeik fejlesztésére, valamint megállapodtak az információ-megosztás javításáról, a közös oktatások, kiképzések, továbbá gyakorlatok szervezéséről is [28].

Jelen cikk a kiképzés egyik, de nem egyetlen lehetséges eszközét, az un. Table Top Exercise-okat mutatja be. Az ilyen jellegű gyakorlatok közelebb hozzák a különböző területeken dolgozó szakembereket, és a kiberbiztonság technikai vetületei mellett, a gazdasági, diplomáciai, politikai, nemzetbiztonsági, vagy akár katonai hatásaira is felhívják a figyelmet [29].

Jelen cikk célja az oktatásban való alkalmazás lehetőségeinek bemutatása, azonban a TTX-ek ennél szélesebb körben alkalmazhatóak, és az informatikai rendszerekkel kapcsolatban állókat segíthetik a biztonságtudatosság elsajátításában, és a mindennapok során annak gyakorlásában. Reményeim szerint a bemutatott lehetőségek másokban is felkeltik az érdeklődést, és a saját szervezetük igényei és lehetőségei szerint alkalmazzák is a TTX-ekben rejlő lehetőségeket.

Sun Tzu, vagy Julius Caesar óta minden klasszikus stratéga tudta, hogy a győzelemhez ismernünk kell az ellenfél, valamint a saját erőink és eszközeink képességeit, azok alkalmazásának taktikáját. Nincs ez másképpen a kibertérben sem, azonban az új dimenzió újfajta eszközök, és újszerű taktikák alkalmazását követeli meg.

Azt is fontos látni, hogy az új hadviselési dimenziónak vannak kapcsolatai a fizikai (szárazföldi-, vízi-, légi- és űr- telepítésű) infrastruktúrákkal, így ezek kölcsönös egymásra hatásával is számolni kell. Ezek a dependenciák pedig növelik a fenyegetések számát. Továbbá a döntési lehetőségeket (és egyben a hibás döntések) száma is bővül ennek a komplex "játéktérnek" a bevezetésével. Szükség van hát gyakorlott játékosokra, akik a TTX-eken felkészültek a valóság kihívásaira.

FELHASZNÁLT IRODALOM

[1] *Chemical Warfare - World War I :* https://www.awm.gov.au/system/files/documents/051%20Chemical%20Warfare%20in%20FWW.pdf Letöltve:2017.08.20

[2] C. W. (CHARLIE) WILLIAMSON – *Carpetbombing in cyberspace* http://armedforcesjournal.com/carpet-bombing-in-cyberspace/ Letöltve:2017.08.20

[3] S. D. CARBERRY – *Why there's no one deterrent for cyber* :https://fcw.com/articles/2017/02/16/cyber-rsa-deterrent-carberry.aspx Letöltve:2017.08.20

[4] NATO - *NATO Future Online Learning Vision* https://innovationhub-act.org/sites/default/files/Future%20Online%20Learning%20Report%20IH.pdf Letöltve:2017.08.20

[5] *NATO Joint Advanced Distributed Learning Online Course Catalogue* https://jadl.act.nato.int/CourseCatalog.pdf Letöltve:2017.08.20

[6] T.GRANCE,T. NOLAN, K. BURKE, R. DUDLEY, G. WHITE, T. GOOD - *Guideto Test, Training, and Exercise Programs for IT Plans and Capabilities (NIST SpecialPublication 800-84)*, p. 21. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf Letöltve:2017.08.20

[7] DEF CON 25 – G. KASPAROV - *The Brain's Last Stand* (előadás) https://www.youtube.com/watch?v=fp7Pq7_tHsY Letöltve:2017.08.20

[8] *No Patch for Human Stupidity – Three Social Engineering Techniques You Might Not Know About* https://www.packtpub.com/books/content/no-patch-human-stupidity-three-social-engineering-techniques-you-might-not-know-about Letöltve:2017.08.20

[9] A. LEVIT - *The Future of Education According to Generation Z* http://time.com/3764545/future-of-education/ Letöltve:2017.08.20

[10] Northern Illinois University - *Millennials: Our Newest Generation in Higher Education* http://www.niu.edu/facdev/_pdf/guide/students/millennials_our_newest_generation_in_higher_education.pdf Letöltve:2017.08.20

[11] V. S. COOK – *Engaging Generation Z Students* https://sites.google.com/a/uis.edu/colrs_cook/home/engaging-generation-z-students Letöltve:2017.08.20

[12] KOVÁCS, L.; NEMESLAKI, A.; ORBÓK, Á.; SZABÓ, A. – *Structuration Theory and Strategic Alignment in Information Security Management: a Comprehensive Research Approach and Program*, Academic And Applied Research In Military And Public Management Science 16:(1) pp. 5-16. (2017),p. 10.

[13] S. M. KERNER – *How Hackers Brief the Board to Improve Security Outcomes Black Hat 2017* konferencia előadása

[14] BENCSÁTH-BUTTYÁN-KAMARÁS-ÁCS-KURUCZ-MOLNÁR: *Az információgyűjtés feladata és lehetőségei informatikai támadások megelőzése és kezelése céljából (A terrorizmus Rubik-kockája, avagy a fenyegetések komplex*

megközelítése) http://www.bm-tt.hu/assets/letolt/t3konf/tanulmanykotet_t3.pdf Letöltve:2017.08.20

[15] JASON M. BENDER - *The Cyberspace Operations Planner Challenges to Education and Understanding of Offensive Cyberspace Operations* http://smallwarsjournal.com/printpdf/14857 Letöltve:2017.08.20

[16] F. ABDUL KARIM, K. SAMSUDIN AND W. AZIZUN WAN ADNAN -*WikiTTX: A Web Collaboration Technologybased Table-TopExercise System* http://www.ipcsit.com/vol2/21-A205.pdf Letöltve:2017.08.20

[17] K. HOLLAND (SANS) – *Incident Handling Annual Testing and Training* https://www.sans.org/reading-room/whitepapers/incident/incident-handling-annual-testing-training-34565 Letöltve:2017.08.20

[18] *National Level Exercise 2012 CyberSecurityTable Top Exercise (Facilitator Background Information)* https://www.fema.gov/media-library-data/20130726-1834-25045-1623/nle_12_ttx___facilitator_s_notes_5.10.12_final__508.pdf Letöltve:2017.08.20

[19] SKOLKAN: *NATO's operational battlespace THINK DIFFERENT* http://www.jwc.nato.int/images/stories/_news_items_/2016/SKOLKAN_interview.pdf Letöltve:2017.08.20

[20] MUNK S. - *Számítógéppel segített gyakorlatok a NATO hadseregekben*, Akadémiai közlemények, 1995. 207. szám p. 191-202.

[21] Department of the Army - *Field Manual No. 3-38: Cyber Electromagnetic Activities* Forrás: https://fas.org/irp/doddir/army/fm3-38.pdf Letöltve:2017.08.20

[22] KOVÁCS L. - *Az elektronikai hadviselés jelene és lehetséges jövője* HADMÉRNÖK 12:(1) pp. 213-232. (2017) Forrás:http://hadmernok.hu/171‚7_kovacs.pdf]

[23] A. GEORGIEV - *NATO LESSONS LEARNED PROCESS* előadásanyag (26 January 2017) https://www.cmdrcoe.org/download.php?id=575 Letöltve:2017.08.20

[24] NATO Lessons Learned Conference 2016 - Day 2 (online) http://www.jallc.nato.int/activities/events_2016.asp#20161130 Letöltve:2017.08.20

[25] HAIG ZS., KOVÁCS L. - *Fenyegetések a cybertérből;* Nemzet és Biztonság: Biztonságpolitikai Szemle 1:(5) pp. 61-70. (2008) http://www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf Letöltve:2017.08.20

[26] A. GREENBERG - *How An Entire Nation Became Russia's Test Lab for Cyberwar* https://www.wired.com/story/russian-hackers-attack-ukraine/ Letöltve:2017.08.20

[27] KOVÁCS L., SIPOS M. - *A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala;* Hadmérnök 5:(4) pp. 163-172. (2010); http://hadmernok.hu/2010_4_kovacs_sipos.pdf Letöltve:2017.08.20

[28] North Atlantic Council - Warsaw Summit Communiqué http://www.nato.int/cps/en/natohq/official_texts_133169.htm Letöltve:2017.08.20

[29] KOVÁCS L., KRASZNAY CS. - *Mert övék a hatalom: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során* Stratégiai Védelmi Kutató Központ (Elemzések) / Center For Strategic And Defense Studies Analyses 2017:(9) pp. 1-11. (2017)