NEMZETI
KÖZSZOLGÁLAT
EGYETEM
A HAZA SZOLGÁLATÁBA

Humánvédelem - békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése

(Tanulmánygyűjtemény I., e-book)

[Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar] | [2016]

Nemzeti Közszolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar

Szerzők:
© Kállai Attila – Krajnc Zoltán – Kristóf Zoltán – Szűcs Pál – Kalmár István – Csengeri János – Szabó Csaba – Horváth Tibor – Katona Zoltán – Varga Zsolt – Földi László – Halász László – Petró Tibor – Horváth Attila – Bányász Péter – Derzsényi
Attila – Boldizsár Gábor – Bolgár Judit – Holndonner Hermann – Für Gáspár – Tuba Zoltán – Körmös Csaba

Kiadja:

Lektor: Horváth J. Csaba

Olvasószerkesztés, tördelés:
Csengeri János - Krajnc Zoltán

ISBN 978-615-5305-34-4ö
978-615-5305-35-1

TARTALOMJEGYZÉK

Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai

Bevezető gondolatok

A 2001. szeptember 11-ei terrortámadás sorozat közvetett hatása miatt napokra lebénult az Egyesült Államok külkereskedelmi forgalma. A tragikus eseménysorozat egyben rávilágított a globális gazdaság sérülékenységére. Ezt követően mind az USA-ban, mind pedig az Európai Unióban felértékelődtek az ellátási láncok kockázataival és biztonságával kapcsolatos kutatások. Chickán Attila és Gelei Andrea az ellátási láncot értékteremtő folyamatok és erőforrások összehangolt rendszereként értelmezi, amely több vállalatot érintve az alapanyagok beszerzésével kezdődik és a végtermék fogyasztóhoz történő eljuttatásával fejeződik be. Részét képezik a beszállítók, a gyártók, logisztikai szolgáltatók, raktárak és a disztribúciós folyamatok egyéb szereplői is. Működését elsősorban a végső fogyasztók igényei határozzák meg, közös érdekeltséget teremtve a lánc résztvevői számára.[1]

Az ellátási láncok zavartalan működésében minden állam érdekelt. A beszerzési, termelési, elosztási és értékesítési helyek térbeni és időbeni dekoncentrációja követelte meg az ellátási lánc menedzsment személet elterjedését, egyben érzékenyebbé és sérülékenyebbé tette a reálgazdasági folyamatokat. A felsorolt hatások alól egyetlen ország sem képes kivonni magát.

Az utóbbi években a témával összefüggő kutatások az Európai Unióban és a NATO-ban is felértékelődtek. A kutatási téma fontossága ellenére Magyarországon az ellátási láncok biztonságával kapcsolatban komplex, tudományos igényű elemzések terén jelentős hiátusok mutatkoznak. Az elemzések és a vizsgálatok magyarországi elterjesztése a gazdaság- és nemzetbiztonsági érintettség mellett társadalmi szempontból is szükségessé válik. Az ellátási láncok biztonsága olyan területeket érint, mint a közigazgatás, egészségügy, az élelmiszer és vízellátás, infokommunikációs eszközök vagy az energetika.

A nemzetközi szakirodalom és a mindennapi gyakorlati tapasztalatok egyértelműen igazolják, hogy az ellátási láncokhoz kapcsolódó logisztikai folyamatok biztonsága közvetlenül hat a globális gazdaság működésére.[2] A kutatási probléma egyben

---

[1] Chikán, Attila- Gelei, Andrea: Az ellátási láncok és menedzsmentjük In. Harvard Business Manager (magyar kiadás), 2005. január, pp. 35-44.

[2] Horváth Attila: Az anyagáramlással összefüggő logisztikai folyamatok terrorfenyegetettségének jellemzői, In: Tompáné Daubner Katalin, Miklós György, Miklósné Zakar Andrea, Balázs Judit (szerk.), Tudomány határok nélkül. Konferencia helye, ideje: Kalocsa, Magyarország, 2008.11.27- 2008.11.28. Kalocsa: Tomori Pál Főiskola, 2008. pp. 201-208.

gazdaságbiztonsági kérdés, a katonai ellátási lánc vizsgálata pedig nemzetbiztonsági és rendvédelmi szemszögből is értelmezhető.[3]

Az infokommunikációs technológiák napjainkban tapasztalt elterjedése új típusú kihívásokat generál, amelyekre a komplex értelmezés szükségességén[4] túl újfajta szemléletet is megkövetel az ellátási lánc biztonságával foglalkozó szakértőktől a polgári és katonai területen egyaránt. A „dolgok internete", amellett, hogy merőben új kihívásokat fog jelenteni a jövőben, úgy a klasszikus kockázatokat is újra kell értelmeznünk. Ennek megfelelően tanulmányomban azoknak az informatikai kihívásoknak a bemutatására törekszem, amelyek az ellátási lánc biztonságát fenyegetik a szervezett bűnözői csoportok részéről.

A szervezett bűnözés, mint biztonságpolitikai fenyegetés

A hidegháború lezárásával a biztonsági fenyegetések alapvetően alakultak át. Míg az ezt megelőző időszakban a két nagyhatalom, az USA és Szovjetunió kiélezett szembenállása jelentette a fő kihívást, addig mára a „gyenge" államok váltak a biztonságpolitikai gondolkodás fő érdeklődési területévé. A „vasfüggöny" lebontása, ezáltal a határok szabad átjárhatósága, a globalizáció térnyerése felgyorsította az áruk, szolgáltatások és személyek határon átívelő mozgását. Ez azonban magában foglalta azt a veszélyt is, hogy a különböző negatív jelenségek (például terrorista és szervezett bűnözői csoportok tagjai) is szabadabban vándorolhattak az egyes országhatárokon át. A Szovjetunió felbomlásával az is kiderült, egyes utódállamok nem készültek fel az önálló államiságra. Ez a fajta gyengeség a különböző globális hatású biztonsági fenyegetések melegágyul szolgáltak. Kihasználva az állam tehetetlenségét, számos szervezett bűnözői csoport erősödött meg, óriási vagyonra szert téve, többek között kábítószer- kereskedelemből.

Amikor szervezett bűnözésről beszélünk, gyakran a maffia elnevezéssel illetjük. Ez a kifejezés terjedt el a köznyelvben, a szenzációhajhász újságírói, politikai vagy közigazgatási nyelvezetet használók esetében. Szükségesnek mutatkozik tehát a definíció meghatározása mellett a fogalmi különbségtétel is.

Úgy tűnik, a „maffia" szó először egy 1658-as keltezésű írott szicíliai szövegben jelenik meg, de a XIX. század Itáliájában válik közismertté. Jelenleg két értelemben is

[3] A biztonság fogalmának fejlődéséről, a biztonságot veszélyeztető tényezők osztályozásáról bővebben lásd: Zán Krisztina „Az Európai Unió biztonság és védelempolitikája" című cikkét a Határrendészeti Tanulmányokban (Zán Krisztina: Az Európai Unió biztonság és védelempolitikája, In. Határrendészeti Tanulmányok 2004:(2) pp. 99-117., 2004.), illetve a „Még néhány gondolat a biztonságról" című cikkét a Pécsi Határőr Tudományos Közleményekben (Görbe Attiláné Zán Krisztina: Még néhány gondolat a biztonságról, In. Pécsi Határőr Tudományos Közlemények, pp. 185-190., 2006.

[4] Horváth, Attila: Hogyan értessük meg a kritikus infrastruktúra komplex értelmezésének szükségességét és védelmének fontosságát? In. Hadmérnök 5:(1) pp. 377-386. , 2010., és Horváth Attila, Csaba Zágon: On the Vulnerability and Reliability of Towns and Cities, In: Csapó T, Balogh A (szerk.), Development of the Settlement Network in the Central European Countries: Past, Present, and Future. 314 p., Berlin; Heidelberg: Springer Verlag, 2012. pp. 299-312.

használják: elsősorban a Szicília területén kialakult és az ottani történelmet végigkísérő bűnözői csoportot jelenti, másodsorban pedig használják minden olyan, bűnözőkből álló csoportosulás körülírására, mely belterjes, zárt és erőszakos módon szoros kapcsolatokat épít ki egy viszonylag jól körülhatárolható földrajzi területtel és annak népességével.

A szakirodalom – és a területtel foglalkozó rendőrök – egyre gyakrabban használnak egy viszonylag új szóösszetételt, mely a „maffia" szóhoz viszonyítva tágabb területet ölel fel: ez a szervezett bűnözés. Az amerikai eredetű „organized crime" – amelyet a különféle nemzetiségű kutatók együttes munkájának eredményeként egyre gyakrabban használnak Európában, gyökeret vert a magyar nyelvben is. Jelentése nagyjából megegyezik a „maffia" szóéval, legalábbis ami az összetevőit és a hátterét illeti. Az első, szervezett bűnözésről tartott nemzetközi kollokvium résztvevői 1988 májusában, Saint-Cloud-ban egy ideiglenes meghatározást fogadtak el. Eszerint a szervezett bűnözéshez tartozik „*minden olyan vállalkozás vagy minden olyan emberi csoportosulás, mely folytonos, törvénytelen tevékenységet folytat haszon elérése érdekében, nem véve tudomást az országhatárokról*".[5] A szervezett bűnözés fogalmának meghatározására többen kísérletet tettek, ez a szám eléri a 180-at.[6]

Resperger István fogalmi meghatározását alapul véve „*a szervezett bűnözés, foglalkozás, egzisztenciateremtő jellegű, magas fokú konspirációt mutató társulásos bűnelkövetési módszer. Bűnözés, amely legális vállalkozásokba, esetenként a közhatalomba is behatol, és szükségszerűen felhasználja a korrupciót, mivel a bűnözők számára csak két eszköz áll rendelkezésre: az erőszak vagy a korrupció*".[7] A korrupció valójában az erőszak alternatívája, ezért számos országban a korrupció kutatását a kriminológusok, szociológusok, ill. gazdasági szakértők mellett, speciálisan képzett szakemberek végzik. A szervezett bűnözés jellemzőit a szerző az alábbiakban határozza meg:

1. szigorú belső fegyelem, konspiráció és gyakran erőszak jellemzi;
2. szervezeti felépítését tekintve hierarchikusan tagolt;
3. esetenként nemzeti, etnikai, családi alapokon szervezett;
4. az illegális tevékenység fedezésére legális vállalkozásokat tartanak fent;
5. az illegális jövedelmeket – többnyire a saját befolyása alatt tartott – pénzintézeti vonalakon legalizálják;
6. az illegális gazdasági struktúra működtetése érdekében illegális hatalmi struktúrát hoznak létre;
7. a működés és működtetés érdekében befolyásra törekszenek a közigazgatásban (engedélykiadó hatóságok), az államapparátusban (például

[5] Glorieux, Patrick: Európai szervezett bűnözés és a maffia-típusú csoportok: az általuk képviselt fenyegetés és az erre adandó válasz rövid helyzetjelentése, Belbiztonsági Felső Tanulmányok Intézete, IHESI, 1993.

[6] Lampe von, Klaus: Definitions of Organized Crime, http://www.organized-crime.de/organizedcrimedefinitions.htm (2014.11.05.)

[7] Resperger, István: Kockázatok, kihívások, fenyegetések a XXI. században, Az Országos Kiemelt Kutatási Tanulmányok pályázata, Budapest, 2002.

koncessziók elbírálása), a jogalkalmazásban, bűnüldözés területén, valamint a jogalkotásban és a politikai életben;

8. a bűnöző szervezetek hatalmi pozícióik érvényesítése, megtartása, kiterjesztése céljából pszichikai és/vagy fizikai erőszakot alkalmaznak (zsarolás, emberrablás, fenyegetés, leszámolásos emberölések, terrorcselekmények).

Magyarország érvényben levő Nemzeti Biztonsági Stratégiája a következők szerint fogalmaz: *„A szervezett bűnözés, különösen annak a határokon átnyúló súlyosabb formái– a társadalmi-gazdasági átalakulás bizonytalanságait kihasználva – növekvő kihívás elé állítják a társadalmat, valamint az érintett rendvédelmi és igazságügyi szektor működését. A szervezett bűnözői csoportok igyekeznek legális gazdasági tevékenységüket és befolyásukat növelni, továbbá érdekeiket a gazdasági szférán túl is érvényesíteni. A szervezett bűnözés elősegíti a nemzetgazdaságot hátrányosan érintő fekete- és szürkegazdaság fennmaradását,a korrupció különböző eszközeivel élve korlátozza a piaci versenyt. A szervezett bűnözés igyekszik összefonódnia bűnüldözéssel, rendvédelmi szervekkel, az igazságszolgáltatással, ezek működését torzíthatja, és akár működésképtelenné is teheti. A bűnszervezetek célcsoporttá tették az államigazgatási és rendvédelmi szervek tagjait, továbbá kísérletet tesznek a politikai döntéshozatalba való beszivárgásra is*”.[8]

A kormányzati szervek, a média előszeretettel tesz egyenlőségjelet a maffia és a kábítószerekkel összefüggő bűncselekmények között, ezáltal beleesve abba a hibába, hogy nem vesz tudomást – pesszimistább interpretáció szerint nem akar tudomást venni- olyan újszerű bűncselekményfajtákról, mint például a humanitárius segélyek eltérítése, az állami támogatásokkal és szubvenciókkal történő csalások, a nukleáris technológiával való visszaélések, a bűnüldöző szervezetekbe történő beépülések, stb.. A harmadik világ államapparátusába történő beépülés, a végrehajtó hatalmi ág bizonyos részeinek kisajátítása, a törvényhozói hatalmi ág megkörnyékezése, a korrupció, valamint a bírák megvásárlása valóságos szabadrablásos helyzetet teremtett számos államban.

A kábítószer kereskedelem mellett óriási bevételre tesznek szert a fegyvercsempészetből, az emberkereskedelemből, jövedéki termék (például cigaretta) illegális kereskedelméből. Ezek a tevékenységek tökéletesen példázzák, miért is jelent akkora fenyegetést a szervezett bűnözés, hiszen önmagukban is destabilizálhatnak egy országot, egy térséget (különösen a fegyverkereskedelem), ronthatják a lakosság fizikai, egészségi és anyagi helyzetét (drogcsempészet), és az emberi jogok súlyos megsértését eredményezhetik (emberkereskedelem), ráadásul sokszor erőszakos cselekményekkel járnak együtt. Mindezek mellett megjelentek azok az új típusú bűnelkövetési formák, amelyek a kibertérhez kapcsolódnak. Összefoglalva tehát a társadalom normális

[8] A kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti biztonsági Stratégiájáról http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf (2014.11.05.)

működését sodorják veszélybe ezek a cselekmények, ami indokolja az ellenük való fellépés szükségességét. Ez mindenképpen nemzetközi összefogást igényel, hiszen, ahogy a fenti megfogalmazásokból is világosan kiolvasható, a szervezett bűnözés magát a tevékenységet, és sokszor a hatásait tekintve is átnyúlik a határokon.

Az infokommunikációs technológiák elterjedtsége és szerepe

Infokommunikációs technológiák alatt olyan eszközök, technológiák, innovatív folyamatok összességét értjük, amelyek az információközlést, feldolgozást, annak áramlását és kódolását hatékonyabbá és gyorsabbá teszik (például informatikai eszközök, technológiák). A 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről[9] az infokommunikációs technológiákat létfontosságú rendszerelemként azonosítja (lásd 1. számú táblázat). Nevezett jogszabály alapján *„[létfontosságú rendszerelem]…mellékletben meghatározott ágazatok valamelyikébe tartozó eszköz,*[10] *létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna*”.

FSZ	Ágazat	Alágazat
1.	Energetika	villamosenergia-rendszer létesítményei (kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek)
		kőolajipar
		földgázipar
2.	Közlekedés	közúti közlekedés
		vasúti közlekedés
		légi közlekedés
		vízi közlekedés
		logisztikai központok
3.	Agrárgazdaság	mezőgazdaság
		élelmiszeripar

[9] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Magyar Közlöny, Magyarország hivatalos lapja. 2012. évi 154. szám

[10] Ezek az ágazatok: energia, közlekedés, agrárgazdaság, egészségügy, pénzügy, ipar, infokommunikációs technológiák, víz, jogrend- kormányzat, közbiztonság- védelem.

		elosztó hálózatok
4.	Egészségügy	aktív fekvőbeteg-ellátás
		mentésirányítás
		egészségügyi tartalékok és vérkészletek
		magas biztonsági szintű biológiai laboratóriumok
		egészségbiztosítás informatikai rendszere
5.	Pénzügy	pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei
		bank- és hitelintézeti biztonság
		készpénzellátás
6.	Ipar	veszélyes anyagok előállítása, tárolása és feldolgozása
		veszélyes hulladékok kezelése és tárolása (kivéve radioaktív hulladékok kezelése és tárolása)
		hadiipari termelés
		oltóanyag- és gyógyszergyártás (kivéve nukleáris létesítmények)
7.	Infokommunikációs technológiák	információs rendszerek és hálózatok
		eszköz-, automatikai és ellenőrzési rendszerek
		internet-infrastruktúra és hozzáférés
		vezetékes és mobil távközlési szolgáltatások
		rádiós távközlés és navigáció
		műholdas távközlés és navigáció
		műsorszórás
		postai szolgáltatások
		kormányzati informatikai, elektronikus hálózatok
8.	Víz	ivóvíz-szolgáltatás
		felszíni és felszín alatti vizek minőségének ellenőrzése
		szennyvízelvezetés és -tisztítás
		vízbázisok védelme
		árvízi védművek, gátak
		kormányzati rendszerek, létesítmények,

9.	Jogrend – Kormányzat	eszközök
		közigazgatási szolgáltatások
		igazságszolgáltatás
10.	Közbiztonság – Védelem	rendvédelmi szervek infrastruktúrái
		honvédelmi rendszerek és létesítmények

1. számú táblázat Létfontosságú rendszerelemek ágazati besorolása a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény alapján

Megítélésem szerint a 2080/2008. (VI. 30.) Korm. határozat[11] definíciójával jobban meg lehet ragadni a létfontosságú rendszerelemek[12] jelentőségét: *„…azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére”.*

Ahogy Cory Doctorow író, blogger és aktivista találóan megfogalmazta, az internet a 21. század idegrendszere.[13] Életünk szinte minden szegmensében jelen van valamilyen formában. Az információs forradalom lezajlásával az infrastruktúrák irányítása szinte teljes egészében infokommunikációs technológiák segítségével történik, úgy is mint:

- „energiaellátó rendszerek rendszerirányító infokommunikációs hálózatai;
- infokommunikációs hálózatok;
- közlekedés szervezés és irányítás infokommunikációs hálózatai;
- vízellátást szabályzó infokommunikációs hálózatok;
- élelmiszerellátást szabályzó infokommunikációs hálózatok;
- egészségügyi rendszer infokommunikációs hálózatai;
- pénzügyi gazdasági rendszer infokommunikációs hálózatai;
- ipari termelést irányító infokommunikációs hálózatok;
- kormányzati és önkormányzati szféra infokommunikációs hálózatai
- védelmi szféra infokommunikációs hálózatai”.[14]

Az ily mértékű infokommunikációs technológiáktól való függés bekövetkezte előtt az országhatárok bizonyos fizikai korlátot jelentettek az infrastruktúrák ellen elkövetett támadásokkal szemben, azonban az internet lehetővé tette ezen eszközök országhatáron túlnyúló fenyegetésének lehetőségeit, mindezt viszonylag alacsony költségek mellett realizálva. Léteznek olyan vélemények, mely szerint nem kellett

[11] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról, In. Határozatok Tára, 31. szám, Budapest, 2008. június 30.
[12] A 2080/2008. (VI. 30.) Korm. határozat még kritikus infrastruktúraként nevesítette.
[13] BERTA, Sándor: Az internet a 21. század idegrendszere, In. SG, 2013. május 10., http://www.sg.hu/cikkek/97219/az_internet_a_21_szazad_idegrendszere (2014.11.10.)
[14] Haig, Zsolt- Kovács, László et. al.: A kritikus információs infrastruktúrák meghatározásának módszertana, ENO Avisory Kft., 2009.

volna az internetre kötni a kritikus infrastruktúrákat, mert ezzel megnyitották az utat a kibertérből érkező fenyegetéseknek.[15] A vállalatok joggal, a költségek csökkentésének egy módját látták ebben az eljárásban, azonban ez olyan biztonsági kockázatokat jelent, amik alapjaiban veszélyeztetik a szolgáltatások megfelelő működését. Ahogy a fenti felsorolásból láthattuk, a kritikus infrastruktúrák mindegyike használja (és egyúttal erősen függ tőle) az infokommunikációs technológiákat.

Ahogy a fenti felsorolásból láthattuk, a kritikus infrastruktúrák mindegyike használja (és egyúttal erősen függ tőle) az infokommunikációs technológiákat. Ez a függőség olyan mértékű, hogy az infokommunikációs technológiának, mint kritikus infrastruktúrának megsérülése, kiesése súlyos következménnyel járna a többi kritikus infrastruktúra működésére egyaránt. Ilyen mértékű függést csupán az energiaszolgáltatás, mint kritikus infrastruktúra jelent. Amennyiben elfogadjuk ezt a megállapítást, akkor egyenesen következik, hogy pl. egy állam mobil távközlő hálózata önmagában is kritikus infrastruktúrának minősül.

Több tanulmány mutatta ki, hogy az internet jelentős mértékben hozzájárul a gazdasági növekedéshez. Ez alatt nem csak a reklámbevételeket, az e-kereskedelmet és az egyéb, világhálón keresztül lebonyolított tranzakciókat, illetve az internethez köthető gazdasági tevékenységeket kell érteni, hanem az internet elterjedése, sőt, magának a kapcsolatnak a sebessége is jelentős hatással van a GDP növekedésére. Egy, az Ericsson, az Arthur D. Little és a Chalmers University of Technology által 33 OECD-tagországban végzett felmérése kimutatta,[16] hogy egy országban a szélessáv-penetráció 10 százalékkal történő növelése közvetve nagyjából 1 százalékkal növeli az éves GDP-t, a kiépített sávszélesség minden egyes megduplázódásakor pedig 0,3 százalékkal növekszik a GDP. Ez a növekedés nem csupán az infrastruktúra kiépítése kapcsán létrehozott állások közvetlen és közvetett gazdasági aktivitásából és a gazdaságban tapasztalható közvetlen hatékonyságnövekedésből fakad, hanem az indukált hatásból is, amely a munkamódszerek és folyamatok a társadalom minden szintjén tapasztalható változásából származik. Ez az indukált hatás a leginkább fenntartható dimenzió, és az említett GDP-növekedésnek akár egyharmadát is kiteheti.

A széles sávú internet-penetráció növekedésével többek közt a távmunka és a rugalmas munkavégzés terjedése, illetve a szolgáltatások bővítése és hatékonyabbá tétele révén számottevően növelhető egy gazdaság termelékenysége. Az infokommunikációs technológia jelentősége sosem volt ilyen nagy, mint most, hiszen távközlés és informatika nélkül ma már elképzelhetetlen az oktatás, az egészségügy, a közlekedés

[15] Napjainkban a kiberfenyegetéseknek négy fajtáját különböztetjük meg: kiberbűnözés, hacktivizmus és kiberterrorizmus, kiberkémkedés, kiberhadviselés. Ez alapján kiberbűnözés céljaként az informatikai eszközökön keresztüli haszonszerzést nevesíthetjük. Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban, In. Hadmérnök VII:(4) pp. 142-151., 2012.

[16] Ericson Press Release: New study quantifies the impact of broadband speed on GDP, In. Ericson, 2011. szeptember 27., http://www.ericsson.com/news/1550083 (2014.11.10.)

vagy a közigazgatás működtetése. Mindezek alapján úgy vélem, kijelenthető, hogy az informatikailag elmaradott települések lemaradnak. Természetesen ezek az elmaradott, felzárkóztatásra szoruló térségek jellemzői, amelyek nem rendelkeznek megfelelő infrastruktúrával. A piaci, de különösen az állami szereplők akkor gondolkodnak helyesen, ha a javak egyenlőségének utópiája helyett a javakhoz való hozzáférés egyenlőségének megteremtésén fáradoznak. Az infokommunikációs technológiában rejlő lehetőségek kiválóan alkalmasak ennek megteremtésére. Egy, a McKinsey & Co. által 2012-ben végzett kutatása szerint[17] Magyarországon az internet 2010-ben 3,9%-al járult hozzá a GDP-hez. Ez 5,1 milliárd dollárt, azaz 1058 milliárd forintot jelent, ami kétszerese pl. a magyar húsiparnak.

Napjainkban, ahogy az Ericsson 2014-ben megrendezett Innovációs Fórumán elhangzott, világszerte nagyjából 7,1 milliárd mobil előfizetés van, amely a Föld lélekszámával megegyező nagyság.[18] Továbbbontva az adatokat 2,9 milliárd szélessávú mobilnet előfizetéssel számolnak a szakértők. A cég számításai szerint 2019-re, tehát öt év múlva 9,1 milliárd előfizetés lesz, és erre jut majd 7,5 milliárd mobilnet-előfizetés, a mobiladat-forgalom pedig a mostani tízszeresére nő. Az ebből következő digitális függőség nem csak az egyszeri felhasználók számára jelent majd exponenciálisan növekvő „netéhséget", hanem a nagyvállalati igények esetében is hasonlóra számíthatunk. Különösen érvényes lesz ez az úgynevezett networked society-ra, azaz a hálózatra kötött társadalomra, amely az okosváros formájában, a „dolgok internetével" még kiszolgáltatottabbá teszi a felhasználót az infokommunikációs technológiáktól.

Az okosváros koncepciója, Orbók Ákos megfogalmazása alapján *„… olyan várost képzel el, amely dinamikusan változtatja funkcióinak végrehajtását a felhasználók igényei szerint. Ezzel együtt a város komplex működését próbálja fenntarthatóan fejleszteni, valamint a lakói számára nyújtott életminőség javítása a célja."*.[19] Az okosváros koncepciója természetesen a „dolgok internete" körül szerveződik, hiszen a fogalom különböző, egyértelműen azonosítható objektumokra, és azok internet-szerű hálózatára utal. Objektumok alatt ez esetben az összes olyan elektronikai eszközt kell értenünk, amely képes valamilyen hasznos információt felismerni, mérni, illetve ezt kommunikálni egy másik eszköz irányába. Jelenleg közel két milliárd ilyen eszköz kapcsolódik az internetre, de becslések szerint 2020-ra megközelíti a 26 milliárd eszközt.[20]

Az okosváros koncepciójának egyik releváns részét képezi a jól működő közlekedés megszervezése, amely nem csak a lakók közlekedési feltételeinek javulását képezi,

---

[17] McKinsey & Co.: Online and upcoming: The Internet's impact on aspiring countries, 2012. január., http://www.mckinsey.com/client_service/high_tech/latest_thinking/impact_of_the_internet_on_aspiring_countries pp. 81-91. (2014. 11.10.)

[18] Vestberg, Hans: Opening Presentation, Tomorrow Transformed – Leading change In. Ericsson Business Innovation Forum 2014.

[19] Orbók, Ákos: Az okosváros közlekedésirányításának kihívásai. In. Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről, Nemzeti Közszolgálati Egyetem, Budapest, 2014., p. 122.

[20] Press Release: Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020, In. Gartner.com, 2013. december 12., http://www.gartner.com/newsroom/id/2636073 (2014.11.11.)

hanem a logisztikai folyamatok eredményességének növelését is. A logisztika klasszikus fogalma anyagok, információk, személyek rendszeren belüli és közötti mozgatásának tudománya. A logisztikai folyamat a megfelelő áru, megfelelő időben, megfelelő helyre, megfelelő mennyiségben, megfelelő minőségben és megfelelő költségek melletti mozgatása. Ahogy ebből is látszik, a kulcsszó a megfelelő, amely egy magas szintű koordinációs folyamat véghezvitelét igényli az ellátási lánc teljes spektrumában. A logisztika ennek megfelelően az ellátási lánc csupán egy részét jelenti, de a logisztikai folyamatok kiesése a teljes ellátási láncot megbénítja.
Magyarország a logisztikai folyamatok informatikai támogatottságát illetően – 2010-es adatok alapján- az EU-s átlaghoz képest határozottan gyengébben szerepel, az átlag 17,9%-hoz viszonyítva hazánkban ez 11,2%-ra tehető.[21] Már pedig egy vállalat életében, beleértve a logisztikai folyamatokat is, az infokommunikációs technológiák használatba növeli a hatékonyságot. Egy megfelelően működő vállalati IT-nek a teljes ellátás lánc mentén kell biztosítania a rendszer működését. E szerint már a beszerzésnél azonosítani kell a vállalkozáshoz került termékek, anyagok körét, kezelnie szükséges a készletek státuszait, a különböző raktárakat, azok kapacitásait, támogatnia kell a kapcsolódó pénzügyi műveleteket és a szállítási módokat, feltételeket. Ehhez számos infokommunikációs eszköz áll rendelkezésre, mint felhő alapú szolgáltatások, GPS alkalmazások, különböző kommunikációs-, integrált vállalatirányítási rendszerek, azonosítási eszközök. A logisztikai rendszer és az ellátási lánc tehát nagymértékben támaszkodik az infokommunikációs rendszerek használatára.
Az informatikai eszközök azonban rendkívül kitettek a kibertérből érkező fenyegetésekkel szemben. Még ha képesek lennénk megalkotni a tökéletesen biztonságos informatikai rendszert, akkor is támadhatóak lennének a humán faktor következtében. A továbbiakban azokat a lehetőségeket vizsgálom, amelyek sebezhetővé teszik az ellátási láncot az informatikai támadásokkal szemben, és kiemelt jelentőségűek a szervezett bűnözői csoportok számára.

A szervezett bűnözés jelentette kockázatok az ellátási lánc informatikai biztonságában

Tanulmányom alapjául egy 2014 novemberében a Nemzeti Közszolgálati Egyetemen elhangzott előadás szolgált, amelyet Horváth Attila és Csaba Zágon kutatótársaim tartottak.[22] A konferencia a Kritikus Infrastruktúra Védelmi Kutatások TÁMOP 4.2.1.B

[21] Kövesdi, Zoltán: Az e-gazdaság helyzete Magyarországon - az Európai Bizottság elemzése, In. Infotér, 2011. július 11., http://www.infoter.eu/cikk/az_e-gazdasag_helyzete_magyarorszagon_-_az_europai_bizottsag_elemzese (2014. 11.11.)
[22] Horváth, Attila- Csaba, Zágon: Az ellátási lánc és a logisztika, mint közlekedési kritikus infrastruktúra - bizonyítás egy esettanulmánnyal, Előadás, „Szervezeti, szabályozási és innovatív változások a létfontosságú rendszerek védelmében” tudományos-szakmai konferencia, Nemzeti Közszolgálati Egyetem, 2014. November 14.

11/2/KMR 0001 számú projekt, „Közlekedési kritikus infrastruktúra védelme" Kiemelt Kutatási Terület szervezésében került megrendezésre, és a KKT közlekedési infrastruktúra, valamint az ellátási lánc biztonságával foglalkozó kutatásainak eredményeit mutatta be.

Bár a kutatásaink kezdetben a közlekedési rendszer sebezhető pontjainak azonosítására és a védelmére fókuszáltak, de hamar be kellett látnunk, hogy a közlekedési rendszer vizsgálata nem végezhető önmagában, komplex, a határterületekre való kiterjesztett elemzést igényel meg. Így jutottunk el az ellátási láncok biztonságához, de ez a szemlélet vezetett el bennünket a kibertér fenyegetettségeinek kutatásához is. Az említett előadás egy esettanulmányt dolgozott fel, amely az antwerpeni kikötő informatikai rendszerében feltárt kibertámadást és az ehhez kapcsolódó nyomozást ismertette.

Az antwerpeni kikötő a konténeres szállítás tekintetében 2012-es adatok alapján 104 millió tonna konténeres árut mozgatott meg. Globálisan a 15. legforgalmasabb kikötőjének számít, Európára vetítve a 3. helyet foglalja el a rangsorban. 2013 októberében az Europol és a Belga Szövetségi Rendőrség sajtótájékoztatón jelentette be egy 2011 júniusa óta zajló nyomozás befejezését, amely a kikötőbe érkezett és onnan továbbított konténerek eltűnése okán indítottak. Az évekig tartó nyomozás kiderítette, hogy szervezett bűnözéshez köthető egyének betörtek a kikötő logisztikai rendszerét irányító informatikai eszközökbe, amelynek segítségével átvették az irányítást a legális szállítási infrastruktúra felett, lehetővé téve, hogy a kiszemelt konténereket a számukra tetszőleges átvételi pontra irányítsák. Az eljárás során álcázott, nehezen észlelhető módosításokat hajtottak végre a számítógépeken, ami magában foglalta a szállításhoz kapcsolódó információk (konténer tartalma), illetve az átvételhez szükséges hitelesítés (PIN kód) megszerzését is. A kiválasztott, értékes konténereket már a kikötőben átvették a meghamisított információk segítségével, és olyan helyre irányították, ahol aztán feltűnés nélkül hozzáférhettek a konténer tartalmához.

A bűncselekmény a kikötői és logisztikai informatikai rendszer megváltoztatása okán egész addig nem válik ismertté, míg az eredeti címzett be nem jelenti a várt konténer hiányát. Az elkövetőek felismerték a módszerükben jelentkező lehetőségeket, amelynek hatására más bűnszervezetekkel kooperálva is felhasználták az informatikai rendszer felett megszerzett irányítást, így biztosítva a küldemények zavartalan szállítását. A nyomozás végül 12 fő őrizetbe vételéhez vezetett Belgiumban és Hollandiában, illetve több tonna kábítószer, kiberbűnözéshez használatos eszközök, 1,3 millió Euró, illetve lőfegyverek lefoglalását eredményezte.

A bűncselekményben megjelent a mára már trendként értékelhető eljárás, amely szerint a bűnözők az interneten kutatnak fel és bérelnek fel szakértőket, akik kellő informatikai tudással rendelkeznek egy kibertámadás végrehajtására. A 2013-as SOCTA- jelentés[23] szerint a kiberbűnözés terén különösen növekszik a „crime as a

[23] Ahogy Urszán József fogalmazta meg, *„A jelentés célja az EU területén aktív bűnszerveztek által a belső biztonságra gyakorolt sokrétű fenyegetés jellemzőinek feltárása. A SOCTA prioritásokat javasol a politikai*

service", azaz szolgáltatásszerű bűnözés modus operandi elsősorban a különleges szakértelem igény okán.[24] Fontos látni, hogy a szolgáltatásszerű bűnözés nem csupán a tengeri kikötőket veszélyezteti, hanem mindenhol érvényes, ahol infokommunikációs technológiákat használnak. Már pedig, napjainkban, ahogy az előző fejezetekben igazoltam, az életünk minden részén jelen vannak, és irányító funkciót töltenek be ezek az eszközök.
A SOCTA- jelentést erősíti az Europol szervezett bűnözés internetes fenyegetését vizsgáló jelentése (továbbiakban IOCTA).[25] A jelentés úgy számol, jelenleg 2,8 milliárd ember használja az internetet, az internetre kötött eszközök száma (okostelefon, tablet, hűtőszekrény stb.) eléri a 10 milliárdot. A korábban citált Gartner kutatás az okoseszközök számát 2 milliárdra becsülte a saját kutatása alapján, ami az Europol által becsült nagysághoz képest mintegy 8 milliárdos eltérést jelent. A különbséget magyarázhatjuk az eltérő mintavétellel, ugyanis míg a Gartner a telefonok, számítógépek, tabletek esetében végezte a kutatást, addig az Europol minden internetre kötött eszközre vonatkoztatta az általa közölt értéket. Látni kell azonban, hogy mindkét kutatás robbanásszerű terjedéssel számol a jövőre nézve. Az Europol, alapul véve az Internet World Stats adatbázisát, úgy becsüli, hogy a világ fejletlenebb régióban az internet hozzáférés elterjedésével növekedni fog a támadások száma. Az EU államok és polgárok így is kiemelt célpontnak számítnak a magas internet-penetráció, a relatív gazdagság, a pénzügyi szektor fejlett internethez kötött működése okán. Mindezek megteremtik a lehetőséget a bűnözők számára, hogy viszonylag kis befektetés nélkül, az országhatárokon átívelő, egyszerre akár nagyszámú áldozatot követelő bűncselekményt, amely sok esetben az egyes államok eltérő jogi szabályozásából eredően tovább bonyolítja a bűnüldözők hatékony fellépésének lehetőségét. Mindehhez, ha figyelembe vesszük, hogy sok esetben a különböző államok támogatják és felhasználják saját céljaik elérése érdekében az egyes hackercsoportokat, még komplexebb problémával szembesülünk.

A fenti állítás alátámasztására két rövid példa szolgál:[26] a 2007-ben lezajlott orosz-észt kiberháború szolgál, illetve a 2008-ban vívott orosz-grúz háború. A 2007-es események indokául egy második világháborús szovjet emlékmű eltávolítása szolgált. A közel egy hónapos DoS-támadások során a bankokat, közintézményeket másodpercenként 100 megabájtos forgalmat generáló támadások érték 178 országból. A támadók célja az

---

döntéshozatal számára, amelyek iránytűként szolgálnak a bűnszervezetek elleni európai küzdelemhez az elkövetkező öt évben.". In. Urszán, József: A szervezett bűnözés fenyegetettség értékelésének jelentősége az Európai Unióban. Pécsi Határőr Tudományos Közlemények 14:1, 2013. http://www.pecshor.hu/periodika/XIV/urszanj.pdf pp. 431-437.

[24] Europol SOCTA 2013, EU Serious and Organised Crime Threat Assessment. Europol, Hága, 2013., https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf, p. 28.

[25] Europol The Internet Organised Crime Threat Assesment 2014., Europol, Hága, 2014., https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf

[26] Bányász, Péter- Orbók, Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében, Hadtudomány Online 23/1.,2013., pp. 188-209.

ország gazdasági és telekommunikációs hálózatának a megbénítása volt. Hogy mennyire sikerrel jártak a támadók, az észt védelmi minisztérium szóvivőjének nyilatkozata jelzi: a szeptember 11-ei terrortámadásokhoz hasonlította a történteket, amelynek során országát „a digitális kőkorszakba bombázták vissza". 2009-ben Konsztantyin Goloszkokov, egy, a Kreml által támogatott ifjúsági mozgalom, a Nási egyik vezetője bevallotta, hogy szervezetük állt az észt támadás végrehajtása mögött, de nem az orosz kormány megbízásából hajtották végre.[27] Ezt azonban érdemes kritikával fogadni, ugyanis a Nási bizonyítottan Vlagyiszlav Szurkov kezdeményezésére jött létre, aki egy, a Kremlhez köthető ideológus. Az egy évvel később lezajlott orosz-grúz konvencionális háborút párhuzamosan egy kiberháború is kísérte, amelynek esetében bebizonyosodott, hogy a támadók többek között felhasználták egy szentpétervári illetékességű szervezett bűnözői kör, a Russian Buisness Network spamküldő[28] hálózatát is.[29] A szervezett a spamküldéstől kezdve az identitáslopáson át a gyermekpornóig bezárólag minden internetes bűnözési formában képviselteti magát. Az IOCTA által megfogalmazott egyik ajánlás szerint a hatékony rendőrségi fellépéshez elengedhetetlen, hogy az online visszaélésekkel foglalkozó egységek tagjai megtanuljanak oroszul, ugyanis az elkövetők jelentős része orosz anyanyelvű.

Egyre több állam ismeri fel Napóleont idézve, a „legjobb védekezés a támadás" elvének érvényességét a kibervédelemben is. Ennek megfelelően növekszik azon államoknak a köre, amelyek Kínához[30] hasonlóan saját, kiberámadásokra specializált katonai egységeket hoznak létre. Különböző jelentések[31] szerint ezek az egységek számos esetben tehetőek felelőssé olyan kibertámadások végrehajtásáért, amelynek során pl. amerikai katonai titkokat szereztek meg a támadók. India, attól való félelmében, hogy támadás éri kritikus infrastruktúráit, felhatalmazta Defence Intelligence Agency-t és a National Technical Research Organisation-t, hogy szükség esetén nem részletezett támadó műveleteket hajtson végre.[32] A Pentagon Kiberparancsnoksága 2015-re 13 támadó jellegű csoport létrehozását tűzte ki céljául.[33] Az új csoportok a kiterjedt kormányzati erőfeszítések részeiként jönnek létre, hogy megvédjék az országot azoktól

[27] Dajkó Pál: Ifjúoroszok hajtották végre az észtek elleni internetes támadást, IT Café, 2009. március 12., http://itcafe.hu/hir/kibertamadas_esztorszag_oroszorszag.html (2014.11.14.)
[28] Spam alatt a kéretlen reklámküldeményeket értjük. A spamek egy releváns része valójában nem kereskedelmi értékesítést kíván végezni, hanem adat- és jelszóhalászat a tényleg célja.
[29] Kiberháború zajlott a Kaukázusban, SG.hu, 2008. augusztus 14., http://sg.hu/cikkek/62049/kiberhaboru-zajlott-a-kaukazusban (2014.11.14.)
[30] Ide köthető pl. Népi Felszabadító Hadsereg állományába tartozó 61398-as egység.
[31] Mandiant: APT1- Exposing One of China's Cyber Espionage Units, 2013., http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (2014.11.14.)
[32] Muncaster, Phil: India to greenlight state-sponsored cyber attacks, In. The Register, 2012. június11., http://www.theregister.co.uk/2012/06/11/india_state_sponsored_attacks/?goback=.gde_3502864_member_123369450 (2014.11.14.)
[33] Nakashima, Ellen: Pentagon creating teams to launch cyberattacks as threat grows, In. The Washington Post-National Security, 2013. március 12., ISSN: 0190-8286, http://www.washingtonpost.com/world/national-security/pentagon-creating-teams-to-launch-cyberattacks-as-threat-grows/2013/03/12/35aa94da-8b3c-11e2-9838-d62f083ba93f_story.html (2014.11.14.)

a támadásoktól, amelyek például a Wall Street-et vagy az elektromos hálózatot érhetik. Természetesen nem marad el Oroszország sem (ahogy ezt az észtek, illetve grúzok elleni DOS-támadások is mutatták), de jelentős, a becslések szerint 4-5 ezer fős hackersereget birtokló Irán, amely feltehetően a 4. legnagyobb ilyen jellegű egység[34] (egy milliárd dollárt fektetett az iráni állam a létrehozására, ami a Stuxnet pusztítását követően érthető). Nem lebecsülendő Észak-Korea 3000 fősre becsült kiberserege sem, amely egy kiszámíthatatlan, irracionális döntések meghozatalára hajlamos rezsim kezében növeli a veszély mértékét.[35] A hírszerzés történelem több olyan esetet dokumentált, amikor nemzetbiztonsági szolgálatok szervezett bűnözői csoportokat használtak fel műveleteik sikeres végrehajtására vagy az ellenséges államok gyengítésére. Ez alapján joggal feltételezhetjük, hogy a kibertérben sem eltérő szabályok alapján dolgoznak a szolgálatok.
A hírszerzés történelem több olyan esetet dokumentált, amikor nemzetbiztonsági szolgálatok szervezett bűnözői csoportokat használtak fel műveleteik sikeres végrehajtására vagy az ellenséges államok gyengítésére. Ez alapján joggal feltételezhetjük, hogy a kibertérben sem eltérő szabályok alapján dolgoznak a szolgálatok.

Az idézett Europol jelentések a szolgáltatásszerű bűnözés kapcsán egy olyan bűnözői kör kialakulását fogalmazta meg, amely az antwerpeni kikötőben elkövetett bűncselekményhez hasonlóan nem csupán kibertámadás végrehajtását elősegítő eszközök forgalmazását, de olyan szolgáltatásokat is nyújt, amit bérmunkaként a megrendelő igényei szerint végeznek. Mindezt kiegészítik egy rendkívül fejlett telefonos ügyfélszolgálat biztosításával,[36] hogy a mindenféle informatikai szakértelem nélkül is elvégezhesse a megrendelő a kívánt kibertámadást. A bűnözők nem csupán kibertámadást „árulnak" egy adott rendszer, szervezet ellen, de ugyanúgy megrendelhető a támadáshoz szükséges infrastruktúra. Jelenleg a szolgáltatásszerű bűnözés elleni fellépés leghatékonyabb módja, hogy az igazán jól képezett hackerből viszonylag kevés van, így az Europol vélekedése szerint ezeknek a hackerközösségeken belül elismert, kiemelkedő képességű hackerek elfogására kell összpontosítaniuk a rendvédelmi erőknek.

A különböző informatikai támadások végrehajtását a különböző informatikai eszközök vírussal való megfertőzése teszi lehetővé. A vírusokkal, trójai falovakkal, különböző

[34] Nekik tulajdonítják a Saudi Aramco elleni támadást, mi 30 ezer számítógépről törölt le mindent, és az amerikai bankok elleni online inváziót.
[35] Ponemon Institute: 2012 Cost of Cyber Crime Study: United States. http://static.knowledgevision.com/account/idgenterprise/assets/attachment/HPESP_WP_PonemonCostofCyberCrimeStudy2012_US.pdf (2014.11.14.)
[36] Hasonló szolgáltatást nyújt kormányzati szereplőnek többek között a Gamma International nevű cég is, amely Finfisher nevű szolgáltatásukat sajtóinformációk szerint a magyar Nemzetbiztonsági Szakszolgálat is igénybe vette a megvásárolt megfigyelő rendszerhez a technikai támogatást.

sebezhetőségek kihasználásával a bűnözőknek a rendszerhez való hozzáféréssel nem csupán az informatikai rendszer irányítása felett vehetik át az uralmat, de lehetőségük nyílik a számítógépeken tárolt adatok (fényképek, videók, dokumentumok) titkosításához, amelyet csupán egy meghatározott összeg átutalását fejében állítják vissza a hozzáférést. A számítógépeken tárolt adatok természetesen adott esetben versenyelőnyt biztosíthat egy riválisvállalatnak, akár azáltal, hogy a feltört rendszerből megszerzett információkkal előnyösebb üzleteket köt, esetleges technológiai fejlesztésről szóló információkat ellopva előbb lép piacra egy adott termékkel vagy az informatikai rendszer feletti uralmat kihasználva ellehetetleníti/csődhelyzetbe juttatja a kérdéses vállalatot, például a vállalt szállításokat sorozatosan más célra történő irányításával. Az IOCTA jelentés kiemeli, hogy 2014 áprilisa óta a Microsoft megszűntette a Windows XP operációs rendszerekhez biztosított terméktámogatást, és nem bocsájt ki biztonsági frissítéseket a továbbiakban az operációs rendszerhez. A Windows XP napjainkban a használt számítógépek körülbelül a negyedén fut, beleértve a bank automaták jelentős részét. Az Europol vizsgálatai arra utalnak, hogy a bűnözők az évek alatt folyamatosan gyűjtögették az operációs rendszer sebezhetőségeit, de amíg a Microsoft rendszeres karbantartást végzett rajta, nem használták a birtokukban levő tudást. A terméktámogatás megszűnésével vélhetően a bűnözők élni fognak ezekkel a sérülékenységre vonatkozó információkkal, éppen ezért létfontosságú mind a magánembereknek, mind a vállalatoknak, hogy olyan informatikai rendszert használjanak, amelyeken a feltelepített programokhoz, alkalmazásokhoz nem csupán terméktámogatás párosul, de rendszeresen frissítik a gyártók által kiadott biztonsági csomagokat.

Már-már közhelynek számít, de legyen egy rendszer bármilyen védett informatikailag, mindig van egy gyenge láncszem, ami sok esetben a humán fakorból következik. Számos információbiztonsággal foglalkozó jelentés, de a már többször idézett IOCTA jelentés kiemelt kockázatként kezeli a social engineeringet, amely magyarul nagyjából a pszichológiai manipulációnak feleltethető meg. A social engineering lényege, hogy úgy férnek hozzá egy védett rendszer, hogy egy hozzáféréssel rendelkező személyt zsarolással vagy annak becsapásával veszik rá a hozzáférés biztosításával. Sikeres social engingeering nem végezhető, ha nem rendelkeznek a támadók olyan információval, amellyel a célszemélyt zsarolhatják, megtéveszthetik. Ezekhez az információkhoz hozzáférhetnek a magáncélra használt informatikai rendszerük támadásával vagy nyílt forrású információgyűjtés végzésével. Hogy ezzel milyen eredményeket érhetünk el, elég, ha belegondolunk az antwerpeni kikötőben elkövetett bűncselekménybe. A nyomozást követően a kikötő biztonsági előírásait megszigorították, amely az informatikai rendszerek védelemét is érintette. Tegyük fel, a külső támadás lehetetlenné vált, olyan mértékű védelmet valósítottak meg. Ilyen esetben van szerepe a social engineeringnek, hiszen, maradva a hipotetikus példánál, a kikötő takarítószemélyzetéből egy dolgozó megzsarolásával/megtévesztésével a támadók

elérhetik, hogy a takarító azokat az informatikai eszközökhöz hozzáférést biztosítson egy pendrive a számítógépbe történő helyezésével, amivel a támadók olyan hátsó kapukat nyithatnak, amellyel átvehetik az irányítást az eszköz felett. Ahogy fentebb írtam, a bűnözők olyan kibertámadáshoz használatos eszközöket is forgalmaznak, amelynek a rendszerbe történő becsempészését ilyen úton is végezhetik.

A dolgozókról szerzett információk felhasználásával természetesen hozzáférhetnek olyan adatokhoz is, amellyel a klasszikus bűncselekmények végrehajtásához alkalmazhatnak, maradva a logisztikai rendszereknél, például a kamionok eltérítését. A szervezett bűnözői csoportoknak mindig is kiemelt célpontjaik voltak a kamionok kifosztása, sok esetben összejátszva egy belső emberrel. A tanulmányom elején említett okosváros koncepció, amely a közlekedési rendszerre is jelentős hatással van. A fejlesztés egyik fő iránya az autonóm közlekedés, amely megvalósulásával teljes egészében alakíthatja át a közlekedést, ezáltal a logisztikai rendszereket és az ellátási láncot. Horváth Attila megállapítása szerint „*A közlekedési és logisztikai rendszerek kibervédelme a jelenlegi technológiai fejlettségi szinten a létfontosságú rendszerek védelmének leggyengébb területének számítanak. Ezért sem lehet véletlennek tekinteni, hogy a kibervédelem az egyes államok, nemzetközi szervezetek világszerte kiemelkedő jelentőségű kérdésként kezeljék*."[37]

Autonóm közlekedési rendszerekre már napjainkban is találhatunk példákat, egyes vonat- és metrótípusok ilyen rendszerben működnek, de ezek kötött pályán közlekednek, így a változók száma jelentősen alacsonyabb, mint a közúti közlekedés esetében. Az autonóm közlekedés egyik lényegi eleme, hogy a közlekedési eszközt vezérlő informatikai rendszer autonóm módon dönt a jármű irányításáról, kiválasztja az optimális útvonalat, sebességet, és képes kezelni a kialakult vészhelyzeteket is. Az útvonal kiválasztásban figyelembe veszi az út minőségét, a forgalom nagyságát, a sebességkorlátozásokat és egyéb információkat, amellyel a humán vezető döntési szempontjain túl a többletinformációkkal hatékonyabban dolgozza fel az útvonalhoz kapcsolódó változókat. Ahhoz, hogy ez megvalósulhasson, a számítógépnek rengeteg adattal kell rendelkeznie a környezetéről, beleértve ebbe a többi járműből érkező információkat. Az okosváros koncepciója elképzelhetetlen a mindent átszövő szenzorok használata nélkül, amelyek által továbbított információkat az autonóm közlekedési eszközök értelmeznek, felhasználnak, s amelyek alapján meghozzák a döntésüket. Jelenleg a közúti közlekedés tekintetében félautomata rendszerek már megjelentek a forgalomban, de a teljesen automata rendszerek számos megoldásra váró problémával küszködnek. Bár technológiai szempontból is megannyi terület fejlesztése szükséges, elég, ha csak a jármű tájékozódását lehetővé tevő lézerradar és

[37] Horváth Attila: Terrorizmus és térjellemzők a létfontosságú rendszerelemek védelmében, In: Horváth Attila, Bányász Péter, Orbók Ákos (szerk.), Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről. 152 p., Budapest: Nemzeti Közszolgálati Egyetem, 2014. pp. 7-26.

szenzor esős időben, ködben való diszfunkciójára gondolunk, de a legnagyobb probléma mégis a jogi szabályozásban keresendő, hiszen egy autonóm járművet érintő balesetben a felelősség megállapítása rengeteg jogi problémát vet fel, amelyekre jelenleg nem létezik megoldás. Tekintsünk azonban most el ezektől a megoldandó kérdésektől, mert bár jelenleg érvényesek, de vélhetően a jövőben megszületnek azok a technikai fejlesztések és jogi szabályozások, amelyek megteremtik az autonóm közlekedési eszközök elterjedését. A logisztikai rendszerben, illetve az ellátási lánc teljes spektrumában az autonóm járművek megteremtik a pontosabb munkavégzést, csökkentik a humán faktorból eredő kockázatokat, rentábilisabb üzletmenetet teremthetnek. Az autonóm áruszállító eszközök több olyan változást teremtenek, amelyek a már használt fogalmakat újraértelmezik. Erre szolgál példával a konvojok alkalmazása, amely a résztvevő járművek közti kommunikáció által lehetővé teszi a minimális követési távolság biztonságos tartását, ezzel jelentősen csökkentve az üzemanyag fogyasztást. Míg korábban a konvojban való haladást biztonsági megfontolások alakították, amely a szállított termékek védelme köré szerveződött, vezető nélküli azonban csökken azoknak a megállópontoknak a száma, ahol rajtaüthetnek a kamionokon. Ahogy korábban például a kamionsofőr lefizetésével rablásnak álcázva eltéríthették a kamiont, úgy kamionsofőr hiányában ez nem valósulhat meg. Természetesen nem szűnik meg annak lehetősége, hogy az árut eltérítsék, hiszen az informatikai vezérlés lehetővé teszi, hogy kibertámadás segítségével illetéktelenek vegyék át az irányítást a jármű fölött.

Az autonóm járműfejlesztés egyik ága a katonai alkalmazás. 2014. október 31-én a Nemzeti Közszolgálati Egyetemen megrendezett konferencián Orbók Ákos mutatta be előadásában[38] egy fejlesztés alatt álló autonóm katonai szállító-támogató jármű alkalmazási lehetőségeit. A TerraMax néven megalkotott járműrendszer egy olyan autonóm módon is működni képes eszköz, amely mind konvojban, mind önmagában rossz útviszonyok mellett is képes nagy távolságok megtételére. A haladása során emberi beavatkozás nélkül is eldönti, melyek azok a tényezők, amelyek negatívan vagy pozitívan befolyásolhatják haladását. Az útvonal kiválasztása több szinten történik. Az első szinten a GPS alapú helymeghatározás az alapvető, erre épül a geoinformációs adatbázis által közvetített információ, amit a harmadik szinten pontosítanak a járműre szerelt szenzoros érzékelőkből származó adatok. A jármű autonóm és fél autonóm üzemmódban működik. A műveleti területek sajátosságaiból fakadóan a váratlan katonai jellegű szituációk megoldására minden percben késznek kell lenni, hogy a jármű fölött a kísérő személyzet vegye át az irányítást. Az autonóm közlekedési eszköz működése abban tér el a személyzet nélküli járművektől (például UAV), hogy az emberi irányítás megszűnése után képes önállóan döntést hozni a korábban meghatározott feladat végrehajtása érdekében, míg a személyzet nélküli járművek az

[38] Orbók, Ákos: Az autonóm közlekedés technológiai kihívásai, Előadás, „A haza szolgálatában" szakmai-tudományos konferencia, Nemzeti Közszolgálati Egyetem, 2014. október 31.

emberi irányítás nélkül az előre beprogramozott műveleteket képesek végrehajtani (például a kiinduló pontra való visszatérés). Ebből következően a legnagyobb változás a személyzet nélkül járművekhez képest a környezetérzékelő szenzorok bevonása a járművek vezérlésében. Ahogy Csaba Zágon fogalmazza doktori értekezésében, *„Az utóbbi időben egyre több olyan híradással találkozunk, amelyek arra utalnak, hogy az afganisztáni lázadók célirányosan pusztítják az utánpótlási útvonalak infrastruktúráját, zavarják, vagy akár ideiglenesen akadályozzák a szállítást, illetve átmeneti tárolás alatt lévő utánpótlási készleteket semmisítenek meg. Ez nem tekinthető afgán specialitásnak, más missziók esetében is következtek be hasonló események."*[39]

A lehetséges katonai alkalmazás a műveletek logisztikai támogatásában a legvalószínűbb, amely magában foglalhatja a csapatok kísérését, illetve az utánpótlás biztosítását, de szerepet kaphat egyéb alkalmazás is, például aknamentesítés. Figyelembe véve az afganisztáni tapasztalatokat, ahol az ellenállók finanszírozása nagy részben az ópiumtermelésből származó bevételeken alapul, a szervezett bűnözéssel való kapcsolat bebizonyosodott.[40] A legfrissebb becslések 2013-ban a világ ópiumtermelését 6886 tonnára teszik, melyből az afgán részesedés 80%, az ebből előállított heroint pedig 560 tonnára becsülik.[41] Egy ehhez hasonló műveleti környezetben feltételezhetjük, hogy az utánpótlásvonalak ellen végrehajtott támadások egy része nem közvetlenül politikai motivációk vezérlik, hanem anyagi haszonszerzés is szerepet játszhat. A támadás végrehajtásában a hagyományos módszerek mellett (például az útvonalon fekvő híd megsemmisítése) informatikai támadás is szerepet játszhat. Ezek ellen nyújthat védelmet, hogy a jármű fölötti irányítást bármikor átveheti távirányítással a kezelő/kísérő személyzet.

Javaslatok

Az általam feldolgozott téma klasszikus, évszázadok óta létező jelenségek (szervezett bűnözés, logisztika) új kontextusba helyezésnek (kibertér) kockázatait kívánta ismertetni. A dolgozat hiábavaló lenne, amennyiben nem fogalmaznék meg javaslatokat, ajánlásokat, amelyek elősegíthetik a kockázatok csökkentését, prevencióként szolgálhatnak. A megfogalmazottak csupán az új kihívásokra próbálnak választ adni, nem foglalkozok az olyan kérdéssel, hogyan lehet eredményesen harcolni a szervezett bűnözés ellen, hogy javíthatjuk a közlekedési infrastruktúrát stb.

[39] Csaba, Zágon: Gazdasági biztonságot garantáló fegyveres szervezetek szükséges képességeinek és kapacitásainak meghatározása kockázatelemzési eljárásokkal, PhD. értekezés tervezet, Nemzeti Közszolgálati Egyetem, 2014.
[40] Horváth L., Attila: A terrorizmus csapdájában, Zrínyi Kiadó, Budapest, 2014.
[41] Csaba i.m. 2014.

Megítélésem szerint a legfontosabb a megfelelő normatív szabályozás. A jogszabályalkotás egy követő cselekedet, hiszen nem szabályozhatunk valamit, ami nem korábban nem jelentkezett valamilyen problémaként. Az Észtország pénzügyi- és kormányzati rendszere ellen 2007-ben elkövetett kibertámadás véleményem szerint ennek igazolására kiváló példával szolgál, hiszen egy NATO tagállamot ért támadás következtében elvben az 5. cikkely alapján a kollektív védelemnek kellett volna érvényesülni. Mivel az eset annyira újszerű, korábban nem tapasztalt volt, nem véletlen tehát, hogy a NATO nem katonai támadásként értelmezte a történteket. A NATO, de az egyes államok vezetői is megérezték, hogy a felmerült jogi hézagot pótolni szükséges. Ennek megfelelően a NATO kérésére nemzetközi szakértők által összeállított ajánlást dolgoztak ki arra nézve, hogy a kiberhadviselés milyen nemzetközi jogi elvek szerint legyen szabályozva.[42] A Tallini jegyzőkönyv[43] nevet viselő kézikönyv az online háborút próbálja értelmezni a klasszikus hadviselés elvei alapján, követve a genfi és hágai konvenciókat követve, deklaráltan a civilek védelmére. Ebből adódóan tiltja a kórházak, vízi- és nukleáris erőművek ellen intézett támadásokat. A halálos áldozatokkal, illetve különösen nagy anyagi kárral járó támadásokat háborús cselekménynek minősíti, ami kiváltja a konvencionális eszközökkel való válaszcsapás jogát is, valamint a támadást végrehajtó hackereket nem civilekként, hanem katonákként értelmezni. Fontos azonban látni, elképesztően nehéz bizonyítani, hogy ki állt a támadások mögött. Ahogy az orosz-észt példa is mutatta, hiába lehetett tudni, hogy kikhez köthető a támadás, nem lehetett egyértelmű bizonyítékokkal alátámasztani az orosz érdekeltséget. Már pedig, ha a tallinni jegyzőkönyv háborús cselekményként aposztrofált kitételeit nézzük, a különösen nagy anyagi kárral járó támadás kiváltja az önvédelemhez való jogot.

A kibervédelem megszervezése azonban rendkívül komplex feladat, amelynek törvényi szabályozásban az elején járunk. A magyarországi rendvédelmi szervek tekintetében a Belügyminisztériumnak különösen fontos szerep jut.[44]

Megfelelő szakértelemmel, ahogy egy létfontosságú infrastruktúrát ért kibertámadásnál, úgy egy bűncselekménynél megvalósított informatikai betörés esetében is el lehet tüntetni a nyomokat, hogy azokat ne lehessen visszakövetni a valódi elkövetőkre, esetleg olyan hamis nyomokat hátrahagyni, amellyel ártatlanokra tereljük a gyanút. A jogi szabályozásnál ezt mindenképp figyelembe kell venni.

---

[42] NATO Cooperative Cyber Defence Centre of Excellence 2013: Tallinn Manual on The International Law Applicable to Cyberwarfare, Cambridge University Press, http://issuu.com/nato_ccd_coe/docs/tallinnmanual?mode=embed&layout=http%3A%2F%2Fskin.issuu.com%2Fv%2Flight%2Flayout.xml&showFlipBtn=true

[43] A név nem véletlen, az Észtországot ért kibertámadásra reflektál az ország fővárosáról elnevezett kézikönyv.

[44] Krasznay Csaba: A rendvédelmi szervek helye a kibervédelemben, In. Magyar Rendészet, XIII: (különszám) pp. 109-118., 2013.

További nehézséget okoz a normatív szabályozás megalkotásánál az érintett ágazatok határokon átnyúló természete. A közlekedés európai kritikus infrastruktúrának minősül, hiszen megfelel az Európai Tanács által elfogadott 2008/114/EK irányelvének,[45] amely az európai kritikus infrastruktúrát olyan létfontosságú rendszerelemként értelmezni, amely megsemmisítése, vagy működésének megzavarása legalább 2 tagállamban súlyos hatásokat okoz. A közlekedési rendszerhez hasonlóan az infokommunikációs technológiák is túlnyúlnak az országhatárokon, ahogy a szervezett bűnözés jellemzőinél is igazoltam, egyaránt nemzetközi színtéren értelmezhető. A fentiekből következően elengedhetetlen, hogy az egyes államok által megalkotott jogszabályok harmonizációs folyamatait lefolytassák. A különböző bi- és multilaterális együttműködéseknek azonban nem csupán a jogszabály harmonizációra kell fókuszálniuk, hanem az egyes bűnüldöző szervek között a kölcsönös jogsegély egyezményeket is erősíteni szükséges, ahogy az együttműködés kereteit is célszerű javítani.

A megfelelő normatív szabályozást mindenképpen oktatásnak kell követnie, amelynek célja az adat- és információbiztonságra vonatkozó érzékenység megteremtését kell ellátnia. Mindez különösen fontos, ahogy reményeim szerint korábban igazoltam, még ha meg is teremtjük a tökéletes technikai védelmet, a humán tényező kihasználásával a támadók social engineeringet alkalmazva hozzáférhetnek a védett adatokhoz/rendszerekhez. A felkészítésnek nem csupán az érintettekre, de a családtagjaira egyaránt vonatkoznia javasolt, elvégre, ha a célszemélyhez másképp nem is férnének hozzá a bűnözők, szerettei, barátai felhasználásával célt érhetnek.

Az információvédelemhez hozzátartozik az informatikai eszközök megfelelő biztonsági védelme, amely a munkahelyi eszközökön kívül a privát használatban levő eszközökre is érvényesnek kell lennie. A mai világban nem csupán egy informatikai eszközt használunk, munkahelyi e-mailjeinkhez ugyanúgy hozzáférhetünk otthonról, út közben telefonunkról, tabletünkről. Amennyiben ezek bármelyikre megfertőződött korábban kártékony kóddal, a támadók ugyanúgy hozzáférhetnek azokhoz az adatokhoz, amelyeket egyébként a védett vállalati rendszeren keresztül nyitnánk meg. Ehhez kapcsolódik a használt programok, alkalmazások naprakész, frissített verzióval való telepítése minden informatikai eszközön, de itt kell megemlítenünk az olyan alkalmazások használatának elkerülését, amelyek megfertőzhetik az eszközt vagy adathalászatra készültek.[46]

A védekezés egy másik területe az idézett Europol jelentésben is megfogalmazott fókuszpont, amely azoknak a hackereknek a semlegesítését kell jelentse, akik megfelelő tudással rendelkeznek egy kibertámadás végrehajtására. Természetesen mindez elképzelhetetlen megfelelő felderítés nélkül. A veszélyt jelentő hackerek semlegesítése mellett az infrastruktúra felszámolására is törekedniük kell a

[45] Az Európai Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről

[46] Bányász, Péter: A közösségi média használat biztonsági kérdései a védelmi iparban. In. Hadtudomány Online, 24/1., 2014., pp. 49-67.

hatóságoknak. Elengedhetetlen a megfelelő szakember gárda felkészítése, akik nem csupán magas szintű informatikai képességgel rendelkeznek, de beszélik azokat a nyelveket (lásd például a korábban említett orosz), amely lehetővé teszi a célcsoportok megfigyelését, esetleges beépülést a szervezetekbe.

Törekedni kell azoknak a weboldalak megszüntetésére, amelyeken kibertámadásra alkalmas szolgáltatásokat, tanácsokat nyújtanak. Természetesen ez rendkívül nehéz feladat, hiszen az internet sötét oldalán, elterjedt elnevezése szerint a Darknetet, a Kaspersky Lab szakértői szerint több mint 900 különböző illegális, elsősorban kiberbűnőzői csoportok által üzemeltett szolgáltatás található.[47] Ezt elsősorban a TOR[48] hálózat és infrastruktúra fejlődése teszi lehetővé, amely megteremti a képességet arra nézve, hogy az internetet hagyományosan felügyelő és figyelő szervezetek látóterén kívül helyezkednek el a felhasználók.[49] A TOR használatával ugyanúgy folytathatjuk az online tevékenységet, mint korábban, azzal a különbséggel, hogy teljes anonimitást biztosít. Ezt persze érdemes fenntartásokkal fogadni, különösen a Snowden ügy kirobbanása óta, de épp az NSA megfigyelési botránya növeli azt az igényt, hogy a felhasználók online élete rejtve maradjon a mindent figyelő szemek elől. Mindez növelte azoknak az oldalaknak az elterjedését, amik rejtve maradnak a hatóságok elől. Meg kell jegyezni, amennyiben sikerül feltörni egy ilyen weboldal titkosítását, úgy kiváló segítség lehet a nyomozó hatóságok számára.

A hackerek mellett kiemelt célpontként kell megjelenjenek a rosszindulatú programokat fejlesztő és terjesztő személyek, valamint a spamküldő hálózatok, botnetek üzemeltetői. Fejleszteni szükséges továbbá az együttműködést a különböző információbiztonság megteremtéséért hivatott szervezett között, beleértve az úgynevezett Computer Emergency Response Teameket (CERT). A magyarul Számítástechnikai Sürgősségi Reagáló Egységnek nevezett szervezetek feladata, hogy időben reagáljanak és kezeljenek minden hálózatbiztonságra és kritikus információs infrastruktúrára veszélyes internetes eseményt. Hazánkban a Nemzetbiztonsági Szakszolgálaton belül működő Kormányzati Eseménykezelő Központ (CERT-Hungary) a magyar kormányzati hálózatbiztonsági incidenskezelő központ. Feladata a teljes magyar állami szféra informatikai rendszereinek hálózatbiztonsági támogatása. A Központnak kiemelt szerepe van a nemzetgazdaság és az állami működőképesség szempontjából alapvető fontosságú informatikai rendszerek védelmében. A Központ jogszabályi hátterét Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény[50] biztosítja. Nevezett jogszabály egy

[47] Dunn E., John: Tor network used to hide 900 botnets and darknet markets, says Kaspersky Lab. In. TechNews, 2014. március 5., http://news.techworld.com/security/3505255/tor-network-used-to-hide-900-botnets-and-darknet-markets-says-kaspersky-lab/ (2014.11.17.)

[48] The Onion Router.

[49] Ezt úgy éri el, hogy a használatával nem lehet megállapítani a felhasználó IP címét, aminek hatására nem lehet visszakeresni a felhasználót, illetve a Darknet úgynevezett pszeudó domaint használ, amely megakadályozza, hogy eljussanak az erőforrás tulajdonosához.

[50] 2013. évi L. törvény - az állami és önkormányzati szervek elektronikus információbiztonságáról.

rendkívül fontos lépés volt azon az úton, amely hazánk információbiztonságát hivatott megteremteni, ahogy ezt a fejezet elején prioritásként megfogalmaztam.
Figyelembe kell venni, hogy a vállalatok ellen elkövetett támadások sok esetben nem kerülnek bejelentésre a nyomozó szerveknél, ennek okán ki kell építeni azt a bizalmat, amely elősegíti a hatékonyabb nyomozást. Mivel egyes esetekben érzékeny adatok lopnak el vagy a megtámadott vállalat jó hírnevét veszélyeztető bűncselekményeket követnek el, így megfelelő érzékenységgel és diszkrécióval kell élniük a hivatalos szerveknek a nyomozati cselekmény alatt.
Végezetül pedig nem szabad elfelejteni, hogy költeni szükséges a védelemre, hiszen igen komoly aszimmetria jelentkezhet egy kibertámadás elkövetésének költségei és a valós károkozás között. Aszimmetria során *„egymáshoz képest össze nem hasonlítható (összemérhetetlenül eltérő) anyagi, emberi és szellemi készségeket, képességeket (ha úgy tetszik kompetenciákat) és eljárásokat vetnek össze*”.[51] Már pedig, a javaslatban megfogalmazottak jelentős része megköveteli az anyagi ráfordítást, legyen szó oktatásról, a törvényi elírásnak megfelelő működésről stb.

Összegzés

A 2000-es évek elején az internet forradalmáról beszélt mindenki. Azóta eltelt egy évtized nem hogy csökkentette, de nagyban növelte az infokommunikációs technológiánktól való függőségünk. A forradalom tovább zajlik. Életünk majd’ minden része valahol a kibertérben zajlik, megnyitva ezzel korábban nem tapasztalt kockázatok, kihívások, fenyegetések tárházát. Ahogy a modern technológiák elterjedése számos pozitív hozadékkal jár, úgy folyamatosan észleljük a veszélyeket. Amennyiben a forradalmak természetrajzát elfogadjuk, úgy jogosan merül fel a kérdés, a forradalom vajon felfalja saját gyermekeit, azaz minket? Tanulmányomban az ellátási láncok biztonságát veszélyeztető informatikai kihívásokat kívántam bemutatni a szervezett bűnözés aspektusából. A közlekedési kritikus infrastruktúra és az ellátási láncok biztonságával harmadik éve folytatok kutatásokat, amelyek egyre inkább az a kibertér jelentette kockázatok vizsgálatára fókuszált. A szervezett bűnözés megítélésem szerint korunk egyik legkomolyabb biztonsági kockázata, nem csupán az általa elkövetett bűncselekmények a társadalomra káros mivolta okán, hanem azért is, mert az államba történő beépülésével a demokratikus jogállamok rákfenéjeként jelenik meg. A témával közel hét éve foglalkozok, és az utóbbi években tapasztalt tendenciák, amellyel a kiberbűnözők tevékenységüket folytatják, megköveteli a tudományos

[51] Forgács Balázs, Kaló József, Németh József Lajos: Aszimmetrikus kihívások a haderő, az állam, valamint a társadalom viszonyában, In. Hadtudomány 25:(1-2) pp. 106-110., 2015.

kutatóktól, hogy alapos vizsgálat alá vessék. Ahogy a dolgozat elején említettem, a téma ötletével a Horváth Attila- Csaba Zágon szerzőpáros előadása szolgált. Munkámban igyekeztem azonosítani azokat a kritikus pontokat, ahol a szervezett bűnözők megjelenhetnek, illetve javaslatokkal éltem az ellenük való védekezésre. Úgy vélem, nem kell különösen bizonyítanom, a szervezett bűnözés ellen való fellépés mindannyiunk közös érdeke. Bár a tanulmány a közlekedési rendszer és az ellátási lánc biztonságára összpontosított, látnunk kell, hogy bármelyik ágazat esetében megfogalmazhattam volna a leírtakat.

FELHASZNÁLT IRODALOM

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Magyar Közlöny, Magyarország hivatalos lapja. 2012. évi 154. szám

2013. évi L. törvény - az állami és önkormányzati szervek elektronikus információbiztonságáról

2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról, In. Határozatok Tára, 31. szám, Budapest, 2008. június 30.

A kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti biztonsági Stratégiájáról http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf (2014.11.05.)

Az Európai Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről

Bányász, Péter- Orbók, Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében, Hadtudomány Online 23/1., 2013.

Bányász, Péter: A közösségi média használat biztonsági kérdései a védelmi iparban. In. Hadtudomány Online, 24/1., 2014.

Berta, Sándor: Az internet a 21. század idegrendszere, In. SG, 2013. május 10., http://www.sg.hu/cikkek/97219/az_internet_a_21_szazad_idegrendszere (2014.11.10.)

Chikán, Attila- Gelei, Andrea: Az ellátási láncok és menedzsmentjük In. Harvard Business Manager (magyar kiadás), 2005. január

Csaba, Zágon: Gazdasági biztonságot garantáló fegyveres szervezetek szükséges képességeinek és kapacitásainak meghatározása kockázatelemzési eljárásokkal, PhD. értekezés tervezet, Nemzeti Közszolgálati Egyetem, 2014.

Dajkó Pál: Ifjúoroszok hajtották végre az észtek elleni internetes támadást, IT Café, 2009. március 12., http://itcafe.hu/hir/kibertamadas_esztorszag_oroszorszag.html (2014.11.14.)

Dunn E., John: Tor network used to hide 900 botnets and darknet markets, says Kaspersky Lab. In. TechNews, 2014. március 5., http://news.techworld.com/security/3505255/tor-network-used-to-hide-900-botnets-and-darknet-markets-says-kaspersky-lab/ (2014.11.17.)

Ericson Press Release: New study quantifies the impact of broadband speed on GDP, In. Ericson, 2011. szeptember 27., http://www.ericsson.com/news/1550083 (2014.11.10.)

Europol The Internet Organised Crime Threat Assesment 2014., Europol, Hága, 2014., https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf

Europol SOCTA 2013, EU Serious and Organised Crime Threat Assessment. Europol, Hága, 2013., https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf

Forgács Balázs, Kaló József, Németh József Lajos: Aszimmetrikus kihívások a haderő, az állam, valamint a társadalom viszonyában, In. Hadtudomány 25:(1-2) pp. 106-110., 2015.
Glorieux, Patrick: Európai szervezett bűnözés és a maffia-típusú csoportok: az általuk képviselt fenyegetés és az erre adandó válasz rövid helyzetjelentése, Belbiztonsági Felső Tanulmányok Intézete, IHESI, 1993.
Görbe Attiláné Zán Krisztina: Még néhány gondolat a biztonságról, In. Pécsi Határőr Tudományos Közlemények, pp. 185-190., 2006.
Haig, Zsolt- Kovács, László et. al.: A kritikus információs infrastruktúrák meghatározásának módszertana, ENO Avisory Kft., 2009.
Horváth L., Attila: A terrorizmus csapdájában, Zrínyi Kiadó, Budapest, 2014.
Horváth Attila: Az anyagáramlással összefüggő logisztikai folyamatok terrorfenyegetettségének jellemzői, In: Tompáné Daubner Katalin, Miklós György, Miklósné Zakar Andrea, Balázs Judit (szerk.), Tudomány határok nélkül. Konferencia helye, ideje: Kalocsa, Magyarország, 2008.11.27- 2008.11.28. Kalocsa: Tomori Pál Főiskola, 2008. pp. 201-208.
Horváth, Attila- Csaba, Zágon: Az ellátási lánc és a logisztika, mint közlekedési kritikus infrastruktúra - bizonyítás egy esettanulmánnyal, Előadás, „Szervezeti, szabályozási és innovatív változások a létfontosságú rendszerek védelmében" tudományos-szakmai konferencia, Nemzeti Közszolgálati Egyetem, 2014. November 14.
Horváth Attila, Csaba Zágon: On the Vulnerability and Reliability of Towns and Cities, In: Csapó T, Balogh A (szerk.), Development of the Settlement Network in the Central European Countries: Past, Present, and Future. 314 p., Berlin; Heidelberg: Springer Verlag, 2012. pp. 299-312.
Horváth, Attila: Hogyan értessük meg a kritikus infrastruktúra komplex értelmezésének szükségességét és védelmének fontosságát? In. Hadmérnök 5:(1) pp. 377-386. , 2010.
Horváth Attila: Terrorizmus és térjellemzők a létfontosságú rendszerelemek védelmében, In: Horváth Attila, Bányász Péter, Orbók Ákos (szerk.), Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről. 152 p., Budapest: Nemzeti Közszolgálati Egyetem, 2014. pp. 7-26.
Kiberháború zajlott a Kaukázusban, SG.hu, 2008. augusztus 14., http://sg.hu/cikkek/62049/kiberhaboru-zajlott-a-kaukazusban (2014.11.14.)
Kövesdi, Zoltán: Az e-gazdaság helyzete Magyarországon - az Európai Bizottság elemzése, In. Infotér, 2011. július 11., http://www.infoter.eu/cikk/az_e-gazdasag_helyzete_magyarorszagon_-_az_europai_bizottsag_elemzese (2014. 11.11.)
Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban, In. Hadmérnök VII:(4) pp. 142-151., 2012.
Krasznay Csaba: A rendvédelmi szervek helye a kibervédelemben, In. Magyar Rendészet, XIII: (különszám) pp. 109-118., 2013.
Lampe von, Klaus: Definitions of Organized Crime, http://www.organized-crime.de/organizedcrimedefinitions.htm (2014.11.05.)

Mandiant: APT1- Exposing One of China's Cyber Espionage Units, 2013., http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (2014.11.14.)
McKinsey & Co.: Online and upcoming: The Internet's impact on aspiring countries, 2012. január., http://www.mckinsey.com/client_service/high_tech/latest_thinking/impact_of_the_internet_on_aspiring_countries pp. 81-91. (2014. 11.10.)
Muncaster, Phil: India to greenlight state-sponsored cyber attacks, In. The Register, 2012. június11., http://www.theregister.co.uk/2012/06/11/india_state_sponsored_attacks/?goback=.gde_3502864_member_123369450 (2014.11.14.)

Nakashima, Ellen: Pentagon creating teams to launch cyberattacks as threat grows, In. The Washington Post- National Security, 2013. március 12., ISSN: 0190-8286, http://www.washingtonpost.com/world/national-security/pentagon-creating-teams-to-launch-cyberattacks-as-threat-grows/2013/03/12/35aa94da-8b3c-11e2-9838-d62f083ba93f_story.html (2014.11.14.)

NATO Cooperative Cyber Defence Centre of Excellence 2013: Tallinn Manual on The International Law Applicable to Cyberwarfare, Cambridge University Press, http://issuu.com/nato_ccd_coe/docs/tallinnmanual?mode=embed&layout=http%3A%2F%2Fskin.issuu.com%2Fv%2Flight%2Flayout.xml&showFlipBtn=true

Orbók, Ákos: Az autonóm közlekedés technológiai kihívásai, Előadás, „A haza szolgálatában" szakmai-tudományos konferencia, Nemzeti Közszolgálati Egyetem, 2014. október 31.

Orbók, Ákos: Az okosváros közlekedésirányításának kihívásai. In. Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről, Nemzeti Közszolgálati Egyetem, Budapest, 2014.

Ponemon Institute: 2012 Cost of Cyber Crime Study: United States. http://static.knowledgevision.com/account/idgenterprise/assets/attachment/HPESP_WP_PonemonCostofCyberCrimeStudy2012_US.pdf (2014.11.14.)

Press Release: Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020, In. Gartner.com, 2013. december 12., http://www.gartner.com/newsroom/id/2636073 (2014.11.11.)

Resperger, István: Kockázatok, kihívások, fenyegetések a XXI. században, Az Országos Kiemelt Kutatási Tanulmányok pályázata, Budapest, 2002.

Urszán, József: A szervezett bűnözés fenyegetettség értékelésének jelentősége az Európai Unióban. Pécsi Határőr Tudományos Közlemények 14/1, 2013. http://www.pecshor.hu/periodika/XIV/urszanj.pdf

Vestberg, Hans: Opening Presentation, Tomorrow Transformed – Leading change In. Ericsson Business Innovation Forum 2014.

Zán Krisztina: Az Európai Unió biztonság és védelempolitikája, In. Határrendészeti Tanulmányok 2004:(2) pp. 99-117., 2004.