HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Szegediné Lengyel Piroska
l.piroska@t-online.hu

AZ INFORMATIKA „PISZKOS BOMBÁJA" A SZÁMÍTÓGÉPES BŰNÖZÉS
Bevihetők-e az informatika távoktatásába a számítógépes bűnelkövetést lehetővé tevő ismeretek?

Absztrakt

Az informatika radikális fejlődése, illetve a vele együtt rohamosan terjedő számítógépes bűnözés, analóg és hasonló súlyú kérdéseket vet fel manapság, a 21. század elején, mint amilyeneket – például a nukleáris láncreakció békés, illetve pusztító célú alkalmazási lehetőségeinek áldás-átok dilemmája kapcsán – már több mint fél évszázada próbál több-kevesebb sikerrel kezelni az emberiség. Számos irodalom foglalkozik azzal, hogy a legújabb kor legnagyobb katonai és egyúttal társadalmi veszélye már nem az atomháború [1], hanem az informatikai bűnelkövetés következtében jelentkező kockázatok és lehetséges katasztrófák valószínűségének a növekedése. Az informatika hatalmával tehát ugyanúgy, mint ahogyan a nukleáris energia erejével, lehet élni és visszaélni. Hovatovább, a romboló célú informatikai tudást és potenciált, sokkal kisebb anyagi- és energiaráfordítással is meg lehet szerezni, miközben a vele való visszaélés veszélyével, sajnos, sokszorta nagyobb dimenziókban is szükséges számolnunk. Mint a legmodernebb, egyúttal legalattomosabb fegyverek egyike az informatika, pontosabban a – vele együtt elburjánzó – „romboló informatika" mindennél gyorsabb, „sui generis" globalizálódása, gyakorlatilag minden társadalmat, minden háztartást, minden egyes élőlényt, sőt a természetes és az épített környezetünket is egyaránt fenyegeti. Mindezen realitások a – veszély megelőzését, elhárítását, az esetleges bekövetkezett katasztrófák kezelését, a károk enyhítését és reparálását végezni hivatott – civil és a katonai erők számára új kihívásokat jelentenek. A kihívás részeként új dimenzióban jelentkezik az a dilemma is, hogy milyen körben terjeszthetők, oktathatók az informatikai bűnözéshez, és annak kivédéséhez szükséges ismeretek és ezen ismeretek mely halmaza alkalmas arra, hogy távoktatási keretek között is terjeszthető, illetve oktatható legyen. Mindenekelőtt, releváns-e egyáltalán az a kérdés, hogy a nyilvánvalóan bizalmas és nagyon kényes informatikai ismeretek bevihetők-e a távoktatás szférájába?

The radical speed of developments in the field of the informatics and the parallel accelerating pace of cyber criminality are raising similar serious questions, today, at the beginning of the 21st century, as the ones which – connected e. g. to the "boon/curse" dilemma of peaceful and destroying use of nuclear chain reaction – have been tried to be managed by the societies, with more and less success, since more than five decades. Several papers underline that it is not the nuclear war [1] which must have been the most threatening military and, also, social danger in the latest age, but the increasing likelihood of risks and potential catastrophes due to the cyber criminalities. The power of informatics can, as that of the nuclear energy, be used in a good and bad way, as well. Moreover, the "destroying knowledge and potential" can be gained by investing far less material and energy input in case of informatics, while one has to face multiplied dimensions of danger of using it for bad goals. The fastest than ever "sui generis" globalisation of the informatics, more precisely, that of the even growing "destroying informatics", as a weapon among the most up-to-date and, at the same time, most treacherous ones, has been threatening practically all societies, households, each and every being creatures, furthermore our natural and constructed environment, as well. All these realities represent new challenges for the civil and military forces dedicated for avoiding catastrophes, handling the eventually occurring ones, diminishing and repairing the damages. As a part of challenges, a new dimension is added to the dilemma of "what can be the extent of the population to be addressed by teaching materials on cyber criminalities and defending techniques against them and which parts of these materials can be treated as appropriate for spreading over by distance education (e-learning)". Nevertheless, has or has not any relevance the question of "whether to put obviously confidential and very sensitive types of information into the sphere of distance education?"

Kulcsszavak: *távoktatás, informatika didaktika, informatikai intelligencia, számítógépes bűncselekmények, kritikus infrastruktúrák, informatikai biztonság ~ online/distance education, didactics in informatics, intelligence in informatics, cyber criminality, critical infrastructures, security in informatics*

BEVEZETŐ

Az elmúlt években a didaktika „Mit, miért, mivel, hogyan?" kérdése az informatika-oktatásban folyamatosan napirenden volt, függetlenül attól, hogy az oktatás hagyományos vagy távoktatási keretek között folyt-e. Az a dilemma pedig, hogy „miként épüljön fel az informatika tananyag, milyen legyen az elmélet és a gyakorlat aránya, ugyanaz az informatika kell-e mindenkinek, milyen a jó informatika terem, befolyásolja-e az eszköz a gondolkodásmódot, mi legyen az informatika tankönyvben, kell-e az elektronikus tananyag mellé oktató…?", ma, a számítógépes hálózatok, az Internet radikális térhódításának és azzal párhuzamosan a számítógépes bűnözés, az informatikai bűncselekmények terjedésének időszakában, különösen aktuálissá vált és további kérdéseket szül.

A kérdésekkel együtt, természetesen egyre többször vetődnek fel az alábbiakhoz hasonló kétségek, kételyek:

- Az informatikai tananyagok, műveltségi területek milyen speciális részeit, és milyen mélységig tanítsa meg az oktató?
- Az egyes tananyagrészek oktatásához milyen példákat, milyen esetpéldákat célszerű használni?
- Milyen veszélyekkel jár, járhat a valós események modellezése, a valós rendszerek modelleken keresztül való megismertetése?

Az informatikaórákon alkalmazott nevelési feladatok kapcsán felvetődik a jogos kérdés: Hogyan alakítható ki, fejleszthető tovább a pozitív informatikai intelligencia? Az informatikai ismeretek rossz irányú, illetve célú felhasználásának lehetőségeit, módozatait szükséges-e, illetve szabad-e oktatni?

Újfent szemben találjuk magunkat azoknak a „déjà vue" paradoxonoknak a tömkelegével, amelyeket a nukleáris fegyverek, a „szegények atombombái"-nak is nevezett piszkos bombák, a biológiai-, vegyi- és radiológiai fegyverek előállításának problémái kapcsán kezelni véltünk, de megoldani aligha tudtuk. Talán még az elmélet szintjén sem. Legfeljebb lokalizálni sikerült. A paradoxonok lényege ugyanis, miszerint az ilyen fegyverek előállításához szükséges technológia és szakértelem is „duális célú és felhasználású", tehát hasznos, de egyúttal pusztító is lehet, ténykérdés. Ebből fakadóan, a negatív fejlemények és kimenetek eshetősége, mintegy Damokles kardjaként, elkerülhetetlenül, folyamatos fenyegetettségként jelentkezik. A cél pedig a lokalizálás hatékonyságának az erősítése, a negatív fejlemények és kimenetek eshetőségének minél biztonságosabb kizárása, a gerjesztő jelenségek kiszűrése, kivédése, megszűntetése lehet.

E vonatkozásban, kézenfekvő eligazítást kínálnak az előző generációk mindennapjainak példái, amelyekről számos formában találhatunk – az irodalomtól kezdve a tudománytörténetig – plasztikus megfogalmazásokat. Több mint száz évvel ezelőtt, a radioaktivitás első alkalmazásai során például még senki sem gondolt arra, hogy évtizedekkel később majd tömegpusztító fegyvereket fejlesztenek ki a segítségével, inkább az orvosi terápiában látták hasznosan alkalmazhatónak a felfedezett jelenséget. Először Otto Walkhoff és F. Giesel észlelte, hogy a sugárzás roncsolja a szöveteket. Erről értesülve, Pierre Curie tíz órán keresztül tartott a kezén rádiumforrást, majd tapasztalatai alapján arról készített tanulmányokat, hogy az eljárás alkalmas lehet bizonyos bőrbetegségek kezelésére. Bár bizonyos jelek arra mutattak, hogy akár több kára is lehet az alkalmazásnak, mint haszna, mégis egy szörnyű halálesetre kellett várni, hogy felrázza a tudományos életet: egy amerikai üzletemberére, aki éveken át rádiumkészítményt használt közérzetjavítónak.

A paradox helyzet „kiteljesedésére" sem kellett sokat várni. Történelmi léptékkel mérve, pillanatok alatt következett be a nukleáris fegyverek gyors kifejlesztése és katonai alkalmazása. A magyarázathoz a világháborús körülményekre való utalás közismert. Olyannyira, hogy a világ iskolázott része a tananyag részeként, már tizenéves korában megtanulja, hogy az Egyesült Államokban 1939-ben kezdődött a nukleáris fegyver kifejlesztését szolgáló Manhattan-terv. Hogy a kutatások 1945. július 16-án értek be és felrobbantották az első kísérleti atomfegyvert. Hogy az új szuperfegyver alkalmazása is hamarosan bekövetkezett, hogy az amerikai hadsereg augusztus 6-án Hirosimára a Little Boy, 9-én Nagaszakira pedig a Fat Man elnevezésű atombombát dobta le. Miközben kérdéses, hogy mindezen történelmi események megismerése során a tizenéves generációk milyen mélységben gondolják végig a szörnyűséges paradoxonok tényét, illetve az oktatók mennyire érzik kötelességüknek és felelősségüknek ezen típusú empatikus képesség, emberi intelligencia kialakítását és fokozását.

Meggyőződésem, hogy a morálisan helyes oktatói intelligencia magában hordozza az ismeretek duális felhasználhatóságának teljes körű ismeretét, és megismertetési kötelezettségét, bemutatva annak mindennemű erkölcsi és jogi következményeit. Ugyanakkor, természetesen vizsgálni kell, hogy miképpen ellenőrizhető az ismeretátadás megbízhatósága, hogyan oldható meg a felelősségrevonás, amennyiben felmerül a gyanú, hogy a terjesztett ismeretek a társadalomra nézve károsak és hátrányosak. Más szavakkal, foglalkozni kell azzal a kérdéssel, hogy bizonyos ismeretek és tudás átadása meg kell ugyan történjen, az érintettséget, az illetékességet azonban – szakmai, etikai alapon – kénytelen-kelletlen, de elengedhetetlenül szabályozni szükséges.

A probléma, érthetően, egyre sűrűbben vetődik fel úgy az egyedi, mint a hétköznapok bejáratott távoktatásos rendszereinek alkalmazásakor is. Annak ellenére fenyeget, hogy a korszerű keretrendszereknek – pl. Moodly, ILIAS – köszönhetően a nyitott oktatás akár a széles körben alkalmazott megoldások esetében is „zárttá" tehető, technikailag tehát kizárólag csak a kurzusra beiratkozott hallgatók körére szűkíthető. Ezáltal természetesen lokalizálható az érzékeny információk és tudás távoktatásos kereteinek kockázata, teljes mértékben azonban nem zárható ki. A valóságban ugyanis reális lehetőségként kell számolni például azzal, hogy az arra feljogosított felhasználó, bár saját kódjával lép be a rendszerbe, de nem akadályozza meg arra illetéktelen felhasználók jelenlétét, sőt, rosszabb esetben – egyébként akár a rosszhiszeműség legkisebb jele és szándéka nélkül is – előfordulhat, hogy még támogatja is őket a tudás elsajátításában. Elgondolkoztató, Karen F. Owen, a Duke University végzős hallgatójának esete, aki „kvázi" diplomamunkát készített „An education beyond the classroom: excelling in the realm of horizontal academics" címmel, amelyben mintegy tucatnyi fiatalember, nevekkel ellátott legprivátabb adatait rögzítette, majd néhány ismerősének bizalmasan e-mail-ezte, akik szintén bizalmasan, továbbküldték másoknak, végül a világhálón kötött ki. [10]

HOGYAN? MIVEL?
A TÁVOKTATÁS MÓDSZERTANA

Az oktatás eszközrendszerének számbavétele kapcsán fontos leszögezni, hogy az Informatikai ismeretek a távoktatásos formában való közvetítésre ugyanúgy alkalmasak, mint bármely más ismeretanyag [2], ugyanakkor a tantárgy speciális területei – számítógépes hálózatok elleni támadások, informatikai bűncselekmények – újfajta távoktatásos módszertant igényelnek.

Paradigmaváltásra, új gondolkodásmódra, újfajta problémafelvetésre van szükség, amiből újfajta problémamegoldás fakad. A javasolt megközelítési mód találóan összegezhető a relativizmus atyjának, Albert Einsteinnek egyik híres mondásával: „Egy problémát nem lehet ugyanazzal a gondolkodásmóddal megoldani, mely a problémát előidézte."

Mindenekelőtt le kell szögezni, hogy az Informatika ismeretek távoktatása csak akkor lehet hatékony, ha a hagyományos tantermi oktatást – aminek alapja az „oktató és hallgatók közötti személyes kapcsolat", mint tantárgy specifikusság – teljes mértékben képes pótolni, ha a „távolság" nem csorbítja az oktatás minőségét, az átadott tudás tartalmát. Természetesen még nagyon sok olyan oktatási terület létezik, ahol elengedhetetlen az oktató és a hallgatók közötti személyes közreműködés, ugyanakkor az informatika előbb említett néhány speciális anyagrésze, a szakanyag közlésén túl, komoly nevelési feladatokat, azonnali reakciókat, reagálásokat követel meg az oktatótól.

Figyelembe véve az említett nevelési feladatokat, az Informatika tantárgy távoktatásának módszertani megoldásai céljára, hasznosnak ítélem a – Számviteli ismeretek e-könyveimben már sikerrel alkalmazott [11] – négyszintű modell [3] rövid áttekintését.

Az Informatika tantárgy távoktatásának négyszintű oktatási modellje		
Stratégia	**Módszer**	**Technológia**
Tanulás információn keresztül	Információ átadás **elektronikus könyveken** keresztül	Internet CD
Tanulás interakcióval	**Interaktív tanulás** Tanulás szimulációk, játékok, modellek segítségével. Saját ütemezésű tanulás on-line előadásokon	Multimédiás eszközök
Tanulás együttműködve	**Kooperatív-munka** **On-line foglalkozások** virtuális oktató termekben	Személyes kapcsolat Együttműködés
Tanulás csoportban	**Pódium - Drámapedagógia** **Tapasztalat-orientált oktatás, a szerzett ismeretek elmélyítése** szerepjátékok, esettanulmányok, projekt feladatok	Személyes kapcsolat Együttnevelés

A négyszintű modell egyik alapelve a fokozott együttműködés. A modell az ismeretátadás és az együttműködés lépcsőfokain halad előre, az alapvető információk megszerzésétől a felsőfokú ismeretek szintjéig terjed.

Ez a modell arra igyekszik rávilágítani, hogy a távoktatásra szánt anyag tantárgyi programjának kidolgozása során nem szabad megfeledkezni arról, hogy az e-oktatás teljes mértékben nem helyettesítheti a tantermi oktatást, a képességek fejlesztésének bizonyos fokán mindig is szükség van az oktatóval, az adott téma szakértőjével való találkozásra.

A tanulási folyamat első szintjén – **„Tanulás információn keresztül”** – az alapvető ismeretek átadása, az alaptudás biztosítása az „Olvasd!”módszeren alapszik. Cél, hogy a tanuló könnyen és egyszerűen megtalálja az információt, könnyen és gyorsan elsajátítsa azt, amit a tananyag, a könyv közölni akar. A módszertanilag és didaktikailag átgondoltan szerkesztett könyv alapján a felhasználók világosan átlátják a tananyag elsajátításának lépéseit, az abban való haladás ütemét.

A második szinten – **„Tanulás interakcióval”** – a **„**Fedezd fel!”módszer az alapvető képességek fejlesztésére fókuszál: az új alkalmazások, eljárások megismerése szimulációk, modellek, esetleg játékos feladatok közvetítésével történik, időfüggetlen on-line előadásokon.

A harmadik szint – **a „Tanulás együttműködéssel”** – a **„**Vitasd meg!” alapvetően a társakkal való együttműködési technikákra épül, ahol a képzés nevelési feladatainak meghatározó elemeként megjelenik a tanterem. A felhasználók virtuális osztályteremben csoportos feladatot kapnak, véleményt cserélhetnek, tapasztalataikból közösen tanulhatnak. A háttérben megjelenik/megjelenhet az oktató, akinek lehetősége nyílik az egyéni képességek feltérképezésére, a felhasználók gondolkodásmódjának megismerésére.

A negyedik a – **„Tanulás csoportmunkával" – „**Játszd el**!"** szinten**,** a tanterem mellett az oktató is a tanulási folyamat „főszereplőjévé" válik. A modellnek ez a szintje, a tanulási folyamat eredményeként jelentkező, az igazán fejlett, illetve színvonalas ismeretek és képességek birtokában használható hatékonyan, az alapfokú tudástranszfernél nem. A gyakorlati feladatok és konkrét esetek kivitelezése során felhasználói oldalról lehetővé válik az ismeretek elmélyítése, oktatói oldalról, pedig a felhasználók elsajátított tudásszintjének felmérése, gyakorlati problémamegoldó képességük megismerése.

MIT? MILYEN MÉLYSÉGIG? A TANTÁRGYI PROGRAM

A tantárgyi program összeállításakor nem kis dilemmát okoz, hogy az informatikai tananyagok, műveltségi területek milyen speciális részeit és milyen mélységig tanítsa meg az informatika-oktatásra vállalkozó szakember, illetve tanár?

Gyorsan változó világunk és a globalizáció, az Informatika-oktatást is komoly kihívások elé állította. Magyarország esetében is egyértelművé vált, hogy a NATO és az Európai Unió tagjaként csak akkor maradhatunk versenyképesek a társországokkal szemben, ha korszerű, az információs technológiák rohamos fejlődésével lépést tartó, versenyképes tudást tudunk közvetíteni a felhasználók/tanulók felé. Ha a tudást nem csupán egy lexikális adathalmazzal azonosítjuk, hanem olyan aktív készletnek tekintjük, amely az összefüggések rendszeréből táplálkozik.

A felhasználó/tanuló fejlődéséért felelősséget vállaló oktatónak/tanárnak arra kell törekednie, hogy felkészítse a felhasználót/tanulót a gazdasági, társadalmi folyamatokban való aktív részvételre, ami napjainkban kizárólag magas színvonalú, elmélyült, gyakorlat-orientált informatikai oktatás mellett valósítható meg. Természetesem az informatika gyakorlati alkalmazásakor a szinte korlátlan lehetőségeken túl, az előbbiekben bemutatottak szerint, nem feledkezhetünk meg arról, hogy a romboló célú alkalmazhatósága komoly veszélyeket is hordoz. Ezzel együtt és mindenekelőtt tekintettel arra, hogy az informatikai eszközök és tudás alkalmazása normális mindennapjaink elengedhetetlen részévé vált, szükség van egyfajta kompromisszumos megoldásra a tanterv kidolgozása terén.

Véleményem szerint ez a kompromisszumos megoldás egy **„két szinten" történő probléma-megközelítést** igényel. Jelen írás rövid terjedelme nem teszi lehetővé ennek részletes kidolgozását, ezért alapvetően csak az irányok meghatározására szorítkozik.

AZ ELSŐ SZINT

Az első szintet a **tömegek elérését célzó szintnek** is nevezhetjük. Először is, a távoktatás a számítógépes bűnözés általános veszélyeinek, a megelőzésnek, az elhárításnak, illetve az esetleges károk reparálásának a nagy tömegekkel való megismertetéséhez a lehető legszélesebb mértékben alkalmas. Ezért, illetve ennek érdekében indokolt és szükséges a távoktatás legkorszerűbb módszereit alkalmazni, azaz, a legkorszerűbb tananyagokat kifejleszteni és terjeszteni. Amikor nagy tömegekről beszélünk, ennek azért van rendkívüli jelentősége, hogy tudatosuljon az informatika tömeges, mindennapi használói számára az „informatikai hirosimák és nagasakik", az „informatikai piszkos bombák" veszélye és ártalmassága, megelőzésük és kivédésük fontossága.

Ha például az informatika oktatás során a feldolgozandó téma **az elektronikus adatfeldolgozó és adatátviteli rendszer,** akkor a rendszer felépítésének, működésének ismertetése nem lehet teljes körű a rendszerbe történő illetéktelen belépés módozatainak, hatásainak ismertetése, megvitatása nélkül. Az oktatónak szakmai, de nevelési célzattal is fel kell vetnie a "jó hacker" és „rossz hacker” kérdést [4], meg kell vitatnia a felhasználókkal/tanulókkal a rendszerbe történő jogszerű/illetéktelen belépés direkt és indirekt előnyös/kártékony hatásait. Felelősen állást kell foglalnia a „hacker munkáról”, be kell mutatnia és kommentálnia kell az eseteket: például a jó hacker letörli a gyűlöletkeltésre alkalmas uszításokat, a szélsőséges politikai és vallási nézeteket tükröző képeket, a kábítószer fogyasztását vagy a bombakészítést népszerűsítő oldalakat, a valóságos háborúkat rendszeresen kísérő cyber-háborúskodás üzengetéseit, megtévesztő híreit, illetve arról az esetről is amikor „csak egy jó hecc”, „egy jó balhé” [5] kedvéért betör például egy bank informatikai rendszerébe**.** Konkrétan, visszautalva a felvázolt oktatási modell „Tanulás csoportmunkával” szintjére, a „jó hacker”, illetve „rossz hacker” tevékenységének elemzése a filozófiai, az erkölcsi, etikai problémák részletes mélységéig hatolhat. A felhasználók/tanulók állásfoglalásait, véleményeit az oktató/tanár kiegészítheti, az esetleges téves elgondolásokat jó mederbe terelheti. A felhasználó/tanuló és az oktató/tanár közötti személyes kapcsolat megteremti a lehetőségét annak, hogy utóbbi tudatosítsa az előbbiekben, hogy a „jó hacker”, bár beavatkozásával a rendszer tökéletlenségeit kijavíthatja (például a leginkább használt fájlokat könnyebben elérhetővé teheti), a védelmi, biztonsági elemek hiányosságait felfedheti, ugyanakkor bármennyire nemes szándék is vezérli, mégis egy védett rendszerbe lép be jogosulatlanul és azon túl, hogy ezzel vagyoni, de sokszor pénzben ki sem fejezhető kárt okoz a helyi hálózat üzemeltetőjének (a weboldalak újraépítése, a jelszavak, kódok ismételt előállítása), számolnia kell az illetéktelen belépés jogi következményeivel is.

Érheti-e tehát az a vád az informatika-oktatást, az informatika tanárt, a távoktatási anyag készítőjét és terjesztőjét, hogy segíti a „fehérkalapos” bűnözés [4] terjedését?

A kompromisszumos megoldás ezen első szintjének esetében, amennyiben a számítógép, a programok és az adatok ellen véghez vitt intellektuális támadásokat, a programok és információhordozók jogosulatlan megszerzését, másolását, a bankkártyákkal történő visszaéléseket, a mobiltelefonokhoz tartozó SIM-kártya manipulálását, valamint az interneten elkövethető, azokon megjeleníthető jogellenes cselekmények oktatásának részleteit elutasítja, de az ellenük való védekezési módokat hangsúlyosan beépíti a tananyagba, akkor a jó célt tartva szem előtt, közvetlenül nem kell tartania a megvádolhatóság veszélyétől, miszerint a „fehérkalapos” bűnözést segíti.

Ezen első szint vonatkozásában szükséges külön kitérni azon szempont fontosságára, miszerint az oktatásnak elengedhetetlenül ki kell terjednie a tudatos Internet használatra. Az Internet által az emberi közösségek számára kitárul a világ, bárki számára hozzáférhetővé válnak addig ismeretlen, vagy nehezen hozzáférhető információk, felgyorsul a kommunikáció. Az Internet hihetetlen lehetőségek tárát nyitja meg, amely újfajta gondolkodást igényel a felhasználóktól, és erre az újfajta gondolkodásmódra való felkészítésben az oktatásra különös feladat hárul. Ezzel együtt, az Internet a számítógépes bűnözés „táptalaja”: az Internet segítségével világszerte, nehezen ellenőrizhető módon, nagy gyorsasággal lehet elkövetni számítógépes bűncselekményeket. [5]

Amennyiben áttekintjük a számítógépes bűnözés fejlődését, észrevehetjük, hogy míg a technika és a szakképzés nem vált tömegessé, addig nem is ölthetett olyan méreteket, mint napjainkban.

Az Interneten végrehajtott támadások napjainkig egyelőre főleg helyi jellegűek voltak, határozott és pontos célokkal, csak néhány esetben fordultak elő globális méretű kihatások, illetve nagyobb közösségeket, vagy a globális társadalmat jelentős mértékben érintő katasztrófa-következmények, ám a jövőben – pusztán az Internet egyre gyorsuló, globális elterjedésével és széles körű használatával párhuzamosan – az „Internet-oldali fenyegetettség", az „Internetes piszkos bombák" szaporodásának a veszélye növekszik. Nem zárható ki például, hogy több támadás ér majd olyan rendszereket, amelyek létfontosságú infrastruktúrák, katasztrófavédelmi és pénzügyi létesítmények működését támogatják.

Mindez megköveteli, hogy a jövőben, az oktatásban, ezen belül a távoktatási keretek között kellő hangsúlyt kapjon a számítógépes bűnözés elleni védekezés, mivel az emberek csak kellő informáltság mellett képesek felkészülni az ellenük irányuló támadásokra.

A MÁSODIK SZINT

A megközelítés általam javasolt második szintjén azokról **az érzékeny ismereteket jelentő legszofisztikáltabb és legmélyebb informatikai technológiákról és tudásról**, illetve mindezek megfelelő alkalmazásáról van szó, aminek elérhetőségét kizárólag és szigorúan csak az illetékes, arra feljogosított személyek részére kívánjuk biztosítani. Ezen szint esetében a távoktatásos megoldásokat – megítélésem szerint – csak korlátozott mértékben indokolt és szabad alkalmazni.

Álláspontom alapja az a tény, hogy korunkban, az információs társadalom korában megnőtt az információs támadásokkal való fenyegetés és bekövetkezésének veszélye. Az információs terrortámadások és agressziók olyan reális veszélyforrások, amelyek elleni védekezés csak országos (*sőt, globális*) szinten lehet hatékony [6]. A megelőző intézkedések megtételében, a veszélyhelyzetre való felkészülésben, az elhárításban a katonai-védelmi szféra felelőssége megkérdőjelezhetetlen. Az információs társadalom reális elvárása tehát, hogy a katonai szférában az informatikai oktatás programjából ne hiányozzanak a kritikus információs infrastruktúrák [7] [8], a kritikus infrastruktúrák elleni lehetséges támadások témakörei [9].

Ennek kapcsán sokszor felvetődik a kérdés: a távoktatás módszereivel kezelhető-e a szuper érzékeny informatikai ismereteknek és tudásnak – például a kritikus infrastruktúrák informatikai veszélyeztetési módszerei, technológiája, konkrét célpontok stb. – az illetékesekhez való eljuttatása? Véleményem szerint, az ilyen típusú ismeretanyagnak a távoktatásos átadása, még a legkifinomultabb megbízhatósági kritériumokhoz igazított zártkörű felhasználói környezetben is, mindenképpen kockázatosabb a hagyományos tantermi oktatási körülményekkel szemben. Bármilyen szűk körű ugyanis egy hálózat és bármilyen erős biztonsági kritériumokkal is látják azt el, annak puszta léte kockázatnövelő tényezőként jelentkezik. Egyrészt, a virtuális körülmények talaján megnövekszik az információbirtokosoktól történő esetleges információkijutás/kijuttatás veszélye. Ezt mutatja a már hivatkozott Owen-botrány, de még számtalan hasonló esetre lehetne utalni. Másrészt, egy ilyen távoktatási hálózat kialakítása esetén, pótlólagos kockázatként automatikusan megjelenik a külső behatolás veszélye is.

Ezzel együtt a második szinten is lehetnek olyan területek, amelyek a távoktatás eszközeivel kezelhetők, például a már bekövetkezett kritikus infrastruktúrák elleni támadások elemzése, vagy a már publikussá vált, a szakma képviselői számára már elérhető – bizalmas információ-átadást nem jelentő – információk, technikai, technológiai kérdések megvitatása.

Véleményem szerint, az oktatási koncepció analóg kell legyen a 21. századi hadviselésben bekövetkezett változásoknak megfelelően kialakított katonai doktrínákkal [6]:

ahogy az új hadviselési modellben különös figyelmet kap a kritikus infrastruktúrák, a számítógépes hálózatok védelme, a nemzetközi terrorizmust nyíltan vagy burkoltan támogató országok aszimmetrikus csapásainak elhárítása, úgy a katonai informatikai oktatás témaköreinek palettájáról sem hiányozhatnak ezek a témakörök.

.

ÖSSZEGZÉS

Ma, az információs társadalom – a tudomány eredményeinek intenzív és folyamatos felhasználására alapozott társadalom – korában, az informatika-oktatásban új típusú oktatási modellre van szükség. A „high-tech" kultúra, az informatikai és számítógép-hálózati alapú termelés, szolgáltatás, egyéni és közösségi életvitel, azaz a fejlett számítógépes technika társadalmi beágyazódása új kihívások elé állítja az oktatást.

Az informatika-oktatásnak jelentős szerepe van abban, hogy a fiatalok a társadalom hasznos tagjaivá váljanak, sikeres, elégedett életet éljenek. Ennek megfelelően egyfelől olyan tartalmat kell közvetítenünk a felhasználók/tanulók felé, amelynek gyakorlati haszna megkérdőjelezhetetlen, amelyet az élet legkülönbözőbb területein hasznosítani tudnak, másfelől törekednünk kell olyan gondolkodásmód kialakítására, amely az állandó változásokhoz képest időálló, képes azokkal együtt haladni, képes azokra gyorsan reagálni.

A technika fejlődésével megjelenő legmodernebb jogsértéseket, informatikai bűncselekményeket a hagyományos tantermek falait áttörve, a nyitott, virtuális teremben, a távoktatás keretei között is lehet, sőt a Life Long Learning, illetve a Life Wide Learning követelményeként szükséges is oktatni, de a megvalósítandó feladatoknak, célkitűzéseknek védelmi szempontúaknak kell lenniük.

A védekezés orientáltság dominanciáján túl, az érzékeny, speciális ismereteket, intellektust igénylő módozatok oktatása terén, pedig egyelőre a tradicionális képzési megoldások képesek biztosítani az elvárt biztonsági követelményeket. E területen tehát az e-learning hálózatok alkalmazása felé csak nagyon korlátozott és kontrollált szinten indokolt elmozdulni.

Oktatási intézményeinkkel, illetve rendszereinkkel szemben fontos elvárás, hogy a fiataloknak egyrészt magas szintű, az üzleti életben is hasznosítható informatikai ismereteket oktassanak, másrészt, hogy kiemelt hangsúlyt fordítsanak az információbiztonsági műveletek oktatására.

Az oktatásnak a cyber-terrorizmus nemzetközivé válásával is lépést kell tartania. A számítógépes hálózatok világméretűvé válásával ugyanis nem zárható ki, hogy illetéktelenek bármilyen távolságra lévő hivatal vagy intézmény bármilyen adatállományához hozzáférhetnek, ami egyrészt növeli a bűncselekmények veszélyét, másrészt felhívja a figyelmet a bűnüldözés nemzetközi összefogásának szükségességére, ami a képzést is újabb és újabb feladatok elé állítja.

Felhasznált irodalom

[1] Hanka László - Dr. Vincze Ádám - Dr. Solymosi József: A nukleáris terrorizmus, mint potenciális fenyegetettség napjainkban, ZMNE, Hadmérnök, On-line tudományos folyóirat, II. évfolyam, 4. szám, 2007. december, ISSN 1788 1919 p.: 4-24

[2] Szegediné Lengyel Piroska: Ötven éves a távoktatás? Hadmérnök On-line tudományos folyóirat, V. évfolyam, 3. szám. 2010. szeptember, ISSN 1788 1919 p.: 246-263

[3] Szegediné Lengyel Piroska: Élménypedagógia a virtuális térben, Selye János Egyetem „Társadalmi jelenségek és változások” II. Nemzetközi Tudományos Konferencia Tanulmánykötet, CD, Komárno, 2010

[4] Kovács László: Az információs terrorizmus eszköztára, ZMNE, On-line tudományos folyóirat, Különszám, 2006. november. ISSN 1788 1919 http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html (letöltés: 2010. április 07.)

[5] Szegediné Lengyel Piroska: Fiatalok a cyber-térben, Hadmérnök On-line tudományos folyóirat, V. évfolyam, 2. szám. 2010. június, ISSN 1788 1919 p.: 366-379

[6] Dr. Várhegyi István, Dr. Haig Zsolt, Dr. Kovács László: Információs műveletek, Multimédiás tananyag, CD-ROM, ZMNE, 2005

[7] Dr. Kovács László: Kritikus információs infrastruktúrák, ZMNE, Egyetemi jegyzet, CD, Budapest, 2007

[8] Dr. Kovács László: Kritikus információs infrastruktúrák, ZMNE, Multimédiás oktató program, CD, Budapest, 2007

[9] Kovács László, Krasznay Csaba: Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság, III. évfolyam. 1. szám. 2010. február ISSN 1789-5286 p.: 44-56.

[10] http://www.cbsnews.com/8301-504763_162-20018888-10391704.html

[11] http://www.lengyelpiroska.hu/elkonyv.html