Sibalin Iván – Vass Gyula

AZ ENISA ÁLTAL MEGHATÁROZOTT AKTUÁLIS TECHNOLÓGIAI KIHÍVÁSOK KEZELÉSE A KATASZTRÓFAVÉDELEM SZEMSZÖGÉBŐL

Absztrakt

A technológia rohamos fejlődése – amellett, hogy jellemzően az emberiség javát szolgálja – számos bizonytalanságot hordoz magában, amelyek helyénvaló és megfelelő időben történő kezelése komoly kihívást jelent a biztonságos felhasználást szavatolni hivatott szervezetek és szakemberek számára. A cikkben bemutatásra kerülnek az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA)[1] által felvázolt aktuális technológiai kihívások megoldására vonatkozó, irányadó jelleggel megfogalmazott javaslatok, valamint azok katasztrófavédelmi szempontú értékelése.

Kulcsszavak: technológiai kihívás, ENISA, javaslat, kiberbiztonság, katasztrófavédelem

TREATMENT OF CURRENT TECHNOLOGICAL CHALLENGES DEFINED BY THE ENISA IN TERMS OF DISASTER MANAGEMENT

Abstract

The rapid development of technology – in addition to being typically beneficial to mankind – involves a number of uncertainties. The appropriate and timely treatment of these unsecurities is a serious challenge for organizations and experts who are in charge of safe use. This paper presents the proposals for resolving the current technological challenges outlined by the

[1] A 2004. március 13-án alapított Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) a hálózat- és információbiztonság európai uniós szakértői központja. Székhelye: Heraklion (Görögország).

European Network and Information Security Agency (ENISA) as well as their assessment in terms of disaster management.

Keywords: technological challange, ENISA, proposal, cybersecurity, disaster management

1. BEVEZETÉS

Az ENISA egyedülálló szerepet tölt be az Európai Uniót és annak tagállamait fenyegető információbiztonsági kihívások kezelésében, a kiberbiztonság megőrzésében és fenntartásában. Az információs technológia rohamos fejlődése következtében a hálózat- és információbiztonság, a személyes adatok védelmének biztosítása egyre komplexebb feladatot jelent a szakértők, az üzemeltetők és a felhasználók számára egyaránt. A cikkben a szerzők nemzetközi kitekintést nyújtanak az aktuális kiberbiztonsági kockázatok kezelési javaslatait illetően. A tanulmány célja felhívni az olvasó figyelmét az ENISA által meghatározott hét technológiai kihívásra, és – az indikatív jelleggel megfogalmazott megoldási javaslatokon túlmutató – részletes kockázatkezelési módszerek tervszerű kidolgozásának a szükségességére.

2. AZ ENISA ALAPÍTÁSÁNAK CÉLJA, SZERVEZETE, FELADAT- ÉS HATÁSKÖRE

A biztonság olyan fenyegetettség nélküli állapotot jelöl, amely a mindennapi élet egyik alapfeltételének tekinthető. A biztonság dimenziója a bipoláris világrend megszűnésével markánsan megváltozott. A katonai veszélyeztetettségből eredeztetett biztonság megközelítés az új világrend kihívásait szem előtt tartó biztonságfogalommá alakult át. Ebből kifolyólag a biztonság alkotóelemei alatt napjainkban már a társadalmi, gazdasági, politikai, környezeti pénzügyi, egészségügyi, katonai, belügyi és informatikai biztonságot értjük. [1]

A hálózat- és információbiztonsági feladatokat ellátó szervezet létrehozataláról 2004. március 10-én döntött az Európai Parlament és a Tanács a 460/2004/EK rendelet [2] elfogadásával, amely közel egy évtizedig szabályozta az ENISA működését, részletesen meghatározva annak feladatait, céljait és szervezetét. A 2013. június 19-én hatályba lépett 526/2013/EU rendelet

[3] azonban már új szabályokat állapított meg az ENISA-ra nézve, és egyben hatályon kívül helyezte a 460/2004/EK rendeletet. Az új jogszabály 2. cikke meghatározza az ENISA létrehozatalával elérni kívánt célokat, míg a 3. cikk részletesen szabályozza az ügynökség feladatait, amely az alábbiakban foglalható össze:

-*„segítségnyújtás és tanácsadás az uniós szervek és tagállamok számára az uniós szintű hálózat- és információbiztonsági politikához és joghoz kapcsolódó kérdésekben;*

- *a hálózat- és információbiztonság területén előkészítő és elemző munkát végez;*

- *támogatja a hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT-ek) működését, a hálózat- és információbiztonsági képességek fejlesztését, a tagállamok és az uniós szervek közötti valamint a harmadik országokkal és nemzetközi szervezetekkel folytatott együttműködést;*

- *kiberbiztonsági gyakorlatok, képzések szervezésében közreműködik;*

- *kiberbiztonsági témájú tanulmányokat és jelentéseket készít;*

- *kérelemre tanácsokat ad uniós intézmények, szervek, hivatalok és ügynökségek, valamint a tagállami szervek részére a biztonság sérülése és az integritás megszűnése esetén.”* [3]

Az Ügynökség – melynek napi szintű igazgatásával kapcsolatos feladatait az ügyvezető igazgató látja el – az Igazgatóságból és annak végrehajtó testületéből, az ügyvezető igazgató személyi állományából, valamint az érdekeltek állandó csoportjából tevődik össze. Az Igazgatóság határozza meg az Ügynökség működésének általános irányát, és elfogadja az éves és többéves munkaprogramját. Tagállamonként egy-egy képviselőből és a Bizottság által kijelölt két képviselőből áll, tagjai sorából három évre elnököt és elnökhelyettest választ. Az érdekeltek állandó csoportját az igazgatóság az ügyvezető igazgató javaslatára hozza létre, amely a releváns érdekelteket, képviselő szakértőket, valamint a nemzeti szabályozó hatóságok, a bűnüldöző és a magánélet védelmével foglalkozó hatóságok képviselőit tömöríti. [3]

Az ENISA 2018 januárjában közzétett egy jelentést *"Looking into the crystal ball"* [4] címmel, amelyben összegzésre kerülnek a technológiai fejlődés aktuális biztonságvédelmi kihívásai, és az azokra vonatkozó kockázatkezelési javaslatok. A dokumentum hét fejlesztési irányt jelöl meg. Ezek rövid ismertetését követően összegzi az adott területre jellemző kihívásokat, majd indikatív jelleggel javaslatokat fogalmaz meg azok kezelésére.

3. AKTUÁLIS TECHNOLÓGIAI KIHÍVÁSOK

3.1. A dolgok internete (IoT)

Az ENISA jelentésében a technológiai kihívások között elsőként említi a médiában egyre gyakrabban emlegetett dolgok internetét (IoT). Míg korábban csak az asztali számítógépek, majd a hordozható eszközök (laptopok, tabletek, okostelefonok) rendelkeztek internetes kapcsolattal, napjainkban e jellemző már más tárgyakról is elmondható. Az IoT bizonyos mindennapjainkban használt eszközök online hálózatba kapcsolását jelenti, amelyek egymással is képesek kommunikálni.

Az IoT eszközök jellemzően tömegcikkek, melyek esetében a gyártó – tipikusan költséghatékonysági okokból – nem minden esetben fordít kellő figyelmet a biztonságos használat követelményének érvényre juttatására. Általános célokra használt termékek lévén, pedig nehéz előre meghatározni a felhasználásuk konkrét területét a gyártás során, ami különösen megnehezíti a gyártó dolgát a védelmi követelmények szavatolása tekintetében.[2] A biztonsági deficitnek, az IoT rendszerekről megszerezhető információk értékének, valamint az ellenük irányuló rosszindulatú támadások által kiváltható károk súlyosságának köszönhetően nyilvánvaló, hogy a dolgok internete a kiberbűnözés első számú célpontjai között fog szerepelni. [4] Különösen kockázatos a katasztrófavédelem által felügyelt veszélyes anyagokkal foglakozó üzemek, valamint a létfontosságú rendszerek és létesítmények működtetéséhez alkalmazott IoT eszközök kibervédelmének elhanyagolása. E rendszerek sérülése, működési zavara technológiai káresemények, üzemzavarok előidézője lehet, amely többek között a lakosság és az anyagi javak védelme szempontjából jelent kockázatot. A probléma meglehetősen komplex, kezelése összetett munkát igényel. E körben csupán az Ügynökség megoldási javaslatai, valamint az Európai Bizottság intézménymódosítási tervei kerülnek nevesítésre.

Az ENISA 2017. november 20-án közzétett egy átfogó dokumentumot, amelyben alapvető biztonsági ajánlásokat fogalmaz meg a „dolgok internetéhez” a kritikus információs

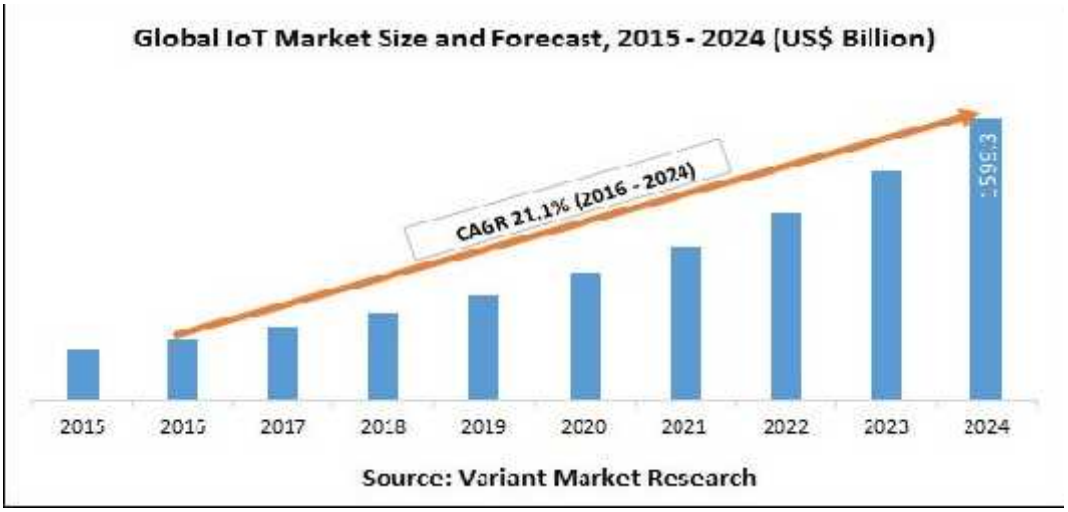
[2] Mindazonáltal az iparban egyre szélesebb körben alkalmazandó ipari IoT eszközök (IIoT) esetében – használatuk célirányos mivoltának köszönhetően – hatékonyabb biztonságvédelmi eredmények érhetők el a gyártás során.

infrastruktúrák vonatkozásában. A tanulmány biztonsági intézkedéseket fogalmaz meg, melyek alkalmazását indokoltnak tartja, továbbá az alábbi hét konkrét javaslatot nevezi meg:

- *„az IoT rendszerre vonatkozó védelmi szabályozások harmonizációjának szükségességét,*
- *valamennyi érdekelt (gyártok, fejlesztők, felhasználók, fogyasztók) figyelmének felhívását a kiberbiztonság fontosságára,*
- *a biztonságos szoftver/hardver fejlesztési életciklus irányelvek meghatározását,*
- *az IoT rendszerek közötti interoperabilitás biztosítását,*
- *az IoT-biztonság megvalósítását ösztönző gazdasági és adminisztratív intézkedések előmozdítását,*
- *az IoT termékek/szolgáltatások biztonságos életciklus-menedzsmentjének létrehozását,*
- *a felelősségi kérdések tisztázását."* [5]

A védelem további eszközeként az Európai Bizottság javaslatot tett egy új szerv, nevezetesen az EU Kiberbiztonsági Ügynökség létrehozására, amely az ENISA továbbfejlesztésével valósulna meg. A Kiberbiztonsági Ügynökség célja, a tagállamoknak történő segítségnyújtás a kibertámadások megelőzésében és az azokra való reagálásban. E tevékenység keretében páneurópai kiberbiztonsági gyakorlatok szervezését, valamint információmegosztási és analitikai központok létrehozását helyezi kilátásba. A Kiberbiztonsági Ügynökség támogatná a termékek és szolgáltatások számítástechnikai szempontú biztonságosságát garantáló uniós tanúsítási keretrendszer kialakítását és végrehajtását is. Az európai kiberbiztonsági tanúsítványok garantálják majd az IoT eszközök megbízhatóságát, amelyek alapvető fontosságú szerepet töltenek be napjaink létfontosságú rendszereiben is, például az energia- és közlekedési hálózatokban. [6]

Az alábbi táblázat mutatja be a globális IoT piac összetett éves növekedési rátáját (CAGR - Compound Annual Growth Rate) 2015-től 2024-ig. A táblázat szerint a globális IoT piac mérete évente átlagosan 21,1%-kal növekszik, így 2024-re már várhatóan eléri az 1599,3 milliárd USA dollár (USD) összeget.



1. ábra: A globális IoT piac mérete, 2015-2024 [7]

3.2. A technológiafejlődés és a társadalmi változások közötti kölcsönhatás

Történelmi tapasztalatok bizonyítják, hogy bizonyos társadalmi változások gyakran technológiai fejlődést generálnak, és fordítva; technológiai újítások, találmányok – megváltoztatva az emberek mindennapjait – átalakítják a társadalom szerkezetét.

Napjainkban sem történik ez másképp, sőt a technológia fejlődésének és a társadalom változásának a kölcsönhatása sokkal kifejezettebben érzékelhető, mint a korábbi évtizedekben, évszázadokban. A technológiai fejlődéssel történő lépéstartás kényszeréből adódóan a felhasználók tetemes hányada megfeledkezik azon biztonsági kockázatokról, amelyek a rohamos fejlődéssel együtt járnak. Különösen igaz ez a kiberbiztonság területére, ahol egyes becslések szerint a végfelhasználók biztonságtudatosabb magatartásával a jelenlegi biztonsági események több mint 50%-kal csökkennének. A probléma megfelelő kezelése érdekében a felhasználói magatartás alapján a kibervédelem tudományos és szakmai képviselői, művelői fontos következtetéseket vonhatnak le az alábbiakra nézve:

- visszaéléssel kapcsolatos ügyek elemzésére;
- felhasználói eszközök azonosítására, értékelésére;
- olyan biztonsági ellenőrzések kidolgozására, amelyeket nem szakemberek is képesek kezelni;
- a biztonságtudatos felhasználás erősítésére;
- a társadalmi igények, az oktatási módszerek és a felhasználói viselkedési minták közötti összhang megteremtésére, stb. [4]

A katasztrófavédelem információ és hálózatbiztonsági feladatkörében jelenleg is szerepel az általa felügyelt létfontosságú rendszerek és létesítmények esetében a kibervédelemmel kapcsolatos tudatosítási tevékenység, annak hatékonyabb érvényesítése érdekében célszerű az oktatási és gyakorlati módszerek alkalmazásával a biztonságos felhasználói magatartást a fentiekkel összhangban erősíteni. A biztonságtudatosságra nevelő katasztrófavédelmi ismeretek általános és középiskolás korban történő elsajátításával számos – a technológiai fejlődéssel összefüggésben jelentkező – biztonsági deficit elkerülhető.

3.3. Az it infrastruktúrák új generációja

Az információs technológia számos területére jellemző az IT infrastruktúrák új generációinak a kialakítása, fejlesztése, melyek alkalmazása jelentős technológiai, gazdasági és kiberbiztonsági kockázattal járhat. Ezen infrastruktúrák közös jellemzője a nagymértékű virtualizáció[3], melynek több fajtája ismert, azonban azok bemutatása meghaladná e cikk kereteit. A virtualizációval kapcsolatos kiberbiztonsági kockázatok szemléltetésére jó példa a virtuális számítógép alkalmazása, melynek során egy fizikailag létező számítógép több fizikailag nem létező számítógép működését szimulálja.

E megoldás rendkívül költséghatékony és energiakímélő, azonban kiberbiztonsági szempontból meglehetősen kockázatos. A potenciális támadó számára ugyanis rendkívül vonzó lehet az a tény, hogy egy sikeres támadás következtében viszonylag nagy számú felhasználó által kezelt adathoz juthat hozzá. [4]

Gazdasági kockázatra jó példa a fizetésre használható virtuális eszközökkel[4] történő kereskedés. Mivel e fizetési eszközöket olyan külföldi cégek és természetes személyek bocsátják ki, akik nem tartoznak az EU-tagállamok jegybankjainak és az Európai Unió pénzügyi felügyeleti intézményeinek a joghatósága alá, ezért az ilyen eszközökbe való befektetés különösen kockázatos lehet. Fizetésképtelenség esetén ugyanis a fogyasztók kártalanításban nem részesülnek, a befektetések után biztosítékot sem az Országos Betétbiztosítási Alap, sem a Befektető-védelmi Alap nem nyújt. [8]

[3] A fizikai környezetben nem létező mesterséges állapot, mely a felhasználó számára a valódiság hatását képes előidézni. ld: virtuális valóság, virtuális számítógép, stb.

[4] Legismertebb fajtája a bitcoin.

3.4. Az autonóm rendszerek

Az autonóm rendszerek napjaink egyik meglehetősen gyorsan fejlődő technológiai újításai közé tartoznak, különösen a járműipar területén. E rendszerek jellemzője, hogy minimális emberi beavatkozás mellett, vagy akár anélkül, önállóan képesek felismerni cselekvési lehetőségeiket, és az adott körülmény vonatkozásában a legoptimálisabb döntést meghozni. Alkalmazásuk ezért katasztrófavédelmi feladatok ellátására, mint például a tűzoltás, műszaki mentés, árvízi védekezés esetében különösen hasznos lehet. Autonóm rendszerek, robotok veszélyes zónába, káresemények helyszínére juttatásával emberi életek veszélyeztetése nélkül lehetne katasztrófa-elhárítási beavatkozásokat végrehajtani.

Mindazonáltal e rendszerek alkalmazása – az általuk ellátandó funkció függvényében – kiberbiztonsági szempontból igencsak kockázatos lehet. [9] Fontos hangsúlyozni, hogy az autonóm rendszerek „gondolkodásmódja" merőben eltér az emberétől, amely tény komoly kihívásokat von maga után különösen a katonai célokra történő alkalmazásuk során. Az ellenfél ugyanis képes kihasználni a gép érzékelési (felfogási) és megismerési képességeiben rejlő hiányosságokat, ami nem szükségképpen jelenti azt, hogy az autonóm rendszerek sérülékenyebbek az emberi ellenőrzéssel működő rendszereknél, de használatuk mindenképp újabb – az eddig megszokottaktól eltérő – támadási lehetőségeket eredményez. E tény az autonóm rendszerek széleskörű katonai alkalmazása során viszont már komoly kockázatot jelenthet az érintett haderőre nézve. [10]

E rendszerek biztonságos használatához új védelmi mechanizmusok alkalmazása válik szükségessé. Különösen igaz ez az autonóm rendszerek és bizonyos kevésbé megbízható eszközök, mint például szenzorok és más IoT eszközök közötti interakciókra. [4] A kockázatok csökkentése érdekében alapvető fontosságú a rendszer támadási felületének elemzése, értékelése, a koherens teszttervezés kialakítása, valamint az autonóm rendszerek tesztelése és újratesztelése. [10] Meg kell találni a módját annak, hogy a támadások, működésbeli zavarok még időben – a kedvezőtlen folyamatok bekövetkezése előtt – felismerhetők, azonosíthatók legyenek. Fontos, hogy feltárjuk, és megismerjük a különböző működésbeli zavarok észlelhető tüneteit előidéző tényezőket, okokat, és képesek legyünk azokat megfelelően és hatékonyan kezelni. Egyes vélekedések szerint bizonyos értelemben párhuzam fedezhető fel az emberi elme pszichopatológiája és az autonóm rendszerek működésbeli zavarai között, amiből fontos következtetéseket vonhatunk le e rendszerek védelme érdekében. Ahogyan az emberi elme kóros működésének a tanulmányozásával

betekintést nyerhetünk az agyműködés komplex rendszerébe, hasonlóan az autonóm rendszerek működésbeli zavarainak elemzésével a mesterséges intelligenciára vonatkozóan állíthatunk fel törvényszerűségeket. Az *„autonóm rendszerek pszichopatológiája”* tézisének a felállításával és annak továbbfejlesztésével az intelligens eszközök működése témakörében felmerülő számos kérdésre választ kaphatunk, e tekintetben tehát mindenképpen érdemes további kutatásokat folytatni. [9]

3.5. A bio-nano eszközök internete

Míg az IoT jellemzően a mindennapi használatra szánt tárgyak internet alapú hálózatba kapcsolását jelenti, addig a bio-nano dolgok internete a nanoméretű dolgok, eszközök online csatlakozását teszi lehetővé. Ezen eszközök méretükből adódóan könnyen beültethetők akár élő szervezetekbe is, ahol kölcsönös együttműködésben képesek funkcionálni, egészségállapotra vonatkozó információkat gyűjteni, és azokat interneten keresztül továbbítani az egészségügyi szolgáltató felé, és végrehajtani annak utasításait (például a gyógyszeradagolás kapcsán).

A bio-nano dolgok segítségével a sejtek programozható szubsztrátumokká válhatnak, amelyek működése, szerkezete ellenőrizhető és módosítható lenne. A nanoeszközök kooperációjával pedig megelőzhetők a jellemzően idegi alapú kommunikációs zavarok a szervezeten belül, és a különféle kóros elváltozások késedelmes diagnózisából eredő kockázatok kiküszöbölhetők lennének.

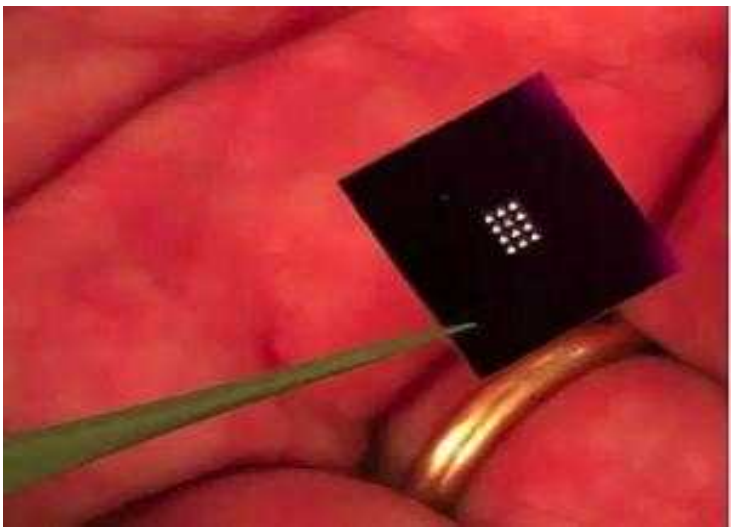
E dolgok az orvostudományon kívül azonban számtalan más területen is hasznosíthatók, példaként említve katasztrófavédelmet és a környezetvédelmet, mivel a környezetbe jutatott bio-nano eszközök alkalmasak lennének a mérgező, szennyező anyagok felismerésére és ártalmatlanítására egyaránt. [11] Az ipari létesítmények esetében bekövetkezett káreseményeknél kibocsátott káros anyagok környezetbe kerülésének ellenőrzése és kimutatatása jelentős mértékben leegyszerűsödne, így a katasztrófavédelmi hatóságok a nanoeszközökkel fenntartott internetes kapcsolatuk révén könnyen tájékozódhatnának az iparbiztonsági és vízvédelmi szempontból aggályos eseményekről.

E bio-nano dolgok működtetése számos kockázatot hordoz magában, melyek számbavételéhez multidiszciplináris szemlélet szükséges, és jelenleg még csak becslésekkel rendelkezünk arra nézve, hogy ezen eszközök használata milyen következményekkel járhat. Példaként említve egy orvos feltehetné a kérdést hogy, vajon az élő szervezet meddig

tolerálná a szintetikus anyagokból készült, egymással elektromágneses úton kommunikáló – ennélfogva elektromágneses sugárzást kibocsátó – nanoméretű eszközöket. [11]

Kiberbiztonsági szempontból vizsgálva a kockázatokat pedig sejthetjük, hogy egy esetleges kibertámadás működésüket milyen mértékben zavarhatná meg vagy lehetetleníthetné el, ami beláthatatlan következményekkel járna attól függően, hogy az eszköz milyen funkciót tölt be. Kérdéses továbbá a megbízható és hatékony kommunikációs infrastruktúra kiépítésének, valamint az interneten keresztül történő adatcserének a módja is. [12] Az ENISA a következőket javasolja a bio-nano dolgok használata kapcsán:

- *„Kezdeti kockázatértékelés szükséges ahhoz, hogy megértsük e technológiák kihatásait.”*
- *„Az alkalmazási terület jellege és az érintett komponensek sajátossága és kölcsönhatása miatt, a szükséges védelmi szint elérése érdekében ki kell terjeszteni a meglévő biztonsági technikákat.”* [4]



1. kép: Emberi testbe ültethető bio-nano chip [13]

3.6. A mesterséges intelligencia

A mesterséges intelligencia alkalmazása, fejlesztése napjaink egyik legégetőbb morális, etikai kérdése, amely – amellett, hogy hatalmas lehetőségeket hordoz magában – számos veszély és végeláthatatlan megoldandó probléma forrása lehet, legyen szó akár reál/természettudományi akár társadalomtudományi kérdésről. A kiberbiztonság fokozására kiváló lehetőség a mesterséges intelligencia alkalmazása, azonban ugyanígy akár rosszindulatú kibertevékenységre is felhasználható. Egyes becslések szerint a mesterséges intelligencia

alkalmazásának elterjedése olcsóbbá és egyszerűbbé fogja tenni a kibertámadások végrehajtását, valamint lehetőséget biztosít a kiberfenyegetések újabb módszereinek a megvalósítására. A világnak tehát a kibertámadások újabb hullámával kell számolnia az elkövetkezendő években, amelyek az eddig megszokottakhoz képest várhatóan nagyobb kárt képesek majd előidézni. [14]

A mesterséges intelligencia, az IoT és az Ipar 4.0 koncepció[5] egymással szoros összefüggésben értelmezendők. Az előbbi előfeltétele az utóbbi kettőnek, lévén, hogy a mesterséges intelligencia az automatizált döntéshozatal alkalmazását mozdítja elő. [4] Ennélfogva, az alkalmazásukból eredő kihívások sem kezelhetők egymástól elkülönítve, a megfelelő védelem kialakításához elengedhetetlen a rendszerszintű szemlélet.

A katasztrófavédelem három szakterülete közül különösen az iparbiztonság számára válhat szükségessé az eddigi balesetvédelmi szempontok átértékelése, újabb védelmi mechanizmusok kidolgozása a mesterséges intelligencia iparban történő alkalmazásával összefüggésben.

Az ENISA javaslata szerint mindenekelőtt a mesterséges intelligencia és a robotika használatával kapcsolatos fenyegetések és sérülékenységek felmérése szükséges. Az államvezetésnek tekintettel kell lennie a mesterséges intelligencia alkalmazásával összefüggésben felmerülő valamennyi társadalmi és technológiai kérdésre, az érdekelt személyek szerepének azonosítására, a megfelelő szabályozási szint kialakítására, stb. Az Ügynökség jelentésében javaslatot tesz a megfelelő védelem biztosítására a termékek és szolgáltatások életciklusának valamennyi szakaszában, különösen a tervezés, fejlesztés, valamint a használat és a karbantartás során. [4]

3.7. A virtuális és az augmentált valóság (VAR)

A virtuális és az augmentált valóság célja, hogy alternatívát biztosítson a fizikai környezet helyett, azonban míg a virtuális valóság tulajdonképpen teljes mértékben elzárja a

[5] 4. ipari forradalom; az ipari eszközök információs hálózatba kapcsolásának a biztosításával az ipari folyamatok teljes mértékű digitalizációjának a megvalósítása.

felhasználót a valós környezettől, addig az augmentált valóság csupán kiegészíti a meglévő fizikai környezetet, azaz segítségével további információk szerezhetők a valódi miliőről.

Napjainkban egyelőre csak szűk körben, a szórakoztatóiparban, valamint bizonyos szakmai kiképzések során, mint például az űrhajósok vagy katonák kiképzése keretében alkalmazandóak a VAR vívmányai. Általánosságban elmondható, hogy a kibertér és a valós, fizikai környezet jelenleg egymástól jól elkülöníthető, ezért a kiberbiztonság relevanciája a virtuális és augmentált valóság alkalmazása kapcsán meglehetősen csekély. [4] Be kell látnunk azonban, hogy a VAR hatalmas lehetőségeket rejt magában, és belátható időn belül számolnunk kell alkalmazásának elterjedésével, különösen a hadiipar, űrkutatás, oktatás, kereskedelem, stb. területén. Különösen hasznos lehet a katasztrófavédelem számára bizonyos válsághelyzetek VAR általi szimulálása, a katasztrófák gyakran váratlan és precedens nélküli jellege miatt. A VAR alkalmazásával biztosítható lenne a katasztrófavédelem magasabb fokú felkészültsége és hatékonyabb fellépése olyan veszélyhelyzetek során is, amelyekre az eseményt megelőzőleg még nem volt példa. A virtuális valóság vívmányai segítségével az iparbiztonság balesetmegelőző (preventív) szerepe is fokozhatóvá válik, mivel az egyes veszélyes üzemek és létesítmények működésével kapcsolatos hibák, üzemzavarok szimulálásával – bekövetkezésük elkerülése érdekében – precízebb és biztonságosabb védelmi rendszert kialakítására nyílhatna lehetőség.

Nem túlzás azt állítani, hogy – az okostelefonokhoz és más okos eszközökhöz hasonlóan – a VAR mindennapjaink részét fogja képezni, ennélfogva tekintettel kell lennünk vívmányainak használatával járó lehetséges kiberbiztonsági kockázatokra is. Példaként említve számolnunk kell azzal a lehetőséggel, hogy egy hackertámadás keretében rögzítésre kerül a felhasználónak a VAR alkalmazása során tanúsított magatartása, cselekményei. Ezzel a – személyiségi jogokat sértő – támadó számára kiváló lehetőség kínálkozik a jogaiban megsértett felhasználó zsarolására (például a felvétel titokban tartásáért cserébe bizonyos pénzösszeget követelhet).

Rosszindulatú VAR applikációk alkalmazásával a támadó szintén könnyen hozzájuthat a felhasználó személyes adataihoz. Bizonyos adatok vagy információk közbevetésével a gyanútlan felhasználók könnyen félrevezethetők, és személyes azonosításra alkalmas adatokat adhatnak meg magukról. [15] Különösen nagy kárt okozhatnak az ipari és egészségügyi célokra alkalmazott VAR eszközök ellen intézett támadások, amelyek során akár emberek élete foroghat kockán.

Az IoT eszközökkel kapcsolatos kibervédelmi megoldásokhoz képest további védelmi intézkedések, módszerek szükségesek, melyeket folyamatosan fejlesztve – mintegy lépést tartva a technológiai fejlődéssel, és a rosszindulatú támadók felkészültségével – szavatolhatjuk a VAR biztonságos használatát. Az ENISA tanulmányában meglehetősen szűkszavúan – konkrétumok mellőzésével – fogalmaz a kibervédelmi megoldások kapcsán, mindazonáltal bizonyos biztonságvédelmi módszerek megvalósítására számos szakértői javaslat született, és a vizsgálódások tovább folytatódnak a naprakészség követelményének szem előtt tartásával. Ezek közözött említhetjük a biztonságos üzenetküldés szavatolásának, a VAR tartalom integritásának, a VAR eszközök közötti kommunikáció hitelesítésének a követelményét, [15] a VAR-hoz köthető felelősségi kérdések egzakt jogi szabályozásának kidolgozását.

4. KÖVETKEZTETÉSEK

A cikkben bemutatásra kerültek az ENISA által meghatározott aktuális technológiai fejlődési tendenciákkal kapcsolatos bizonyos kockázatok, és a kezelésükre vonatkozó indikatív jellegű javaslatok. A technológia fejlődése napjainkban olyan rohamosan történik, hogy a társadalom gyakran nem képes választ találni olyan kérdésekre, amelyek szükségesek lennének ahhoz, hogy a technológia új vívmányait képesek legyük kellő biztonsággal kezelni.

Mind a hét területre jellemző a hiányos vagy nem kellően adekvát jogi szabályozás, amely nélkül – társadalmi változásokat potenciálisan magukban hordozó – új vívmányok alkalmazása kontraproduktívvá válhat. Néhány esetben, bizonyos fejlesztési módszerek műszaki megvalósítása sem tisztázott kellőképpen.

A megoldási javaslatok konkretizálása, tervszerű kidolgozása a katasztrófavédelem által biztosított lakosságvédelmi szempontok figyelembevételével elengedhetetlen feltétele a biztonságos működés megvalósításának. A technológia legkorszerűbb vívmányain alapuló új típusú termelési eszközök biztonságos működtetése különösen az iparbiztonság számára jelent komoly kihívást a jövőre nézve.

Láthatjuk, hogy a probléma meglehetősen összetett, és a kockázatok kezelésére kizárólag informatikai (kiberbiztonsági) eszközökkel nem tudunk megfelelő választ adni, ezért a

kihívások és az azokból fakadó nehézségek hatékony megoldása széleskörű, jogi, technológiai, gazdasági, szociológiai, etikai szemléletet igényel.

FELHASZNÁLT IRODALOM

[1] BOGNÁR B., KÁTAI-URBÁN L., KOSSA Gy., KOZMA S., SZAKÁL B, VASS Gy. KÁTAI-URBÁN L.: (szerk.): *Iparbiztonságtan I: Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához.* Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., 2013. 53. o.

[2] *Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról.* eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:HU:HTML (A letöltés ideje: 2018. 04. 24.)

[3] *Az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről.* eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32013R0526&qid=1523875537765 (A letöltés ideje: 2018. 04. 24.)

[4] ENISA: *Looking into the crystal ball. A report on emerging technologies and security challenges.* 2018. 01. 31. www.enisa.europa.eu/publications/looking-into-the-crystal-ball (A letöltés ideje: 2018. 04. 24.)

[5] ENISA: *Baseline Security Recommendations for IoT.* 2017. 11. 20. www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot (A letöltés ideje: 2018. 04. 25.)

[6] (s.n.) Kiberbiztonság iránti uniós fellépések - Cél az Európai Uniós Kiberbiztonsági Ügynökség létrehozása. *Jogi Fórum.* www.jogiforum.hu/hirek/38196 (A letöltés ideje: 2018. 04. 25.)

[7] (s.n.) Variant Market Research: Global Internet of Things (IoT) Market: Rising Adoption of Cloud Platform Noticed by Variant Market Research. *iot.do,* iot.do/global-internet-of-things-iot-market-2017-12 (A letöltés ideje: 2018. 04. 26.)

[8] (s.n.) Újabb kockázatok a fizetésre használható virtuális eszközök körében. *Magyar Nemzeti Bank - Online,* www.mnb.hu/sajtoszoba/sajtokozlemenyek/2015-evi-sajtokozlemenyek/ujabb-kockazatok-a-fizetesre-hasznalhato-virtualis-eszkozok-koreben (A letöltés ideje: 2018. 04. 26.)

[9] ATKINSON, D. J.: Emerging Cyber-Security Issues of Autonomy and the Psychopathology of Intelligent Machines. *2015 AAAI Spring Symposium,* www.aaai.org/ocs/index.php/SSS/SSS15/paper/viewFile/10219/10049 (A letöltés ideje: 2018. 04. 26.)

[10] AHNER, D., PARSON, C.: Workshop Report: Test and Evaluation of Autonomous Systems. *Department of Defense - United States of America,* www.afit.edu/stat/statcoe_files/Workshop%20Report%20-%20T&E%20of%20Autonomous%20Systems.pdf (A letöltés ideje: 2018. 04. 27.)

[11] AKYILDIZ, I. F., PIEROBON, M., BALASUBRAMANIAM, S., KOUCHERYAVY Y.: The internet of Bio-Nano things. *IEEE Communications Society, Institute of Electrical and Electronics Engineers,* www.researchgate.net/publication/273780747_The_internet_of_Bio-Nano_things (A letöltés ideje: 2018. 04. 27.)

[12] DE FARIAS, C., PIRMEZ, L., COSTA, G., DE FARIAS, F.: Internet of Bionano-Things: Perspective and Future Directions. *MedCrave - International Journal of Biosensors & Bioelectronics,* medcraveonline.com/IJBSBE/IJBSBE-03-00050.pdf (A letöltés ideje: 2018. 04. 27.)

[13] FORD, J.: Programmable Bio-Nano-Chips: First Viable Medical Lab on a Chip? *SingularityHub*. singularityhub.com/2011/02/16/programmable-bio-nano-chips-the-first-viable-medical-lab-on-a-chip/#sm.0001kekx4kkggdnsusw2lb6j1go28 (A letöltés ideje: 2018. 04. 28.)

[14] ASHFORD, W.: AI a threat to cyber security, warns report. *ComputerWeekly.com,* www.computerweekly.com/news/252435434/AI-a-threat-to-cyber-security-warns-report (A letöltés ideje: 2018. 04. 28.)

[15] RITESH., K.: Virtual and Augmented Reality (VR/AR) Cybersecurity Challenges. *LinkedIn,* www.linkedin.com/pulse/virtual-augmented-reality-vrar-cybersecurity-kumar-ritesh/ (A letöltés ideje: 2018. 04. 29.)

Sibalin Iván doktorandusz

Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézet

Iván Sibalin PhD student

Institute for Disaster Management National University for Public Service

orcid.org/0000-0002-7228-6832

sibalin4@gmail.com

Dr. habil. Vass Gyula tűzoltó ezredes PhD egyetemi docens, igazgató,

Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézet

vass.gyula@uni-nke.hu

Col. Gyula Vass PhD, associate professor, director of Institute of Disaster Management, National University for Public Service

orcid.org/0000-0002-1845-2027