Horváth Attila

A létfontosságú rendszerelemek és a technológiai fejlődés új kockázatai II. rész

(Kölcsönhatások és a mesterséges intelligenciák elterjedésének kihívásai)

DOI 10.17047/HADTUD.2016.26.E.216

Rezümé:
A tanulmány az utóbbi évtizedekben megváltozott felfogások alapján áttekinti a biztonságot veszélyeztető kockázati tényezőket. A szerző korábbi kutatásaira alapozva és az újabb kutatási eredményeként a tanulmány részletesen elemzi a kritikus infrastruktúrák (létfontosságú rendszerelemek) működésével kapcsolatos veszélyeket. A létfontosságú rendszerelemek kölcsönhatásainak vizsgálatával bizonyítja egy átfogó biztonsági szemlélet elterjesztésének szükségességét. A szerző új típusú biztonsági kockázatok közül a mesterséges intelligenciák társadalmi, katonai és etikai kockázatait vizsgálja.
Kulcsszavak:
kölcsönhatások; technológia fejlődés; mesterséges intelligencia.

Horváth, Attila

New Risks of Critical Infrastructure and Technological Development. Part II. (Challenges of Interdependence and the Evolution of Artificial Intelligence)

Abstract:
This study reviews the factors of security risks, in the light of the changing perceptions in the last decades. It analyses the hazards for the operation of critical infrastructure systems in detail, based on the previous and current research results by the author. With the investigation on the interactions between critical systems elements, he provides the evidence for the necessity of spreading a comprehensive security approach. Among the new type of security hazards, the author examines the societal, military and ethical risks relevant with the appearance of artificial intelligence.
Key words:
interdependencies; technological development; artificial intelligence.

A tanulmány első részében áttekintettem a megváltozott biztonság felfogás és annak szemlélete elterjedésének okait. Túllépve a hagyományosnak tekinthető biztonság kockázatokon elsősorban a létfontosságú rendszerelemek (kritikus infrastruktúrák) biztonsági kockázatai mellett a technológiai fejlődés újszerű kihívásait vizsgáltam.

A második részben esettanulmányokra alapozva mutatom be a kritikus infrastruktúrák kölcsönhatásaiból eredő kockázatokat. Részletesen kitérek a mesterséges intelligencia elterjedésének a társadalomra, a gazdaságra, és hadügyre gyakorolt várható hatásokra és megoldandó problémákra.

A kritikus infrastruktúrák kölcsönhatásaiból eredő kockázatok

A korábbiakban már kitértem arra, hogy a kritikus infrastruktúrák egyes ágazatai és alágazatai hálózatosan kapcsolódnak egymáshoz. Ez azt is jelenti, hogy az egyik alrendszerben bekövetkező rendkívüli események következményei akár a teljes létfontosságú rendszert érinthetik. A térbeli hatásokat nem könnyű behatárolni, emiatt a hatékony kritikus infrastruktúra védelmet csak nemzetközi együttműködésben lehet kiépíteni és megbízhatóan működtetni. A hagyományos nemzetbiztonsági kategóriákban való gondolkodással sem a kibertérben, sem a valóságos fizikai térben nem lehet megelőzni a káreseményeket, illetve felszámolni a következményeket.[1] Ez a megállapítás különösen igaz Európára, ahol az infrastrukturális rendszerek határokat átívelve szervesen kapcsolódnak egymáshoz.

A földrajzi kitettség határa lokális, regionális, országos, kontinentális, de akár globális léptékű is lehet. A térbeli kitettség mértékének növekedését jól szemlélteti a Japán partjai közelében 2011. március 11-én bekövetkezett földrengés és az azt követő szökőár. A kettős eredetű természeti katasztrófa súlyosan megrongálta a fukusimai atomerőművet. A rendkívül súlyos nukleáris következményeket ugyan sikerült csökkenteni, de a közvetett hatások a rendkívüli eseménysorozat második- és harmadik hullámában még a szakembereket is meglepték. A közvetett következmények hamarosan energia-ellátási nehézségeket okoztak, amely a gazdaság működését is nehezítette.

A fukusimai katasztrófa közvetett hatásainak tapasztalatai egyben rámutattak arra, hogy a különösen fontos kritikus infrastruktúránál bekövetkező rendkívüli események káros következményei hullámszerűen jelentkezhetnek. Az is igazolódott, hogy a harmadik hullámig akár növekvő, de azt követően csökkenő hatásokkal számolhatunk.[2] Ezt történt 2011-ben Japánban is. Az első hullámban nyilvánvalóan a nukleáris katasztrófa hatásait kellett csökkenteni, mert az atomerőmű kiesése miatt a szigetországban korlátozni kellett az energia felhasználást. Ennek viszont az lett a közvetett eredménye, hogy a második és a harmadik hullámban jelentkező hatások messze túlmutattak a szigetország határain. Azzal kellett számolni ugyanis, hogy globális szinten az információs technológiában kulcsszerepet betöltő üzemek az energiakorlátozások miatt nem tudnak megfelelő mennyiségben és minőségben termelni és a kulcsfontosságú részegységeket a gyártóknak leszállítani.

Az ellátási láncokban keletkezett zavarokon viszonylag rövid idő alatt sikerült úrrá lenni, de a zavaró hatások szinte az egész világon érezhetők voltak. A közgazdászok azzal is számoltak, hogy a 2008-ban kezdődő gazdasági válságból való kilábalást megnehezítheti a japán IT-iparban keletkezett zavar.[3]

A nemzetközi szakirodalomban kritikus infrastruktúrák interdependenciáinak (kölcsönhatásainak) öt fajtáját különböztetjük meg úgy, mint:

- logikai kölcsönhatások;
- eljárásrendi kölcsönhatások;
- fizikai kölcsönhatások;
- kiber kölcsönhatások;

[1] Fjäder, O. Chirstian: National Security in a Hyper-connected World. Global Interdependence and National Security. In.: Masys, J Anthony (ed). Exploring the Security Landscape: Non-Traditional Security Challenges. Springer, pp. 31–58. DOI 10.10007/978-3319-27914-5. (letöltve: 2016. 04.02.).
[2] Horváth Attila – Csaba Zágon: Critical Transport Infrastructure Protection: A Reserach on the Security of the Supplay Chains. Economics and Management 2015: (2) pp. 47–54.
[3] Horváth Attila: i.m.

– földrajzi kölcsönhatások.[4]

A *logikai kölcsönhatások* azt fejezik ki, hogy egy ágazat vagy alrendszer állapota mennyiben függ egy másiktól. Gyakorlatilag az infrastruktúrák összekapcsolódásának a mechanizmusait és módját kell érteni alatta térben és időben. Az *eljárásrendi tényezőkön* azokat az eljárásokat és intézkedéseket értjük, amelyek a rendkívüli események megelőzésére-, eszkalálódásának megakadályozásra- és felszámolására irányulnak, illetve a későbbiekben bekövetkező hasonló esetek megelőzésére hivatottak. A *földrajzi kölcsönhatások* az adott környezetben a létfontosságú rendszerek bemenetei és kimeneti kapcsolatait fejezik ki, de nem terjednek ki a térbeli kölcsönhatásokra, mert egy esetleges káresemény kiterjedésének nagyságát a logikai szempontokkal jellemezzük. A *fizikai kölcsönhatások* az egyes ágazatok és alágazatok jellemzőiből fakadó kapcsolatrendszerére, pontosabban fogalmazva kitettségre utalnak. A *kiber tényezőket* a kockázatok oldaláról a legkönnyebb érzékeltetni és megértetni. Napjainkban gyakorlatilag nincs olyan kritikus infrastruktúra ágazat vagy alágazat, amelynek irányításában az információs technológiák ne játszanának szerepet. Így egy esetleges sikeres hackertámadással viszonylag könnyen lehet zavart kelteni.[5]

A kritikus infrastruktúrák egyes ágazatai leginkább a villamos-energetikai rendszertől és a telekommunikációs rendszerektől, illetve a kiberkockázatoktól függnek. Túlzás nélkül kijelenthető, hogy az elektromos áramkimaradások következményei minden szektorra hatnak. Gyakorta előfordul az is, hogy áramkimaradás okát viszonylag rövid idő alatt sikerül megszüntetni, de más területeken a következmények felszámolása még esetleg sokkal hosszabb időt is igénybe vehet.[6] Állításomat jól szemléltetik a 2003. augusztus 28-ai londoni áramszünet tapasztalatai. Emberi mulasztás az áramszolgáltatás mindössze 30 percnyi kimaradását okozta, de még órákon keresztül kellett a liftben és a metróalagutakban rekedteket kimenteni, a nagyváros vasúti közlekedése pedig csak órák múlva állt helyre.[7]

Az áramkimaradások hálózatos kölcsönhatásait jól szemlélteti a 2003. szeptember 28-án hajnalban bekövetkező, Olaszországban és Svájcban jelentős fennakadásokat okozó, de Franciaországot, Ausztriát és Szlovéniát is érintő villamos-energetikai ellátási zavar is.[8] Az áramkimaradás közvetlen következményeinek köszönhetően mintegy 56 millió ember maradt áramszolgáltatás nélkül, több mint 30 000 ezer ember ragadt – többségük a nyílt vonalakon – a vonatszerelvényekben, több száz embert kellett a különböző városok metróalagútjaiból kimenteni.[9]

A kölcsönhatásokra visszavezethető közvetett következmények jól szemléltetik a kritikus infrastruktúrák villamos-energetikai alágazattól való függőségét:

– az internet-előfizetők nem tudtak csatlakozni a szerverekhez, a telekommunikációs rendszer többi szektorában is zavarok keletkeztek, de kritikus helyzet nem állt elő;

[4] Little, G. Richard: Managing the Risk of Cascading Failure int the Complex Urban Unfrastructures. In.: Graham Stephen (ed). Disrupted Cities. Routledge, Taylor& Francis Group. New York, London, 2010. pp. 27–39.
[5] Xu, Tie – Masys, J. Anthony: i.m. (2016).
[6] Horváth Attila – Csaba Zágon: i.m. (2012).
[7] Horváth Attila – Csaba Zágon: i.m. (2012).
[8] Learning from the Blackouts. Transmission System Securityin Competitive Electricity Markets. International Energy Agency and OECD, Paris, 2005. 216 p. URL cím: http://www.iea.org/publications/freepublications/publication/blackouts.pdf (letöltve: 2016. 03.19.).
[9] Xu, Tie – Masys, J. Anthony: i.m. (2016).

– az energia ellátás többi szektora (például a gázszolgáltatás, vagy az üzemanyag kiszolgálás) instabillá vált;
– a szivattyúk leállása miatt a vízszolgáltatás szünetelt, de az élelmiszer ellátásban is zavarok alakultak ki;
– a közúti közlekedésben a legnagyobb zavart az okozta, hogy a forgalomirányító lámpák nem működtek, ez lassította az időközben szükségessé váló ivóvízszállításokat és a betegek kórházba juttatását;
– a vasúti közlekedés gyakorlatilag megbénult, az utasokat a vonatszerelvényekből kellett kimenteni;
– a légiközlekedésben az áramszolgáltatás szünetelése miatt érintett repülőterek nem voltak képesek a repülőgépeket fogadni, ezért a járatokat tömegesen törölni kellett.[10]

A vasúti közlekedéssel kapcsolatos közvetett következményekkel kapcsolatban „a mi lett volna ha” kérdésnek nem csak létjogosultsága van, hanem fontos tényezőként kell kezelni. Az áramkimaradás ugyanis vasárnap hajnalban (valamivel három óra után) történt. Abban az esetben, ha az áramkimaradás hétköznap, a közlekedési csúcsidőkben történt volna, nagyságrendekkel több utast kellett volna kimenteni a vonatszerelvényekből és a metrók alagútjaiból.

Az elsősorban Svájcot és Olaszországot majdnem 48 órán keresztül érintő áramkimaradás is bizonyítja, hogy a villamos energia-ellátás zavarai milyen fennakadásokat és kellemetlenséget tudnak okozni az emberek mindennapjaiban. A fejlett országok társadalmaiban élők hozzászoktak a magas szintű szolgáltatásokhoz. A technológiai fejlődés eredményeként az egyének, a háztartások, az intézmények és a szolgáltató, valamint a termelési szféra létesítményei áramszolgáltatástól való függősége jelentős mértékben nőtt. Így a közvetett hatásokat sokkal – akár össztársadalmi szinten is – nehezebben viselik.

Terjedelmi okok miatt a kritikus infrastruktúrák kölcsönös függőségének részleteit nincs módomban bővebben kifejteni. A szakmai és az érthetőségi szempontok alapján azonban úgy vélem, hogy a kiberkockázatok és a telekommunikációs rendszerektől való függőség rövid tárgyalása elengedhetetlen. A kockázat több mint két évtizede valós veszélyt jelent még Magyarországon is. Erre Kovács László és Krasznay Csaba 2010-ben egy szélesebb körben elérhető, másodközlés formájában megjelenő rövid tanulmánya keltette fel igazán a biztonságpolitikával foglalkozó kutatóműhelyek és kutatók figyelmét. Az Egyesült Államokban megjelenő tanulmány a digitális Pearl Harbor lehetőségét vázolta fel. A cikkben megfogalmazottak alapján végeztek el egy kutatást Magyarországon is. Fontos megjegyezni, hogy a kutatókat az Észtország elleni 2007 áprilisában végrehajtott kibertámadás tapasztalatai is motiválták. Ezek arra mutattak rá, hogy az elosztott túlterheléses hacker-támadások komoly veszélyt jelenthetnek akár egy ország működőképességére is. A cikk szerzői egy esetleges „digitális Mohács” forgatókönyv kockázataira akarták felhívni a figyelmet. A széles nyilvánosság számára is elérhető cikknek így is sokkoló hatása volt. [11]

A magyarországi kiberbiztonsággal foglalkozó kutatások a tanulmány megjelenése óta nagy utat jártak be és túlzás nélkül kijelenthető, hogy nemzetközi mérce szerint is számottevőek. Ez érvényes a kérdéskörhöz tartozó rendvédelmi szervekre is. A kibervédelemmel foglalkozó, nemrégiben átszervezett Nemzeti

[10] Xu, Tie – Masys, J. Anthony: i.m. (2016).
[11] Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság III. évfolyam 1. szám, 2010. február, pp. 44–56.

Biztonsági Felügyelet a világ élvonalához tartozó titkosszolgálati szakszolgálatnak számít. A kérdéskörrel foglalkozó civil kutatók már olyan veszélyekre is felhívják a figyelmet, mint például a mindennapjainkat segítő alkalmazásoknak az egyéni és közösségi biztonságot veszélyeztető tényezői.[12]

Az elmúlt években arra is volt példa, hogy szervezett bűnözői csoportok a kritikus infrastruktúrák informatikai biztonsági réseit kihasználva a kibertámadások módszerét alkalmazták extra profitszerzésre. A belga szövetségi rendőrség 2013-ban jelentette be, hogy csak évekig tartó nyomozás után tudta felszámolni azt a szervezett bűnözői csoportot, amelynek sikerült betörnie Európa egyik legfontosabb kikötőjének logisztikai informatikai irányítási rendszerébe. A bűnözők rendkívül egyszerű módszert alkalmaztak: a kiszemelt vagy az általuk küldött (általában kábítószerrel vagy fegyverrel megrakott) konténereket Antwerpen kikötőjéből a számukra kedvező átvételi helyekre irányították. Ezt úgy tudták elérni, hogy az informatikai rendszerben nehezen észlelhető módosításokat hajtottak végre. Természetesen az így ellopott konténerek címzettjei bejelentették a küldemények eltűnését, de évekbe telt, amíg a 12 fős szervezett bűnözői csoportot felfedték. A csoport tevékenysége nemcsak azzal okozott kárt, hogy a legális konténerforgalomból küldeményeket loptak el. A bűnözők letartóztatásakor ugyanis a hatóságok Belgiumban és Hollandiában több tonna kábítószert, kiberbűnözésben használatos eszközt és tekintélyes mennyiségű lőfegyvert és lőszert foglaltak le.[13] Ez az eset is rámutat a közlekedési rendszer és az ellátási láncok sérülékenységére. A biztonsági réseket kihasználva egy terrorcsoport viszonylag könnyen tragikus következményekkel járó terrorakciókat tud végrehajtani a közlekedési alágazatok irányítási rendszerének megzavarásával.

A kritikus infrastruktúrák biztonságával kapcsolatban alapkérdésként jelentkezik a megbízható működés és a sérülékenység vizsgálata. Csak így lehet beazonosítani a létfontosságú rendszerelemek működésének kockázatait. A kölcsönös függőség, az egymástól való kitettség mértékét egy viszonylag újnak számító tudományterület, a „hálózatológia” módszerével lehet meghatározni. Az Erdélyben született, magyar származású Barabási Albert László által kidolgozott skálafüggetlen hálózatokkal meg lehet határozni azoknak a kritikus infrastruktúráknak a gyenge láncszemeit, ahol a rendkívüli események bekövetkezhetnek. A módszer annak feltárására is alkalmas, hogy a beazonosított kritikus rendszerelem kiesése hol veszélyezteti az emberi életeket, illetve hol okozhat anyagi kárt.[14] A hálózatológia alkalmas a kockázatok elemzésére, alapját képezheti a megelőzés, a kárelhárítás és a károk felszámolása során alkalmazható eljárásoknak és protokolloknak.

A kockázat elemzésekor olyan kérdésekre kell választ találni, hogy mekkora a rendkívüli események bekövetkezésének valószínűsége, illetve azoknak milyen várható közvetett és közvetlen következményei lehetnek. Vizsgálni kell azt is, hogy a

[12] Bányász Péter: A közlekedést támogató alkalmazások biztonsági aspektusai. In.: Horváth Attila – Bányász Péter – Orbók Ákos (szerk). Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről. Nemzeti Közszolgálati Egyetem, Budapest, 2014. pp. 47–60.

[13] Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In.: Csengeri János – Krajnc Zoltán: Humánvédelem – békeműveleti és veszélyhelyzeti-kezelés eljárások fejlesztése. (Tanulmánygyűjtemény I., e-book), Nemzeti Közszolgálati Egyetem, Budapest, 2016. pp. 643-672 URL cím: http://real.mtak.hu/33554/1/tanulmanygyujtemeny%20_ujratervezes_CsJ_KZ_1.5.pdf (letöltve: 2016. 03. 11.).

[14] A skálafüggetlen hálózatokról és a hálózattudomány alkalmazhatóságáról lásd bővebben: Barabási, Albert-László: Behálózva. Második, bővített és átdolgozott kiadás. Helikon Kiadó, Budapest, 2008. 320 p.

keletkezett károk térben és időben hogyan és milyen mértékben fejtik ki a hatásukat. A sérülékenység elemzésekor arra is ki kell térni, hogy az esetlegesen bekövetkező károknak milyen társadalmi, környezeti, intézményi, kulturális és természeti hatásai lehetnek.[15] A komplex megközelítésre azért van szükség, mert a rendkívüli események bekövetkezésekor nem elégséges a közvetlen következményeket felszámolni. A másodlagos következmények hosszabb idő távlatában súlyosabbak lehetnek, mint az elsődleges hatások.

A mesterséges intelligenciák alkalmazásának biztonsági kockázatai, ezek kezelési lehetőségei

Az új típusú biztonsági kockázatok tárgyalásakor hiba lenne csak a technológia fejlődés kihívásaira koncentrálni. A globális méreteket öltő éghajlatváltozásnak a biztonságra gyakorolt hatásai többszörösen összetett problémákat vetnek fel.[16] A tanulmány megírása előtt nem tekintettem célomnak, hogy az új típusú biztonsági kockázatok teljes körű elemzésével foglalkozzam. Az éghajlatváltozás azonban olyan biztonsági kihívásokat rejt magában, amelyeknek a megemlítését nem lehet megkerülni.

A globális felmelegedéssel kapcsolatos kihívások egyrészt természeti eredetűek, másrészt a várható negatív hatásokhoz a széndioxid kibocsátás nagymértékben hozzájárul: megváltoznak az ökológiai jellemzők; a tengerszint várható emelkedése miatt csökken az élettér, amely olyan meghatározó megavárosokat is érint, mint például London vagy New York. A természeti környezet megváltozása mellett – amely kétségkívül rugalmasságot kíván a társadalmi és gazdasági szektor minden területén – komoly kockázatokkal jár az is, hogy az elsivatagosodás vagy a vízhiány miatt egész térségek válhatnak az emberi civilizáció számára által nehezen elviselhető területté. Így a milliókat érintő, tömeges migráció reális veszélyt jelent.

A technológia fejlődés[17] valós kockázatait meghatározni nagyrészt még mindig a futurológia kategóriájába tartozik. Vincent C. Müller egy tanulmányában arra hívja fel a figyelmet, hogy a mesterséges intelligencia elterjedésével egzisztenciális kockázatok mellett komoly etikai problémákkal is számolni kell.[18] Nyilvánvaló, hogy a hadviselés az egyik fő terület, ahol a technológiai fejlődés eredményeit felhasználják majd. A haderők ugyanis napjainkban, ha kis késéssel is, de viszonylag rugalmasan tudnak igazodni a technológiai fejlődéshez és a hadműveleti körülményekhez.[19]

---

[15] Xu, Tie – Masys, J. Anthony: i.m. (2016).

[16] Földi László: Az éghajlatváltozás hatása a biztonságra és a katonai erő alkalmazására, a hadviselés ökológiai kérdései. In.: Csengeri János – Krajnc Zoltán: Humánvédelem – békeműveleti és veszélyhelyzeti-kezelés eljárások fejlesztése. (Tanulmánygyűjtemény I., e-book), Nemzeti Közszolgálati Egyetem, Budapest, 2016. pp. 550-615. URL cím: http://real.mtak.hu/33554/1/tanulmanygyujtemeny%20_ujratervezes_CsJ_KZ_1.5.pdf (letöltve: 2016. 03. 23.).

[17] A technológiai fejlődés kockázataihoz sorolja még a szintetikus anyagok elterjedését és a napjainkban zajló „biológiai forradalom” eredményeit is, például a gén-technológia fejlődése révén a gén módosított élelmiszerek elterjedését.

[18] Müller, C. Vincent: ‘Editorial: Risks of artificial intelligence’. in Vincent C. Müller (ed.), Risks of general intelligence. London: CRC Press – Chapman & Hall, 2016 pp. 1–8. URL cím: http://www.sophia.de/pdf/2015_AI-Risk_Editorial.pdf (letöltve: 2016. 05. 21.).

[19] Jobbágy Zoltán: A háború antropológiája: primitív hadviselés, gerilla hadviselés és a szövetséges összhaderőnemi műveletek sikere. Hadtudomány 2015. évi E-szám pp. 67–78.

Ugyanakkor az is kijelenthető, hogy a technológiai fejlődés etikai és egzisztenciális kockázatai messze túlmutatnak a biztonságpolitika problémakörén, de kétségtelenül biztonsági kérdéseket is felvetnek. Ezt egy hadtudományi probléma felvetésével lehet leginkább illusztrálni. Katonai szempontból az egzisztenciális kockázatokat nem tartom olyan súlyúnak, mint az etikai problémákat és a nemzetközi és hadijogi aggályokat. A fejlett haditechnikai eszközökkel rendelkező haderőknél ugyanis a kiszolgáló és támogató erők létszámaránya magas és valószínűleg az is marad. Sokkal inkább fontosnak tartom az etikai és nemzetközi hadijogi vonatkozásokat. A technológiai fejlődés irányai és üteme felveti azt a kérdést, hogy ki lesz a felelős olyan esetekben, ha a jövőben magas vagy önálló intelligenciával rendelkező fegyverrendszerek emberiség elleni bűncselekmény végrehajtására kapnak utasítást, illetve az adott körülmények között a harcfeladat mindenáron való teljesítése érdekében követnek el háborús bűncselekményt. Ezeknek a kérdéseknek a megválaszolására a politika-, a jog- valamint a hadtudománynak már napjainkban kell kutatásokat végeznie.

Az Egyesült Államok haderőiben a mesterséges intelligenciával kapcsolatos kutatások már nem a jövőt, hanem a napjainkban is folyó kutatások egyik főirányát jelentik. A jelenlegi harmadik offset-stratégia meghirdetésekor Chuc Hagel védelmi miniszter kijelentette, hogy az „*ismételten megváltoztatja a játékszabályokat*”.[20] A témával kapcsolatban a Hadtudomány 2006/1–2. számában Porkoláb Imre közölt figyelemreméltó cikket. A kutató szerint a fejlesztések iránya már messze meghaladja hadszíntéri jelek és nagymennyiségű adatok elemzésének kereteit. A kutatási célok között szerepel:

- az ember és gép közötti együttműködés;
- gépek által támogatott műveletek;
- fejlett ember–gép közös egységek;
- hálózatalapú „félautonóm” fegyverrendszerek rendszerbe állítása és alkalmazása.[21]

Napjaink hadügyi forradalomára hívja fel a figyelmet Szenes Zoltán is, amelynek a jellemzőit Haig Zsolt és Várhegyi István korábbi kutatásaira alapozva az alábbiakban látja:

- a tudomány és technológiai eredményeinek intenzív felhasználásában;
- a miniatürizált atomfegyverek elterjedésében;
- high-tech fegyverek elterjedésében;
- a precíziós és integrált fegyverrendszerek elterjedésében;
- a személyzet nélküli robotok alkalmazásában;
- a lopakodó technológia fejlődésében;
- a műholdas felderítő, navigációs és híradórendszerek fejlődésében;
- az információs hadszíntér, a digitális hadszíntér és a hálózatos katona szemlélet elterjedésében;
- az informatikai rendszerek harcászati elterjedésében;
- a korszerű felderítési és vezetési rendszerek fejlesztésében.[22]

Szakértők szerint a polgári életben az intelligens eszközök aránya elérheti az 50%-ot. Az eszközök birtoklása komoly politikai, gazdasági és katonai

[20] A harmadik offset-stratégiáról lásd bővebben: Porkoláb Imre: Az innováció hatása a hadviselésre. Hadtudomány 2016/1-2. szám. pp. 19–27.
[21] Porkoláb Imre: i.m. (2016).
[22] Szenes Zoltán: Tudomány és a korszerű haderő. Magyar Tudomány. 2015, 2. szám. pp. 194–201.

hangsúlyeltolódásokat eredményezhet.[23] A mesterséges intelligenciák kontroll nélküli alkalmazása nagy veszélyt jelenthet az emberiség számára. Az oxfordi székhelyű Future of Humanity Institut kutatói egy 2014-ben publikált tanulmányukban osztják Stephen Hawkingnak azon álláspontját, miszerint a tudósoknak a biztonsági kockázatokról tájékoztatni kell a politikusokat és a közvéleményt, akár olyan anonim pontok létrehozásával is, ahol a kutatók jelezhetnék az aggályaikat. Megelőzésként olyan megoldásokat is javasolnak, hogy a politikai elit vegye figyelembe a jövő generációk érdekeit és a technológiai fejlődéssel kapcsolatos indokolatlanul rövidtávú döntések meghozatalától tekintsenek el.[24] Ezzel kapcsolatban felvetődhet az a kérdés, hogy a politikai elitek mennyiben vannak tisztában a technológiai fejlődés etikai és egzisztenciális kockázataival. Tartok tőle, hogy kevésbé. Véleményem szerint ezzel a fontos kérdéssel még vezető politikusok sem foglalkoznak igazán, de empirikus kutatás hiányában az álláspontomat nem tudom igazolni.

A fejlett országok többsége rendelkezik a mesterséges intelligenciák elterjedésével kapcsolatos problémák kezelésének stratégiájával. A 2015-ben publikált japán *robot stratégia* hangsúlyosan foglalkozik a biztonsági kihívásokkal. A stratégia készítői, abból indulnak ki, hogy a biztonsági kockázatok számbavételéhez nem elég a jelenlegi technológiákból kiindulni. Fontosnak tartják, hogy a szabályozás előzze meg, vagy legalább tartson lépést a fejlődés ütemével. A biztonsággal kapcsolatos szabályok kidolgozásánál globális szintű szabványosítást tartanak szükségesnek. Kiemelten kezelik a vizsgálati módszerek és a kockázat elemzési eljárások bevezetését, ebben a tekintetben is a szabványosítást és a biztonságtechnikai információk gyűjtését tartják szükségesnek.[25] Azzal is egyet lehet érteni, hogy a katonai jellegű kutatásoknak és technológiai fejlesztéseknek új típusú menedzsment szemléletre van szükség.[26] Ellenben a biztonság és az etikai szempontoknak is fel kell értékelődniük.

Egzisztenciális szempontból az informatika és az automatizálás már rövid időn belül azt eredményezheti, hogy a jelenlegi munkahelyek tömegesen kerülhetnek veszélybe. Egy, az Európai Szakszervezeti Intézet által közzétett tanulmány szerint – egy kutatás eredményeire hivatkozva – az automatizálás miatt európai átlagban a munkahelyek 54%-a szűnhet meg. Az egyes országok közötti viszonylag nem túl nagynak tekinthető eloszlási prognózis bekövetkezése még tovább növelheti a centrum és a perifériához sorolható országok közötti különbségeket. Ennek szemléltetésére néhány példa. A Frey és Osborn által készített prognózisból az Európai Unió fejlett országai közül Németországban 51,12%, Franciaországban 49,54%, Hollandiában 49,50%, a fejletlenebb államok közül Bulgáriában 56,56%, Romániában 61,93% lehetséges munkahelyvesztést prognosztizáltak.[27] Igaz, az

[23] Unprecedented Technological Risks. Future of Humanity Institut. Oxford. 2014. 12. URL cím: https://www.fhi.ox.ac.uk/wp-content/uploads/Unprecedented-Technological-Risks.pdf (letöltve: 2016. 05. 11.). (a továbbiakban: Unprecedented Technological Risks 2012.).

[24] : Unprecedented Technological Risks 2012.

[25] New Robot Strategy. Japan's Robot Strategy Vision, Strategy, Action Plan. The Headquarters for Japan's Economic Revitalization. k.h.n., 2015. pp. 11–24. URL cím: http://www.meti.go.jp/english/press/2015/pdf/0123_01b.pdf (letöltve: 2016. 04. 18.).

[26] Erről a kérdésről lásd bővebben: Szenes Zoltán: i. m. Továbbá Petkovics Tamás: A hadiipar fejlesztési lehetőségei Magyarországon. Katonai Logisztika. 24. évfolyam, 1 szám. 2016. pp. 54–87.

[27] Degryse, Christophe: Digitalisation of the economy and its impact on labour markets Working Paper. 2016. European Trade Union Institute. Brussels, pp. 23–25. 2016. URL cím: https://www.researchgate.net/profile/Christophe_Degryse/publication/297392058_Digitalisation_of_the_economy_and_its_impact_on_labour_markets/links/56debb3808aeb8b66f95f7a8.pdf

Európai Szakszervezeti Intézet tanulmánya egy egyetemi kutatócsoport elemzésére hivatkozva egy optimistább forgatókönyvet is felvázol. A hivatkozott számítások 12%-os csökkenéssel számolnak, amelyhez lehet akár rugalmasan igazodni is. Arra viszont fel kell készülni, hogy a jövőben néhány szektornak (például a közlekedés és a logisztika) jelentős mértékben csökken az élőmunka-igénye.

Az infokommunikációs forradalom eddigi eredményei még nem feltétlenül tartoznak a mesterséges intelligenciák fejlesztési kategóriájába. Ugyanakkor ebben a szektorban a már tapasztalt jelenségek előrevetíthetik a gazdasági értelemben vett hangsúlyeltolódást, vagy a társadalmi feszültségeket. Az informatikában a vezető multinacionális cégek (például a Google, a Facebook, az Apple, az Amazon, az IBM vagy a Microsoft) működése szinte kivétel nélkül az Egyesült Államokhoz kötődik. Az Európai Unió tagállamaiban – így Magyarországon is – többször felvetődött már, hogy a közösségi médiával, vagy az online kereskedelemmel foglalkozó cégek (például Amazon, Booking.com) nem fizetnek adót. Az adózatlan bevétel kivitelén túl az amerikai telekommunikációs fölény azzal a veszéllyel is jár, hogy Európa nehezen behozható versenyhátrányba kerül.[28] Az Európában példátlan gyorsasággal terjedő egyszerű mobilalkalmazás, az Uber teljesen megváltoztatta a nyugat-európai városok taxi rendelési módszereit.

Összegzés

A kritikus infrastruktúrák védelmének biztosításához Európában nemzetközi összefogásra van szükség. Az egyes államokon belül a létfontosságú rendszerelemek védelmét össztársadalmi ügyként kell kezelni. A rossz védekezési és irányítási rendszerek növelhetik a halálos áldozatok, a sebesültek számát és az anyagi kár nagyságát. A rendkívüli helyzetek kezelésében a technológia fejlődés eredményeit a lakosság felkészítésében és tájékoztatásában hasznosan és eredményesen lehet alkalmazni. [29] Ennek hiányában viszont a politikai elitnek fel kell készülni a társadalom felháborodására, mint például az Egyesült Államok déli részén 2005-ben pusztító Katrina-hurrikán után.

A biztonsági kockázatokra időről-időre fel kell hívnia társadalom figyelmét, amely egy-egy esemény vagy eseménysorozat hatására gyorsan változhat.[30] Fontos követelmény, hogy a biztonsági kockázatok között egyensúlyt kell tartani. Jó példát jelentett erre, hogy a terrorizmus kockázati primátusként való kezelése az Európai Unióban lassította a kritikus infrastruktúra védelem rendszerének kiépülését. Az új típusú biztonsági kockázatok professzionális kezelésére fel kell készíteni a rendvédelmi szerveket és a haderőt is, s ez a felkészítés a kiképzés és a humánstratégia gyorsan változó biztonsági kihívásai tükrében nem lehet statikus.[31] Arról sem szabad elfeledkezni, hogy a biztonság össztársadalmi jellegű, ezért

[28] Degryse, Christophe: i.m. (2016) pp. 14–16.
[29] Bányász, Péter: A közösségi média szerepe a kasztrófaelhárításban a Sandy-hurrikán példáján. In.: Horváth, Attila (szerk). Fejezetek a kritikus infrastruktúra védelemből II., Magyar Hadtudományi Társaság, Budapest, 2013. pp. 135–148.
[30] Molnár, Ferenc: a magyar társadalom biztonságról, védelemről alkotott képe és a kritikus infrastruktúra. In.: Horváth Attila (szerk). Fejezetek a kritikus infrastruktúra védelemből I., Magyar Hadtudományi Társaság, Budapest, 2013. pp. 107–127.
[31] Jobbágy, Zoltán: Biztonságpolitika, haderőreformok. A humánerőforrás-gazdálkodás katonai életpályával összefüggő kérdései. Hadtudomány, 2015. évi E-különszám. pp. 30–40.

önmagában nem elég a rendvédelmi szervek és a haderő (Magyar Honvédség) felkészítése és fenntartása.

A tanulmányban az új típusú biztonsági kockázatok közül a mesterséges intelligenciák fejlesztésével összefüggő, napjainkban már érzékelhető veszélyekkel foglalkoztam. Ezek messze meghaladják a biztonsági problémakörét. Újszerű gondolkodásmódra van szükség, mert a XIX–XX. századi módszerek alkalmazása nem lesz elégséges a politikai, gazdasági, társadalmi, egzisztenciális feszültségek kezelésére. Az erre való felkészülést jobb korán megkezdeni, mert a történelmi példák sora bizonyítja, hogy a fejlődést jogi és hatalmi módszerekkel nem lehet megakadályozni.

FELHASZNÁLT IRODALOM

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Magyar Közlöny, Magyarország hivatalos lapja. 2012. évi 154. szám. pp. 26105–26106.

2080/2008 (VI.30). Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

Bányász Péter: A közlekedést támogató alkalmazások biztonsági aspektusai. In Horváth Attila–Bányász Péter–Orbók Ákos (szerk.): Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről. Nemzeti Közszolgálati Egyetem, Budapest, 2014. pp. 47–60.

Bányász Péter: A közösségi média szerepe a kasztrófaelhárításban a Sandy-hurrikán példáján. In. Horváth Attila (szerk.): Fejezetek a kritikus infrastruktúra védelemből II., Magyar Hadtudományi Társaság, Budapest, 2013. pp. 135–148.

Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekinttel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In.: Csengeri János–Krajnc Zoltán: Humánvédelem – békeműveleti és veszélyhelyzeti-kezelés eljárások fejlesztése. (Tanulmánygyűjtemény I., e-book), Nemzeti Közszolgálati Egyetem, Budapest, 2016. pp. 643–672. http://real.mtak.hu/33554/1/tanulmanygyujtemeny%20_ujratervezes_CsJ_KZ_1.5.pdf (letöltve: 2016. 03. 11.).

Barabási Albert László: Behálózva. (Második, bővített és átdolgozott kiadás.) Helikon Kiadó, Budapest, 2008. 320 p.

Baudlliard, Jean: Az utolsó előtti pillanat. (A közönyös paroxista). Beszélgetések Philippe Petit-vel. Magvető Kiadó, Budapest, 2000. 148 p.

Beckstead, Nick–Bostrom, Nick–Bowerman, Niel–Cotton-Barratt, Owen–MacAskill, William–Ó hÉgearttaigh, Seán–Ord, Toby: Unprecedented Technological Risks. Global Proorities Project. k.h.n., 2014. 12 p.

Bonnyai Tünde: Úton a kritikus információs infrastruktúrák azonosítása és védelmük kialakítása felé. Hadmérnök, Budapest, VII. évfolyam 2. szám. pp. 90–105. http://hadmernok.hu/2012_2_bonnyai.pdf (letöltve: 2012. 09. 21.)

Buzan, Barry–Waever, Ole– Wilde, de Jaap: A biztonsági elemzés új keretei. In Póti László (szerk). Nemzetközi Biztonsági Tanulmányok. Zrínyi Kiadó. Budapest, 2006. pp. 54–112.

Canneti, Ellias: Tömeg és hatalom. Európa Könyvkiadó, Budapest, 1991. 497 p.

Coaffe, Jon–Wood, Murakami–Davdl Rogers, Peter: The Everyday Resilience of the City. Palgrave Macmillen, New York and London. 2009. 343 p.

Degryse, Christophe: Digitalisation of the economy and its impact on labour markets Working Paper. 2016. European Trade Union Institute. Brussels, 2016.

https://www.researchgate.net/profile/Christophe_Degryse/publication/297392058_Digitalisation_of_the_economy_and_its_impact_on_labour_markets/links/56debb3808aeb8b66f95f7a8.pdf

Diamond, Jared: A harmadik csimpánz felemelkedése és bukása. (Második kiadás) Typotex, Budapest, 2009. 416 p.

Diamond, Jared: Összeomlás. Tanulságok a társadalmak továbbéléséhez. (Második kiadás) Typotex, Budapest, 2009. 577 p.

Doorn van, Menno–Bloem, Jaap–Duivestein, Sander–Ommeren van, Erik: Machine Intelligence. Sogeti, Creative Commons, k.h.n. k.é.n, 40. p. https://www.sogeti.nl/sites/default/files/VINT-rapport%20Machine%20Intelligence.pdf (letöltve: 2016. 05. 09.).

Fjäder, O. Chirstian: National Security in a Hyper-connected World. Global Interdependence and National Security. In. Masys, J Anthony (ed.): Exploring the Security Landscape: Non-Traditional Security Challenges. Springer, pp. 31-58. DOI 10.10007/978-3319-27914-5. (letöltve: 2016. 04. 02.).

Földi László: Az éghajlatváltozás hatása a biztonságra és a katonai erő alkalmazására, a hadviselés ökológiai kérdései. In. Csengeri János–Krajnc Zoltán: Humánvédelem – békeműveleti és veszélyhelyzeti-kezelés eljárások fejlesztése. (Tanulmánygyűjtemény I., e-book), Nemzeti Közszolgálati Egyetem, Budapest, 2016. pp. 550–615. http://real.mtak.hu/33554/1/tanulmanygyujtemeny%20_ujratervezes_CsJ_KZ_1.5.pdf (letöltve: 2016. 03. 23.).

Gazdag Ferenc (szerk): Biztonsági tanulmányok – biztonságpolitika. Zrínyi Miklós Nemzetvédelmi Egyetem. Budapest, 2011. 414 p.

Haig Zsolt–Várhelyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest 286. p.

Horrock, Chirstopher: Baudlliard és a milleneum. Alexandra. (Kiadási hely és év nélkül)

Horváth, Attila–Csaba, Zágon: Critical Transport Infrastructure Protection: A Reserach on the Security of the Supplay Chains. Economics and Management 2015. pp. 47–54. (2015).

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. Berlin–Heidelberg. Springer Verlag, 2012. pp. 299–312.

Horváth Attila: A kritikus infrastruktúra védelem komplex értelmezésének szükségessége. In. Horváth, Attila (szerk.): Fejezetek a kritikus infrastruktúra védelemből I., Magyar Hadtudományi Társaság, Budapest, 2013. pp. 25–48.

Horváth, Attila: ellátási lánc, mint kritikus infrastruktúra (létfontosságú rendszerelem) In. Csengeri János–Krajnc Zoltán: Humánvédelem – békeműveleti és veszélyhelyzeti-kezelés eljárások fejlesztése. (Tanulmánygyűjtemény I., e-book), Nemzeti Közszolgálati Egyetem, Budapest, 2016. pp. 550–615. http://real.mtak.hu/33554/1/tanulmanygyujtemeny%20_ujratervezes_CsJ_KZ_1.5.pdf (letöltve: 2016. 03. 11.).

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. Nemzeti Közszolgálati Egyetem, Budapest, 2014. pp. 7–26.

Horváth, L. Attila: A terrorizmus csapdájában. Zrínyi Kiadó, Budapest, 2014. 287 p.

http://www.automationsmaland.se/dokument/BCG_The_Robotics_Revolution_Sep_2015.pdf (letöltve: 2016. 04. 21.).
Jobbágy Zoltán: A felkelők elleni műveletekről. Egy elfeledett klasszikus: Bernardo de Vargas Machuca. Honvédségi Szemle 2013/2. pp. 15–18.
Jobbágy, Zoltán: A háború antropológiája: primitív hadviselés, gerilla hadviselés és a szövetséges összhaderőnemi műveletek sikere. Hadtudomány: XXV, évfolyam 2015. E-szám pp. 67–78. http://www.mhtt.eu/oldsite/hadtudomany/2015/2015_elektronikus/index.html
Jobbágy, Zoltán: Biztonságpolitika, haderőreformok. A humánerőforrás-gazdálkodás katonai életpályával összefüggő kérdései. Hadtudomány. 2015. évi különszám. pp. 30–40.
Kis-Benedek József: Az Iraki és Levantei Iszlám Állam (ISIL) és az ellene folytatott küzdelem tendenciái. Hadtudomány, 2016/1–2. szám. pp. 29–39.
Kovács László–Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság III. évfolyam 1. szám, 2010. február, pp. 44–56.
Learning from the Blackouts. Transmission System Securityin Competitive Electricity Markets. International Energy Agency and OECD, Paris, 2005. 216 p. http://www.iea.org/publications/freepublications/publication/blackouts.pdf (letöltve: 2016. 03. 19.).
Lewis, Theodore Gyle: Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation. Second Edition. Jon Wiley & Sons., Haboken, New Jersey, 2015. 399 p.
Little, G. Richard: Managing the Risk of Cascading Failure int the Complex Urban Unfrastructures. In.: Graham Stephen (ed). Disrupted Cities. Routledge, Taylor& Francis Group. New York, London, 2010. pp. 27–39.
Macaulay, Tyson: Critical Infrastructure: Understanding its Component Parst, Vulnerabilities, Operating Risks and Interdepencies. CRC Press. New York, London, 2009. 320 p.
Metheny, G. Jason : Reducing the Risk of Human Extinction. Society for Risk Analysis, Vol. 27, No. 5, 2007. pp. 1335-1345. DOI: 10.1111/j.1539-6924.2007.00960x
Molnár Ferenc: A magyar társadalom biztonságról, védelemről alkotott képe és a kritikus infrastruktúra. In. Horváth Attila (szerk.): Fejezetek a kritikus infrastruktúra védelemből I., Magyar Hadtudományi Társaság, Budapest, 2013. pp. 107–127.
Murray, T. Alan–Grubesic, H.Tony: Overview of Reliability and Vulnerability in Critical Infrasturcture. In. Murray T. Alan–Grubesic H. Tony (eds.): Critical Infrasturcture. Reliability and Vulnerability. Springer Verlag. Berlin, Heidelberg, New York, 2007. pp. 1–8.
Müller, C. Vincent: 'Editorial: Risks of artificial intelligence'. In. Vincent C. Müller (ed.): Risks of general intelligence. London, CRC Press – Chapman & Hall, 2016 pp. 1–8. http://www.sophia.de/pdf/2015_AI-Risk_Editorial.pdf (letöltve: 2016. 05. 21.).
New Robot Strategy. Japan's Robot Strategy Vision, Strategy, Action Plan. The Headquarters for Japan's Economic Revitalization. k.h.n., 2015 URL cím: http://www.meti.go.jp/english/press/2015/pdf/0123_01b.pdf (letöltve: 2016. 04. 18.)
Orbók Ákos: Az okosváros közlekedés irányításának kihívásai. In. Horváth Attila–Bányász Péter–Orbók Ákos (szerk.): Fejezetek a létfontosságú közlekedési

rendszerelemek védelmének aktuális kérdéseiről. Nemzeti Közszolgálati Egyetem, Budapest, 2014. pp. 121–128.
Pacione, Michael: Urban Geography. A Global Perspective. Routledge, Taylor& Francis Group. New York, London, 2009. 703 p.
Petkovics Tamás: A hadiipar fejlesztési lehetőségei Magyarországon. Katonai Logisztika. 24. évfolyam, 1 szám. 2016. pp. 54–87.
Porkoláb Imre: Az innováció hatása a hadviselésre. Hadtudomány, 2016/1–2. szám. pp. 19–27.
Porkoláb Imre: Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? Hadtudomány, 2015/3–4. szám. pp. 36–48.
Protecting America's Critical Infrastructures: PDD 63. https://www.hsdl.org/?view&did=456517. p. 14. (letöltve: 2011. 03. 01.)
Sirkin, L. Harold–Zinser, Michael–Rose, Justin Ryan: The Robotics Revolution. The Next Great Leap in Manufacturing. The Boston Consulting Group, Boston, 2015.
Szászi, Gábor: A vasúti közlekedési alágazat, mint kritikus infrastruktúra. In. Horváth Attila (szerk.): Fejezetek a kritikus infrastruktúra védelemből II., Magyar Hadtudományi Társaság, Budapest, 2013. pp. 5–32.
Szenes Zoltán: Tudomány és a korszerű haderő. Magyar Tudomány. 2015/2. szám. pp. 194–201.
Walt, M. Stephen: A biztonsági tanulmányok reneszánsza. In. Póti László (szerk.): Nemzetközi biztonsági tanulmányok. Zrínyi Kiadó, Budapest, 2006. pp. 9–52.
Xu, Tie–Masys, J. Anthony: Critical Infrastructure Vulnerabilities: Embracing a Network Mindset. In. Masys, Anthony J. (eds.): Exploring the Security Landscape: Non-Traditional Security Challenges. Springer International Publishing Switzerland, 2016. pp. 177–194. DOI 10.1007/978-3-319-27914-5.