HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

AZ IOT KATONAI FELHASZNÁLÁSI LEHETŐSÉGEI ÉS A FEJLESZTÉS IRÁNYAI

POSSIBILITIES OF USING IOT FOR MILITARY PURPOSES AND THE DIRECTIONS OF DEVELOPMENT

KOLLÁR Csaba

(ORCID: 0000-0002-0981-2385)

kollar.csaba@uni-nke.hu

Absztrakt

Teoretikus, hazai és külföldi forrásokat feldolgozó tanulmányom célja, hogy az IoT információbiztonsági fókuszának katonai aspektusait, illetve a fejlesztés lehetséges irányait mutassam be. A téma bevezetését követően az IoT katonai döntési folyamatban elfoglalt lehetséges helyéről írok, majd az IoT katonai technikai rendszerének egyik elfogadott ábrája alapján három katonai alkalmazási megoldást ismertetek. Külön alfejezet foglalkozik az IoT és az információbiztonság problematikájával, illetve a fejlődés és a sebezhetőség lehetőségeivel. Tanulmányom zárásaként az eredmények összefoglalása után az IoT civil-katonai fejlesztéseinek lehetséges forgatókönyveiről értekezem.

Kulcsszavak: *digitális kor, információbiztonság, IoT, katonai alkalmazás, hálózatos katona*

Abstract

My theoretical study, which deals with domestic and foreign sources, aims to present the military aspects of IoT's information security focus and the possible directions of development. Following the introduction to the topic, the possible place of IoT in the military decision-making process is described, then three solutions for military exploitation is discussed on the basis of an approved figure regarding the military-technical system of IoT. Separate sub-chapter deals with the issues of IoT and information security, as well as the possibilities of development and vulnerability. My study ends with the summary of outcomes and the possible scenarios of IoT civil-military development trends.

Keywords: *digital age, information security, IoT, military applications, networked soldier*

A kézirat benyújtásának dátuma (Date of the submission): 2017.10.10.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.21.

BEVEZETÉS

Az IoT nemzetközi katonai – elsősorban USA/NATO – jelenlegi és tervezett felhasználási területei közül a fontosabbak a következők: (1) a katonai teljesítmény nyomon követése, (2) a katonák egészségügyi felügyelete, (3) a pilóta nélküli rendszerek elterjedése, (4) a populáció nyomon követése [1], (5) a logisztikai feladatok hatékonyabb elvégzése [2], valamint (6) a műveleti döntések meghozatalához szükséges nagymennyiségű adat biztosítása, illetve (7) a katonai objektumok és kritikus infrastruktúrák védelmét elősegítő megoldások bevezetése. Ez utóbbi védelméről magyarul többek között Munk [3, 4] értekezett.

Suri és Tortonesi [5] felsorolás jelleggel foglalja össze az IoT eszközök katonai felhasználásával kapcsolatos fontosabb elvárásokat:

1. Decentralizált infrastruktúra
    a. nem lehet támaszkodni központosított infrastruktúrára
    b. taktikai felhőkre van/lenne szükség, ezek azonban még fejlesztési fázisban vannak
2. Hálózat felhasználása
    a. a polgári/kereskedelmi környezetben ez nem kihívás
    b. könnyen és gyorsan hozható létre kapcsolat az internethez
3. Együttműködési képesség
    a. néhány általános protokoll létezik, amelyik magába foglalja a szabványokat
4. Bizalom és biztonság
    a. az adatvédelem az elsődleges szempont, de a gyártók teljes hozzáférést szeretnének
5. Eszközök használata
    a. továbbra is kihívást jelent a tápellátás (különösen harci körülmények között)
6. A szemantikus web technológiára épülő alkalmazások
    a. segíthet az interoperabilitásban, az adatelemzésben és -hasznosításban

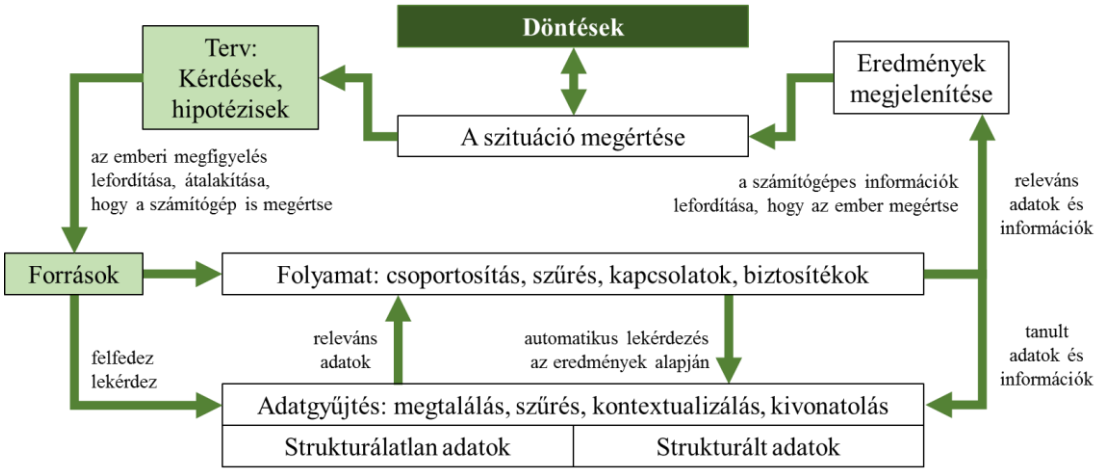
Külön figyelmet érdemel a katonai felhasználásra tervezett IoT eszközök autonómiája (önjáró, automatikus működése). Az Amerikai Védelmi Minisztérium a legfontosabb követelményként az autonómiát fogalmazta meg, különösen az olyan helyzetekre utalva, amikor az eszközök informatikai/elektronikai támadásoknak vannak kitéve. Ilyenkor az eszköznek gyors reakcióidő mellett fel kell ismernie az illetéktelen hozzáférést és meg kell azt akadályoznia (A2AD – anti-access/area-denied).

A hadiipari vállalkozások közleményei alapján megállapítható, hogy az USA hadseregében egyre komolyabb figyelmet kap az információs- és adathadviselés [6]. Ennek az oka az, hogy amint egy adat, vagy információ létrejött, azonnal továbbítható a hírszerző, megfigyelő és felderítő rendszerek felé, ami nagymértékben tudja növelni a hadsereg és az adott egység katonai hatékonyságát. A hadiipari cégek egyre komolyabb erőforrásokat fordítanak arra, hogy az IoT eszközökre épülő megoldások révén elősegítsék a gépi tanulást, illetve automatizálják a döntéshozatalt. Az IoT révén a C2BMC rakétavédelmi rendszer hatékonyabban tud működni, mivel a sok száz szenzorból, radarból és műholdból származó adatokat egy közös kommunikációs nyelv, illetve protokoll szerint továbbítják, illetve dolgozzák fel, ami a rendszerelemek közötti folyamatos kommunikáció mellett a fenyegetésekre és támadásokra történő eredményesebb és gyorsabb reagálást is lehetővé teszi. Az amerikai védelmi hivatal, a DARPA is egyre többet foglalkozik az IoT és a hadiipar kapcsolatával [7]. Olyan fejlesztések kapnak támogatást, amelyek fókuszában a szenzorok és a mesterséges intelligencia áll. Az eredmények révén a hadsereg az eddiginél hatékonyabban lesz képes felderíteni az ellenséges eszközöket és kommunikációs csatornákat, ami helyzeti előnyt jelent a számukra. A tervek között szerepel az is, hogy a már jelenleg működő nagyobb fizikai mérettel (és akár nagyobb

pontossággal) rendelkező fix, vagy telepített érzékelők mellett okostelefon méretű, hordozható eszközökkel lássák el a védelemmel foglalkozó polgári és katonai felhasználókat, illetve olcsó, s így tömegesen kihelyezhető IoT érzékelők monitorozzák folyamatosan a fontosabb út- és vasútvonalakat, hidakat, illetve a kritikus infrastruktúrák környezetét. Az IoT behálózottságnak köszönhetően olyan védelmi rendszer alakítható ki, amelyik még időben képes felfedezni a piszkos bombákat, a radioaktív sugárzást és egyéb, a társadalomra/infrastruktúrára veszélyes eszközöket, anyagokat. A környezeti monitorozás révén nagyon sok adat áll majd rendelkezésre. A hatékonyság, s így a téves riasztások arányának csökkentése érdekében fontos feladat lesz az adatzaj szűrése, az adattisztítás még mielőtt a tényleges és mélyreható elemzés megtörténik.

AZ IOT ÉS A KATONAI DÖNTÉSI FOLYAMAT

Az IoT katonai területeken történő megjelenésének egyik legfontosabb haszna az, hogy sokkal több adattal és a belőlük képzett információval, illetve tudással képes támogatni a döntési mechanizmusokat, valamint magát a katonai vezetők, parancsnokok döntéshozatalát, ahogy az az 1. ábrán is látható.



1. ábra Az IoT a katonai irányításban és ellenőrzésben (saját szerkesztés [5] alapján)

A katonai döntési folyamatban az IoT megjelenésével nagyobb hangsúly helyeződik a környezeti tényezők és hatások vizsgálatára. A műveleti területeken kihelyezett (telepített, szétszórt) IoT eszközök, illetve a támogató hálózati és egyéb infrastruktúra révén a szenzorok nagyon sok adatot tudnak szolgáltatni a környezet fizikai, kémiai, biológiai és egyéb jellemzőiről, s ezek az adatok az idősoros feldolgozásnak köszönhetően sokkal jobban értelmezhetővé teszik a változások időbeli lefolyását.

A rendelkezésre álló adatok akár strukturáltak, akár strukturálatlanok lehetnek. Az előbbibe tartoznak többek között a szöveges dokumentumok, a felhasználói/katonai tapasztalatok, a weblapok, a különböző multimédiás tartalmak, a közösségi hálón megtalálható információk, míg a strukturáltat elsősorban az adatbázistáblák, a térinformatikai adatok és koordináták, valamint a különböző szenzorok által rögzített adatok alkotják. Az adatok feldolgozása során csak a döntés szempontjából releváns strukturált, szemantikus adatok (információk), az absztrakcióra és felfogásra alkalmas tudás, illetve az intelligenciát jelentő bölcsesség kerülhet a katonai vezetők elé. Ezt szolgálják a folyamat egyes elemei, melynek végén olyan eredmény jelenik meg, ahol a számítógépes információkat a katonai döntéshozók által érthető formában (adatvizualizáció) kell bemutatni. Ennek alapján a vezetők képesek a szituációk gyors megértésére, további lekérdezési parancsok megfogalmazására a számítógép által érthető nyelvezet-

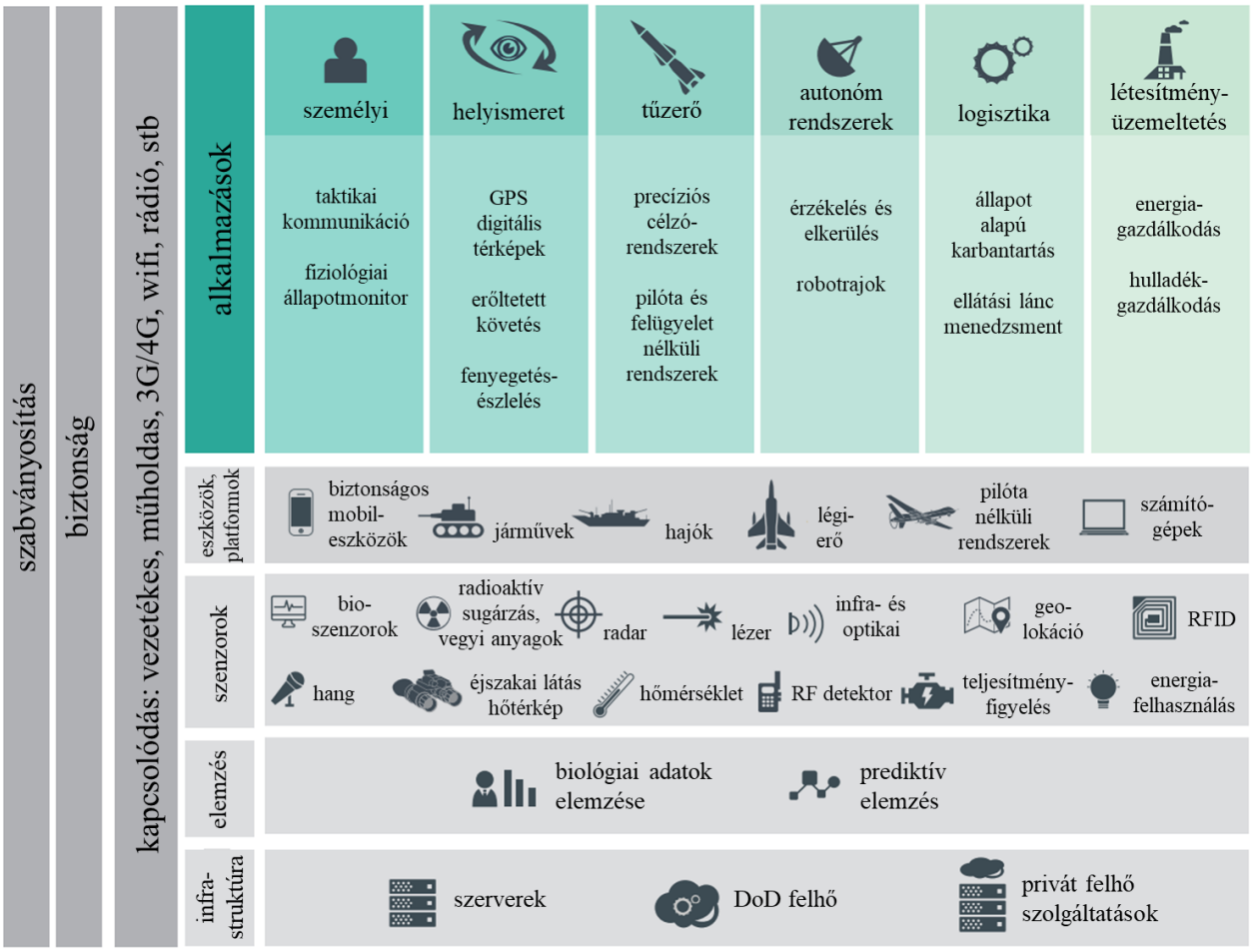
re. Így egyfelől újabb adatok gyűjthetők, másfelől a már rendelkezésre álló adatok új szempontok szerint strukturálhatók a közöttük levő szemantikai kapcsolatok révén. A szituáció megértése és a döntés meghozatala között – amennyiben a katonai vezetők megbíznak az IoT és egyéb támogató technikák által szolgáltatott adatok relevanciájában – kevesebb idő telik, ami különösen éles harci helyzetekben növeli a hatékonyságot, s így helyzeti előnyhöz juttatja a saját erőket.

Ahogy arra tanulmányom későbbi részeiben még utalni fogok, azt az idealizált állapotot, miszerint a katonai/parancsnoki döntéseket az IoT, a szemantikus adatfeldolgozás, a döntési folyamatok automatizálása, a mesterséges intelligencia megkönnyíti, s egyben jobban meg is alapozza, jelentősen árnyalja az, hogy az IoT technológia biztonsági szempontból – a civil felhasználási területekhez hasonlóan – a katonai területeken is meglehetősen sebezhető.

AZ IOT KATONAI TECHNIKAI RENDSZERE

Az IoT katonai technikai rendszerének alapját – a 2. ábra szerint – a szabványosítás, illetve a technikai-technológiai keretrendszer jelenti. Publikus forrás [8] szerint a NATO által 2015-ben indított „Az IoT katonai alkalmazhatósága” elnevezésű, IST-147 jelzésű, Lengyelország vezetésével működő munkacsoportjának (tagok: Belgium, Finnország, Németország, Hollandia, Lengyelország, Románia, Egyesült Királyság, USA) feladatai négy terület köré szerveződnek az IoT fókuszában. Ezek:

1. Meg kell vizsgálniuk az IoT katonai felhasználhatóságát az olyan területeken, mint az alapfeladatok ellátása, a helyzetfelismerés, a határőrizet, vagy az energiaellátás.
2. Fel kell térképezniük az IoT katonai felhasználhatóságának kockázati tényezőit, javaslatot kell tenniük a fontosabb kockázati tényezők konkrét kezelésére. Megoldást kell találniuk többek között a személyazonosság és az okmányok/belépőkártyák kezelésének, az objektumok védelmének, valamint a kereskedelmi biztonsági módszerek jelenlegihez képest lényegesen hatékonyabb módszereire.
3. Meg kell határozniuk azokat a kommunikációs követelményeket, amelyek az IoT által biztosított gép-gép kommunikációhoz köthetőek. Javaslatokat kell megfogalmazniuk a kommunikációs architektúrák vonatkozásában (fejlett gép-gép kommunikáció, robosztusság, skálázhatóság).
4. Technológiákat kell definiálniuk, amelyek hasznosítani tudják az IoT lehetőségeit, többek között az adatelemzés, illetve a rengeteg adat gyors feldolgozása vonatkozásában.



2. ábra Katonai technikai rendszer (saját szerkesztés [9] alapján)

Tervek szerint az említett munkacsoportnak 2018. december 1-ig kell elkészülniük a kitűzött feladatokkal. Megállapításaikat elsősorban két korábbi projektre, az IST-ET-076-ra (IoT katonai felhasználásának releváns témái), illetve az IST-ET-075-re (szenzorok és kommunikációs hálózatok integrációja) alapozzák majd.

Az ábra soron következő részével, az IoT és biztonság kapcsolatával nem ebben, hanem egy másik fejezetben foglalkozom részletesebben, míg az IoT rendszerek kapcsolódási lehetőségeiről, az infrastruktúráról, az adatok elemzéséről, valamint a szenzorokról Kollár [10] már korábban említést tett. Az eszközök és platformok egy része funkcióját, felhasználási területeit illetően nem tér el jelentősen a polgári életben használt társaitól. A polgári élethez képest azonban valamennyi katonai felhasználási területen a biztonságos működés, az energiaellátás, a meghibásodásból eredő esetleges károk minimalizálása még nagyobb hangsúllyal szerepel. Az alábbiakban a katonai alkalmazási lehetőségek közül ismeretetek hármat.

A hálózatos katona és a helyismeret

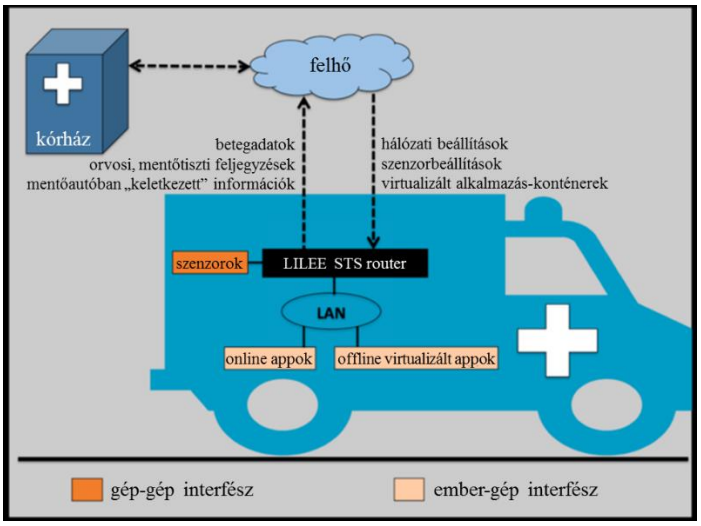
Manapság már senki nem kérdőjelezi meg az információalapú hadviselés fontosságát, illetve azt sem, hogy ennek aránya a többi hadviselési formához képest folyamatosan növekszik. A 2010-2030 közötti időszakot tekintjük az új hadügyi forradalom második hullámának, amelynek egyik fontos jellemzője tanulmányom fókuszában az, hogy „megkezdődik a hálózatos harceszközökkel rendelkező és magasabb hálózatba köthető katona, az úgynevezett hálózatos katona programok kifejlesztése, amellyel befejeződik a haderő digitalizálásának komplex programja” [11; 137. o.]. Hiba lenne azt állítani, hogy a hadügyi forradalmi korszakokat megelőzően a katonákat nem látták el olyan személyi felszereléssel, amelyik vezeték nélküli ösz-

szeköttetés segítségével támogatta a katona, a többi katona, illetve a parancsnok között a kapcsolattartást. A technika fejlődésével ezek az eszközök (pl.: katonai rádió-adóvevők) méretüket és tömegüket tekintve egyre kisebbek lettek (az elektroncsöveket leváltotta a tranzisztor, majd az integrált áramkör), csökkent a fogyasztásuk, miközben – köszönhetően az adás- és vételtechnika, illetve a híradástechnika fejlődésének – hatótávolságuk megnövekedett. Az sem szorul különösebb magyarázatra, hogy az említett forradalmak előtt is használtak a katonák különböző műszereket (pl.: hőmérsékletmérő, szélsebességmérő, Geiger–Müller-csöves sugárzásmérő), de a mért értékeket a katona rendszerint manuálisan rögzítette (papírra, vagy később számítógépre), vagy ugyan az eszköz rögzítette, de az adatok további feldolgozása érdekében az eszköznek el kellett jutnia a parancsnokságra, hogy vezetékes kapcsolaton keresztül rácsatlakozzon a megfelelő számítógépre.

A modern katona arzenáljában megjelentek, vagy meg fognak jelenni mindazok az infokommunikációs megoldások, amelyek a ma, vagy a jövő polgárait is jellemzik. A hálózatos katonák, illetve az általuk használt eszközök között a kommunikáció szélessávú, vezeték nélküli hang és adatátvitelre egyaránt alkalmas taktikai rádióval történik. Az elképzelések szerint a katona testén, ruházatán, sisakjában, esetleg bőre alatt elhelyezett szenzorok által rögzített állapotok (pl.: földrajzi koordináták, testhőmérséklet, pulzus, verejtékezés és annak 1-2 kémiai jellemzője) folyamatosan a személyi hálózatába (body-LAN) kerülnek, ahol megtörténik az adatok elsődleges és gyors feldolgozása, majd az előfeldolgozott adatok továbbítódnak a távolabb, vagy akár felhőben levő adatbázisokba a komolyabb, szemantikus feldolgozás érdekében. Az adatfeldolgozást követően a katona szükség szerint gyors visszajelzést kap akár a többi bajtársától, akár a parancsnoktól, akár a mesterséges intelligenciára épülő szoftveres megoldásoktól. A pontos helyismeret céljából számos olyan alkalmazást tud a katona az okoseszközére tölteni, amelyik lehetővé teszi a számára a harctéren folyó események valós idejű 3D-s nyomonkövetését. A katona sisakjában elhelyezett szenzorok, illetve a szenzorok adatait folyamatosan és valós időben feldolgozó élettani állapotmonitor révén idejekorán felismerhető a traumás agysérülés, a veszélyes kimerülés, vagy bármilyen olyan állapot, ami miatt az egészsége és harctéri aktivitása veszélybe kerülhet. A harctéri katonáról szóló adatok az irányítóközpontba kerülnek, ahol dönthetnek a katonai további sorsáról.

A harcszíntéren sebesült katona ellátásának előkészítése

Ahogy arról a hálózatos katonáról szóló részben már szó esett, a harctéri katonák egészségi állapotát folyamatosan monitorozni lehet, illetve szükség esetén be lehet avatkozni a folyamatokba (pl.: vissza lehet rendelni a bázisra). Gazdasági és praktikus megfontolásokból a katona bőrén, ruházatán, sisakjában elhelyezett egészségügyi szenzorok feladata az alapvetően egészséges katona állapotának a felügyelete, s a biológiai státusában nem várt, hirtelen bekövetkezett változások feldolgozása, az előfeldolgozott adatok továbbítása. Ezek a szenzorok alapvetően nem alkalmasak arra, hogy a sérült, sebesült katona állapotáról részletesebb és komplexebb képet nyújtsanak.



3. ábra A harcszíntéren sebesült katona ellátásának előkészítése (fordítás [12] alapján)

A kialakult gyakorlat szerint a harctéren megsebesült katona elsődleges ellátását a harctéri elsősegélynyújtók oldják meg. A jövő harctéri elsősegélynyújtóinál olyan hordozható vizsgálati eszközök lesznek (noninvazív és invazív egyaránt), amelyeket rá tudnak helyezni a beteg katonákra, így a részletes állapotmonitorozás azonnal elindulhat. Miközben a sérült katonát a kórházba szállítják, kétirányú adatkommunikáció is zajlik (3. ábra). A mentőautóból a felhőbe, s onnan a kórházba küldik a statikus betegadatokat (pl.: név, azonosítószám), a harctéri elsősegélynyújtó, mentőtiszt, orvos feljegyzéseit, illetve a mentőautóban, a beteg állapotával kapcsolatban keletkezett dinamikus adatokat (pl.: várnyomás, pulzus, EKG). A kórház így időben fel tud készülni a traumás beteg katona ellátására (pl.: műtők, szakszemélyzet, specialisták), s arra is lehetősége van, hogy a felhőn keresztül távvezérelje az IoT szenzorokat, illetve letöltesse a mentőautó lokális szerverére a speciális egészségügyi alkalmazásokat (appok) az alkalmazás-konténerekből.

Kiképzés

A katonai kiképzésben a kiterjesztett és virtuális valóságra, illetve egyéb, kevert valóságokra épülő módszerek és eljárások nem ismeretlenek, különösen, hogy a hadtudomány evolúciójában a valós és a virtuális világok egyaránt megjelennek [13]. A pilóták/űrhajósok repülőgép-, illetve űrhajószimulátora, a tantermi/tornatermi körülmények között megvalósított harcászati feladatok (pl.: taktikai tervek realizálása, VV-sisakkal felvértezve a virtuális ellenség megsemmisítése) egyaránt ide sorolhatóak. Az IoT megjelenése és katonai elterjedése annyiban fog változást hozni, hogy a kiképzés valódi terepen történik meg, ahol a különböző szenzorok, s az általuk szolgáltatott és feldolgozott adatok révén a kiképzőtisztek valós időben tudják áttekinteni valamennyi katona tevékenységét, s azonnali visszajelzést tudnak neki adni szükség esetén. A katona ruházatán elhelyezett szenzorok érzékelik majd, ha viselőjét eltalálják, s jelzik, hogy ez a találat az adott virtuális fegyver használata miatt halálos sérülést okozott-e, vagy sem. A katonák folyamatosan rögzített GPS-koordinátái, fiziológiai monitorozásának adatai a hadgyakorlatot követően akár személyre szabottan, akár az adott kötelék közös tevékenységét illetően kielemezhetőek, összevethetőek a kötelék korábbi teljesítményével, s a kiképzők így még jobb tanácsokkal tudják segíteni a katonák szakmai-gyakorlati fejlődését.

AZ IOT ÉS AZ INFORMÁCIÓBIZTONSÁG

Számos szerző ért egyet azzal, hogy a jövőben nagyon sok IoT eszköz veszi majd körül az embert – bár ahogy arra korábban is utaltam az IoT elterjedési dinamikáját illetően komoly

nézeteltérések is vannak. A korábban csak az asztali számítógépekre, majd később a hordozható eszközökre (laptop, tablet, okostelefon) vonatkozó információbiztonsági elvárásokat ki kell terjeszteni az IoT eszközökre és rendszerekre is [14] akár a polgári, akár a katonai felhasználási területekről is legyen szó. Daly [15] négy fontos tanácsot nevez meg a katonai IoT és a biztonság fókuszában. Ezek a következők:

1. Legyünk biztosak benne és ellenőrizzük, hogy az információ hiteles forrásból származik, a rendszereink pedig rugalmasak.
2. Tartsunk lépést a technológiával.
3. Fókuszáljunk a belső fenyegetésekre.
4. Végezzünk folyamatosan adatelemzést.

Az alábbiakban a négy tanács gyakorlati tartalmát ismertetem részletesebben.

Legyünk biztosak benne és ellenőrizzük, hogy az információ hiteles forrásból származik, a rendszerek pedig rugalmasak. A katonai vezetőknek – különösen a katonai információbiztonsággal és kiberhadviseléssel foglalkozó vezetőknek – az IoT által generált hatalmas adatmennyiséggel kapcsolatban fel kell tenniük a kérdést, hogy honnan tudják, hogy a rendszer által generált adatok megbízhatóak? A választ az információbiztonsági stratégiában kell keresniük. Az adatok természetesen kódolt, titkosított formában kerülnek továbbításra az egyes IoT rendszerelemek között. A titkosítás mellett az adatok szétválogatásával és megfelelő csoportosításával is csökkenthető a kockázat. A polgári életben is elterjedt virtuális gép technológia, adatbázis konténerek és egyéb fejlett megoldások a katonai területeken is használhatóak, a katonai fejlesztéseknél és alkalmazásoknál azonban az információbiztonság érdekében a szükségtelen szolgáltatásokat és alkalmazásokat el kell távolítani, s a megmaradt szoftvereket a céloknak megfelelően kell beállítani. Mivel (1) viszonylag sok rendszer épül(t) az IoT kiszolgálása érdekében, (2) a felhőalapú és hagyományos megoldások és szolgáltatások számos operációs rendszer alatt működnek, (3) megannyi felesleges tulajdonság is fut (vagy a tudtunk nélkül futtatható) – ezért a felesleges kockázat szintje magas.

A digitális kor velejárója, hogy egyre több és több, IoT-hez köthető technikai és technológiai újítás jelenik meg, melyek egy része – magától értetődően – ha időben egy kicsit megkésve is, de a katonai területekre is átterjed. A polgári életben, különösen, ha az IoT eszközök sérülékenysége konkretizálható és jelentős anyagi kárral jár, ugyancsak fókuszba kerül a biztonság, a katonai területen azonban ez még markánsabban jelenik meg. Ahogy a katonai rendszerekhez újabb és újabb IoT eszközök csatlakoznak, úgy növekszik a sérülékenység és a fenyegetettség. Ez a biztonsági rések növekvő számában, s ezzel összhangban a katonai szerverek ellen irányuló IoT eszközökkel, vagy azokon keresztül megvalósított támadásokban realizálódik. Szükség van olyan katonai kísérleti laborokra, ahol nem csak az új eszköz és a már meglevő katonai informatikai infrastruktúra kapcsolatát és a kapcsolat sebezhetőségét vizsgálják meg, hanem azt is, hogy a beágyazott rendszerek és rendszerelemek révén milyen adatok keletkeznek, azok hova továbbítódnak, illetve ezek az elemek hogyan kapcsolódnak más eszközökhöz. Ez olyan komoly probléma, amivel a katonai vezetőknek foglalkozniuk kell, különösen azért, mert ha az IoT eszközökkel felruházott katona pillanatnyi adatait (pl.: GPS koordinátái, egészségi állapota, közelében levők száma, egymáshoz viszonyított helyzete) az ellenség megszerzi, akkor a harctevékenység során könnyedén helyzeti előnyre tud szert tenni, vagy akár a katonák kiiktatása révén meghiúsítja az akciót.

Az ellenség információs műveletei az adott kötelék belső rendszereit is érinthetik az IoT eszközök révén. Az összekapcsolt IoT eszközök, s az általuk generált, s a felhőbe küldött adatok, valamint a felhőben végzett adattárolás és adatfeldolgozás révén számos automatizált katonai rendszer működik. Az IoT, mint informatikai rendszer határainak védelme ugyan csökkentheti a fenyegetettség és a kockázat mértékét, de a belső elhárítás révén nem felderített kémek és árulók a digitális kort megelőző korokhoz képest sokkal nagyobb károkat tud-

nak okozni az adatszivárogtatással, az adatok átírásával, az adatfolyam lassításával, vagy blokkolásával, stb.

Az ilyen hibák és (belső) támadások jelentős része kiküszöbölhető lenne azáltal, ha az eddiginél lényegesen szofisztikáltabb és gyakoribb adatelemzést (Big Data Analitika) végeznének a katonai informatikai rendszerekben. A sikeres adatelemzés során számos olyan algoritmus futtatható le, amelyek eredménye segítségével feltárhatóak a rendszerben azok a működési folyamatok, amelyek a nem elvárt és megszokott működésre vezethetőek vissza (pl.: minden ok nélkül hirtelen megnövekszik a felhőből küldött adatok mennyisége az egyik végpont felé). Az analitika arra is lehetőséget biztosít, hogy megjósoljanak (predikció) bizonyos folyamatokat és fenyegetéseket, mielőtt azok megtörténtek volna.

Az IoT és az információbiztonság technikai fókusza mellett érdemes megemlíteni a társadalomtudományos aspektust is. Pomerleau [16] cikkében James Cartwright-ra, az USA Stratégiai és Nemzetközi Tanulmányok Központ védelempolitikai tanulmányokkal foglalkozó részlegének a vezetőjére hivatkozva azt állítja, hogy az IoT, illetve a hozzá kapcsolódó technológiai fejlesztések (pl.: intelligens hűtőszekrények, intelligens termosztátok) gyökeresen fogják megváltoztatni az emberek életét. Cartwright úgy véli, hogy annak ellenére, hogy az IoT több szinten fog hasznosulni akár a polgári, akár a katonai területeken, a fő kérdés nem technikai, hanem kulturális. A biztonság, illetve az eszközök biztonságos használata, valamint a használatukhoz fűződő biztonságtudatosság és annak fejlesztése messze komolyabb feladat, mint a különböző IoT eszközök hardverének a kifejlesztése, illetve a hozzá kapcsolódó megfelelő programkódok megírása.

FEJLŐDÉS ÉS SEBEZHETŐSÉG

Sajnos az IoT eszközök katonai informatikai infrastruktúráját érintő információbiztonsági hiányosságok mellett azzal is számolni kell, hogy az IoT bevezetése és alkalmazása területén lemaradás tapasztalható. Pomerlau [17] Zheng és Carter [9] tanulmányára – melyben 29 kormányzati/katonai és ipari vezető döntéshozó véleményét elemzik – hivatkozva megállapítja, hogy ugyan az IoT (technológiával támogatott) olyan területeken, mint a drónokkal végzett megfigyelés, vagy a felderítés, az USA hadserege a polgári fejlesztésekhez képest előnyben van, általánosságban azonban a polgári élet generálja az IoT fejlesztéseket. Miközben a polgári életben a légjármű-karbantartás, az ellátási lánc menedzsment, vagy az intelligens otthonok területeken megannyi sikeres példával lehet találkozni, addig ezeknek a rendszeres katonai megjelenése és elterjedése még várat magára. Hivatkozott szerzők szerint a jelen valósága az, hogy az adatok gyűjtése és megosztása gyakran attól függ, hogy a mérőeszközök által mért adatok kézi felvitele (vagyis a látott mért eredmények rögzítése valamely informatikai/számítástechnikai rendszerben) mennyire gyorsan történik meg. A másik probléma az, hogy ha meg is történik az adatok rögzítése, a hadsereg sokkal kevesebb tudást és bölcsességet tud ebből kinyerni, mint amennyire egyébként a polgári életben használt algoritmusok és egyéb elemzési módszerek révén lehetősége lenne. A harmadik problémát a széttöredezett és különálló informatikai architektúra jelenti. Ez ugyanis nehézkessé teszi a protokollok és a különböző hálózatok közötti fejlesztéseket, illetve magát a közös használatot is. Negyedik problémaként azt sem szabad figyelmen kívül hagyni, hogy a katonai célú informatikai rendszerek fejlesztése és bevezetése rendszerint a tenderkiírásoktól és a közbeszerzési eljárásoktól függ, aminél gyakran már az igények megfogalmazásakor sem járnak el kellő körültekintéssel és integrált rendszerszemlélettel a katonai felhasználói oldal szereplői.

Campbell [18] úgy véli, hogy a polgári és a katonai informatikai rendszerek összekapcsolódása, vagy legalábbis funkcionális átfedése (pl.: a katonák telefonjain a polgári életben is használatos operációs rendszerek és alkalmazások futnak) sokkal sebezhetőbbé és támadhatóbbá teszi a nem polgári célpontokat, objektumokat. Világviszonylatban megnövekedett a hackerek, a social engineerek, s az általuk a vállalatok, kormányhivatalok ellen elkövetett

támadások száma. A jövőben számítani lehet arra, hogy a katonák és a katonai létesítmények is a támadások fókuszába kerülnek. Nevezett szerző munkájában hivatkozik az egyik, katonai megrendeléseket is kiszolgáló, egészségügyi vállalattal kapcsolatos információbiztonsági tanulmányra, mely megállapította, hogy hackereknek sikerült olyan érzékeny egészségmonitorozási területeken, mint például a kardiológia átvenni az irányítást az eszközök fölött, s manipulálták a gyógyszeradagoló pumpát. Ez előrevetíti annak gondolatát, hogy a harctéren megsebesült katonát az IoT technológiát használó távmonitorozó rendszer eredményes támadását követően akár a halálba is lehet küldeni (pl.: rossz gyógyszer adagolása, vagy túladagolás), mialatt a tábori kórházba szállítják.

Solomon [19] az IoT eszközök fejlesztésével kapcsolatban azon az álláspontonvan, hogy alapvető kritérium – akár van, akár nincs szabvány – hogy a fejlesztők az eddiginél lényegesen nagyobb odafigyeléssel dolgozzanak a biztonság tekintetében. A fejlesztés mellett is nagyobb fókuszt kell, hogy kapjon a biztonság, többek között a statikus kódelemzés (SCA), illetve a statikus alkalmazás-biztonság tesztelés (SAST) során. A fejlesztők és tesztelők információbiztonsági fókusza megtalálható a fejlesztői munkakörnyezetben és a következő előnyökkel jár:

- A programozók olyan fejlesztőkörnyezetben dolgoznak, amelyik elősegíti, hogy a biztonság a fejlesztés valamennyi szakaszában megjelenjen és figyelmet kapjon, így csökken a hanyag kódolásból eredő kockázat.
- Olyan modern, zökkenőmentes fejlesztési módszerek is használhatóak, mint az Agile, a DevOps, vagy a CI (Continuous integration).
- A biztonsági folyamat alapvetően automatizált, mindenki aktívan részt vesz benne. A fejlesztőket a munka megkezdése előtt részletesen felvilágosítják arról, hogy mik a biztonsági alapelvek, amelyeknek meg kell felelniük. Ez különösen a katonai IoT alkalmazások esetében követelmény.
- A fejlesztés során lehetőség van biztonsági küszöbszinteket definiálni. Ennek segítségével ellenőrzőlista-szerűen lehet kontrollálni, hogy az adott lépés, programrész, illetve -elágazás megfelel-e az alapvető biztonsági előírásoknak.
- A biztonságos munkamódszer kedvezően hat a megtérülési mutatóra (ROI), gyorsabban és hatékonyabban lehet a sérüléseket javítani, kevesebbet kell költeni karbantartásra, illetve csökken az adatszivárgásból eredő kár.

EREDMÉNYEK

Tanulmányom legfontosabb eredményének azt tartom, hogy a hivatkozott szerzők véleménye alapján megalapozottnak látom azt a kijelentést, hogy a hálózatos katona az utópisztikus távoli jövőből kézzelfogható távolságba, több területen pedig már a jelen valóságába került. A katonai területen hálózatba kötött emberek, gépek, berendezések, eszközök, járművek, stb. a vezetékes, s egyre gyakrabban vezeték nélküli kommunikációs protokolloknak köszönhetően akkor is képesek a folyamatos kapcsolattartásra, ha földrajzilag egymástól távol helyezkednek el. A katonákról, az általuk használt technikáról, a környezetről az IoT eszközök révén nagyon sok adat gyűjthető össze, ugyanakkor úgy gondolom, hogy a katonai-vezetői döntés támogatásában az IoT technológia még nem játszik döntő szerepet. Ennek okait abban láttam, hogy (1) a szenzorok, a lokális, illetve a távoli adattovábbítás és adatfeldolgozás védelme egyelőre nem megoldott, (2) a keletkezett adatok szofisztikált, szemantikus feldolgozása és közérthető vizuális megjelenése még várat magára, illetve (3) emiatt a katonai vezetés nem tud megbízni a technológiában. Véleményem szerint még egy ok megnevezhető, ami gátolja az IoT katonai elterjedését, ez pedig a róla alkotott meglehetősen heterogén katonai (NATO, USA) álláspontok elegye. Bár tanulmányomban mindvégig kongruens vélemény megalkotására törekedtem, sajnos több helyen is éreztem a publikus nyilatkozatok mögött megtalálható nézetkülönbségeket, melyekről nem gondolom, hogy a kommunikációs hadviselés (tudatos

félrevezetés, összezavarás) része lenne. Legvégül pedig az eredmények között tartom számon azt is, hogy az IoT katonai elterjedésével kapcsolatban rávilágítottam arra, hogy a polgári életben tapasztalt technikai fejlődés/fejlettség szintjéhez képest a katonai fejlődés/fejlettség az IoT területén lemaradást mutat. Ezért is tartottam fontosnak, hogy tanulmányom következő alfejezetében, a „következtetések"-ben nem egy hagyományos summázatát adjam írásművemnek, hanem négy forgatókönyvet vázoljak fel.

KÖVETKEZTETÉSEK

Következtetéseimet tanulmányomban két „tiszta", egy „nem tiszta" és egy „kevert" forgatókönyv köré kívánom rendezni. Kérdéses ugyanis, hogy előbb a polgári/üzleti területeken dolgozó fejlesztők dolgozzanak-e ki az IoT használatára vonatkozó biztonsági megoldásokat (szabványokat), amiket aztán már mint elvileg biztonságosnak mondott rendszereket a katonaság is átvesz, vagy – a hagyományos civil-katonai fejlesztések sémáját alapul véve – a megfelelő biztonsággal ellátott, a katonai elvárásoknak és követelményeknek megfelelő IoT rendszerek majd csak a katonai bevezetést követően jelennek meg a polgári életben.

Ha az első „tiszta" forgatókönyvet vesszük alapul, akkor a katonaság az informatikai technikai/technológiai szintjét tekintve mindig is lemaradásban lesz a polgári területekhez képest. Azzal, hogy az IoT rendszerek/szabványok csak később jelennek meg a katonai területeken azt is jelenti, hogy később ismerkednek meg vele a felelős üzemeltetők, s az adott rendszer gyenge pontjait ismerő polgári (vagy a polgári életből verbuvált) hackerek viszonylag könnyebben tudják feltörni az adott megoldásra támaszkodó katonai rendszereket.

A második „tiszta" forgatókönyv ugyan a katonai információbiztonság fókuszában jónak tűnik, hiszen a katonai területen dolgozók előbb ismerik meg a katonai IoT fejlesztéseket és javítják ki a tesztek során tapasztalt hibákat, tehát a polgári támadók előtt járnak tudásban és tapasztalatban. Ugyanakkor nincs semmi garancia arra, hogy a dinamikusan és exponenciálisan fejlődő IoT területén tevékenykedő fejlesztők és gyártók elsőként a katonai megrendeléseket szolgálják ki, lemondva a polgári megrendelők által kínált nagyobb, globális profitlehetőségéről. Ez a forgatókönyv természetesen nem zárja ki annak a lehetőségét sem, hogy akár nemzeti (pl.: USA), akár szövetségi (pl.: NATO, Visegrádi Négyek) szinten a kimondottan hadiiparra szakosodott vállalatok akár katonai műszaki egyetemekkel, karokkal, tanszékekkel közösen dolgozzanak az IoT fejlesztéseken, de a publikusan elérhető információk alapján erre jelenleg nem nagyon lehet példát találni.

A „nem tiszta" forgatókönyv szerint vannak és lesznek olyan területek – amelyekre már a jelen tanulmányomban is utaltam – amelyeken a katonai fejlesztések dominálnak, s csak ezek katonai bevezetése után jelenik meg az IoT haditechnika (akár egyszerűbb változatban is) a polgári életben. Az információbiztonság szempontjából ez jó megoldásnak tűnik, de nem csökkenti jelentős mértékben az informatikai eszközökre és megoldásokra épülő haditechnikai ágazatok lemaradását a polgári informatikai fejlesztésekhez képest.

A „kevert" forgatókönyv szerint a hadiipari fejlesztésekben polgári és katonai szereplők (katonai és polgári egyetemek, vállalatok, programozó csapatok, projektek, stb.) szoros együttműködés révén vesznek részt, ami azt jelenti, hogy a fejlesztési eredmények közel azonos időben jelennek meg a katonai és a polgári alkalmazásokban. Ez egyfelől elősegíti, hogy a katonai informatikai rendszereket üzemeltetők időben némiképp előbb ismerjék meg a fejlesztési eredményeket, mint a támadók, ugyanakkor felveti az információbiztonság fogalmát egy másik dimenzióban. A többszereplős fejlesztésekben a csapattagok nem azonos megbízhatósági szinten vannak. A nemzetbiztonsági átvilágításon átesett egyetemi oktatók, katonai vállalatok fejlesztői magasabb megbízhatósági szintet képviselnek azokhoz képest, akik szabadúszóként csatlakoznak a polgári fejlesztőkhöz. Az ő esetükben meglátásom szerint ugyan olyan átvilágítás szükséges. Kérdéses persze, hogy egy lezser, a szabadsághoz maximálisan ragaszkodó Z generációs programozó (aki kreativitásában akár messze felülmúlja a többi,

idősebb csapattagot) engedélyezi-e az átvilágítást, illetve elfogadja-e a munkavégzéssel kapcsolatos, számára feleslegesnek tűnő szigorításokat és szabályokat, vagy a felismerve a területen világviszonylatban tapasztalható munkaerőhiányt, idő előtt továbbáll.

A négy forgatókönyv közül meglátásom szerint a modern, infokommunikációs eszközöket használó hadseregek számára a „kevert"forgatókönyv nyújtja a legnagyobb innovációs potenciált. Ha ez az előny kellő információbiztonsággal és biztonságtudatossággal társul, akkor összességében optimális megoldás születhet.

FELHASZNÁLT IRODALOM

[1] KENNY, R.: *All Seeing Sensors – It's About the Data, Stupid*; https://militarycommunicators.org/2015/07/14/all-seeing-sensors-its-about-the-data-stupid (letöltve: 2017.10.10.)

[2] SELTZER, L.: *The internet of military things: Logistics dream, security nightmare?*; http://www.zdnet.com/article/the-internet-of-military-things/ (letöltve: 2017.10.10.)

[3] MUNK S.: *Kritikus információs infrastruktúrákhoz kapcsolódó, sajátos katonai (védelmi szférabeli) képességeket igénylő feladatok*; Hadmérnök, III. évfolyam, 3. szám (2008) 130-146 o.

[4] MUNK S.: *A kritikus infrastruktúrák védelme információs támadások ellen;* Hadtudomány, 2008/1-2. 95-106. o.

[5] SURI, N. – TORTONESI, M.: *Session 13: Military Internet of Things (IoT), Autonomy, and Things to Come*; https://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/57e41eac8419c2f2791befb5/1474567857321/Panel+-+Military+IoT%2C+Autonomy%2C+and+Things+to+Come.pdf (letöltve: 2017.10.10.)

[6] FEARN, N.: *US Army is using IoT tech and data to transform warfare;* https://internetofbusiness.com/us-army-iot-warfare (letöltve: 2017.10.10.)

[7] MURISON, M.: *DARPA wants to militarise the IoT;* https://internetofbusiness.com/darpa-wants-militarise-iot (letöltve: 2017.10.10.)

[8] NATO**:** Military Applications of Internet of Things (IST-147). 2015. https://www.cso.nato.int/activity_meta.asp?act=8647 (letöltve: 2017.10.10.)

[9] ZHENG, D. E. – CARTER, W. A.: *Leveraging the Internet of Things for a More Efficient and Effective Military;* CSIS (Center for Strategic and International Studies), 2015.

[10] KOLLÁR Cs.: *IOT A GYAKORLATBAN, AZ INFORMÁCIÓBIZTONSÁG FÓKUSZÁBAN I. Az IoT működése, fejlődési tendenciái;* Bolyai Szemle (kézirat megjelenésre elfogadva)

[11] HAIG Zs. – VÁRHEGYI I.: *Hadviselés az információs harcszíntéren;* Zrínyi Kiadó, 2005.

[12] PURI, D.: *Mobile IoT provider applies military techniques to improve IoT resiliency;* http://www.networkworld.com/article/3122129/internet-of-things/mobile-iot-provider-applies-military-techniques-to-improve-iot-resiliency.html (letöltve: 2017.10.10.)

[13] FEKETE K.: *Evolution of Military Science: Real and Virtual World;* Fekete Károly (szerk.): Kommunikáció 2015: Communications 2015. NKE Szolgáltató Kft., 2015, 141-148 o.

[14] KUMAR, S.: *Who Hacked Into Your Smart Device?* http://electronicsofthings.com/expert-opinion/hacked-smart-device (letöltve: 2017.10.10.)

[15] DALY, M. K.: *Internet of Things: 4 Security Tips From The Military;* http://www.darkreading.com/mobile/internet-of-things-4-security-tips-from-the-military/a/d-id/1297546 (letöltve: 2017.10.10.)

[16] POMERLEAU, M.: *For the military, the Internet of Things isn't about 'things';* https://defensesystems.com/articles/2015/11/12/internet-of-things-dod-cartwright-csis.aspx?m=1 (letöltve: 2017.10.10.)

[17] POMERLEAU, M.: *Report: Military lagging in IoT adoption;* https://gcn.com/articles/2015/09/25/military-lags-internet-of-things.aspx (letöltve: 2017.10.10.)

[18] CAMPBELL, S.: *Military Security in the Age of the Internet of Things;* http://www.afcea.org/content/?q=Article-military-security-age-internet-things (letöltve: 2017.10.10.)

[19] SOLOMON, S.: *Internet of Things (IoT) – Hack My Army;* https://www.checkmarx.com/2016/03/14/internet-things-iot-hack-army (letöltve: 2017.10.10.)