HADMÉRNÖK

XII. Évfolyam 1. különszám – 2017. július

AZ ÖSSZADATFORRÁSÚ ELEMZÉS ÉS PREDIKTÍV MODELLEZÉS

ALL-SOURCE ANALYSIS AND PREDICTIVE MODELING

AMBRUS Éva

(ORCID: 0000-0002-8354-1296)

ambrus.eva.eszter@gmail.com

Absztrakt

Jelen írás bemutatja az összadatforrású elemzések és prediktív modellezéssel kapcsolatos alapvető irodalmakat és azok megállapításait, az alábbi kulcs területekre koncentrálva: adatok és azok kinyerése (adatbányászat, metaadatok); OSINT a felderítési-elemzési ciklusban; kibervédelem itthon és külföldön és a mesterséges intelligencia felhasználási területei (mély algoritmusok, önvezető járművek, számítógépes látás).

Kulcsszavak: *adat, kiberhadviselés adatelemzés, mesterséges intelligencia*

Abstract

This paper main aim is to introduce the main concepts behind all-source analysis and predictive modeling. The main areas that will be covered are as follows: definition of data and data-mining, open source intelligence in the intelligence cycle, cybersecurity in Hungary and abroad and the use of artificial intelligence (deep algorithms, automated driving, and computer vision.

Keywords: *data, cybersecurity, data analysis, artificial intelligence*

A kézirat benyújtásának dátuma (Date of the submission): 2017.05.25.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.05.31.

BEVEZETÉS

Az elmúlt évtizedek infokommunikációs és technológiai fejlődésének köszönhetően jelenleg az információs társadalom, a tudásalapú társadalom tekinthető a legfejlettebb társadalomnak. Az információs társadalom elmélete szerint az információ előállítása, elosztása, terjesztése, használata és kezelése jelentős gazdasági, politikai és kulturális tevékenység, melynek középpontjában az információ-technológiai áll. [1] Az információs társadalom működésének alapja az infokommunikációs rendszereken alapuló információs infrastruktúrák egymásba kapcsolódó komplex rendszere, melybe beletartoznak az informatikai, távközlési, navigációs, távvezérléséi rendszerek is. [1]

Ahogyan fejlődött a hálózati technológia, növekedett a sávszélesség, lehetővé téve a nagyobb és biztonságosabb adatforgalmat, úgy beszélhetünk egyre nagyobb összekapcsoltságról is. Ez megjelenik például a mindennapi infokommunikációs eszközök teljesítmény-növekedésében (memóriakapacitás, sávszélesség), információ-feldolgozó és adatátviteli kapacitások növekedésében (okos eszközök megjelenése, a *dolgok internete*), valamint a gépi gondolkodásmód fejlődésében (machine learning). A nagyobb összekapcsoltság árnyoldala a nagyobb biztonsági kitettség, a függőség e rendszerektől, és egyre nagyobb kihívást jelent a információbiztonság, a kiberbiztonság.

A kutatás módszertanát tekintve leíró alapkutatást végeztem szekunder adatok feldolgozásával, melynek célja bemutatni az előbb nagyban felvázolt társadalmi fejlődéssel kapcsolatos hazai és külföldi irodalmakat és főbb megállapításaikat négy nagy területre koncentrálva: az adatok, a nyílt forrású adatok / információk feldolgozása és elemzése, a mesterséges intelligencia felhasználási területei (gépi gondolkodásmód, mély algoritmusok, számítógépes látás) és végül a kibervédelem állása itthon és külföldön.

Az adatok integráltabb feldolgozása révén (különböző típusú adatok felhasználása) a gépi gondolkodásmód fejlődésével és az ebből fakadóan a kifinomultabb prediktív modellek felhasználásával egyre közelebb kerülünk egy valós-idejű, szűrt helyzetkép eléréséhez, ahol nem csak a jelent láthatjuk, hanem a potenciális közeljövőt.

AZ ADAT, AZ INFORMÁCIÓ

A globális, információs és tudásalapú világunk egyre inkább automatizált, melynek következtében elektronikus módon történik a dokumentáltság - számítógépek rögzítik vásárlásainkat, internetezési szokásainkat, egészségügyi állapotunkat, azaz adatok keletkeznek.

Az adatok definícióját és felhasználását *Elektronikai hadviselés* [2] kötetben mutatják be, mely szerint az adat egy nagyon tág fogalom: gyakorlatilag bármilyen jel potenciálisan adatnak tekinthető. A jelek nagyon sokfélék lehetnek, a mindennapi gesztikulációtól a tanult jelekig (írás, olvasás). Az adat független az adathordozótól, azonban feltételez valamilyen médiumot, amely közvetíti, hordozza az adatot (szám, betű), valamint abban egyetértés mutatkozik, hogy az adat az információ alapösszetevője. [2] Az ilyen sokszínű fogalmak esetében általában a legegyszerűbb, s egyszersmind a legátfogóbb definíciót érdemes szem előtt tartani: információnak nevezzük az értelmezett adatot. Az adat „még nem információ”, de azzá válhat. Funkcionális szempontból lényeges tulajdonsága, hogy mindig csökkenti a bizonytalanságot. [3]

A fentiekből megállapítható, hogy az információ önmagában értéket képvisel, amely lehet társadalmi, tudományos, gazdasági érték. Az elmúlt évek exponenciális adatnövekedésének köszönhetően a „big data” a legtöbb területet elérte, különösen a gazdasági–üzleti–informatikai szektorokat. Emiatt egyre nagyobb feladattá vált a minőségi adatok kiszűrése, azok, amelyek a kívánt kérdéshez, információhoz relevánsak. Ez az egyik kihívása a big data-

nak (a big data olyan adathalmazokat jelente, amelyek nagyságukból vagy összetettségükből fakadóan nem alkalmazhatóak rájuk hatékonyan a hagyományos adatfeldolgozó rendszerek).

Az adatok jellemzését a „V" -kel lehet összefoglalni, miszerint: [4]

- *Volume*, azaz mennyiség, volumen. Az adatmennyiség, amelyet előállítunk nagymértékben nő az új technológiáknak köszönhetően és ezzel párhuzamosan a megismerhetőségük is, abban az esetben, ha az adatok mögött meghúzódó mintákat és kapcsolatokat képesek vagyunk felfedni.
- *Variety*, azaz változatosság. A közösségi média írott adataitól a geolokációs adatokig sokféle adattal kell a cégeknek és szervezeteknek dolgozniuk, ezek együttes feldolgozása komoly kihívást is jelent számukra.
- *Velocity*, azaz sebesség. Elfogadottá vált, hogy a világ (és az üzleti élet) felgyorsult, így amellett, hogy az adatok mennyisége és változata is növekszik, mindez egyre gyorsabban történik, azaz egyre gyorsabban is termelődnek újabb és újabb adatok.
- *Veracity*, azaz valódiság. Az adatok valódisága, megbízhatósága és teljessége nélkülözhetetlen az adatkezelésnél, ezért vált egyre fontosabbá az adat minősége, tisztasága, hitelessége.
- *Viability*, azaz életképesség. Azon túl, hogy valós időben történik az adatok gyűjtése, fontos a metaadatokra is figyelni, a big data nem csupán nagy mennyiségű adatok gyűjtése, hanem többdimenziós adatok gyűjtése melyek egyben több változóval dolgoznak. Ezek a változók közötti összefüggéseket kell megtalálni, illetve, hogy az adott kérdésre mely változókat érdemes figyelembe venni, melyek relevánsak.
- *Value*, azaz érték. Miután meghatároztuk mely változókat kell figyelembe venni az adott kérdéshez, megalkotható az a modell, amely megadja a választ. Az elsődleges, preskriptív modell[1] mellett érdemes egy prediktív modellt[2] is létrehozni, amellyel további változók hozzáadásával finomíthatok a válaszok.

Ezt a fajta „zajszűrést" végzi többet között az adatbányászat algoritmusok segítségével. Az adatbányászat cikkben használt definíciója „újszerű, érdekes, értelmes, értékes összefüggések keresése nagy adathalmazban". [4] Az adatbányászat népszerűségének növekedése a növekvő versenyhelyzet miatt a piaci szereplőknek köszönhető, akiknek nagy szüksége van az adatbázisokban lévő hasznos információkra. [5]Az adatbányászat egyik alapfeladata a rejtett összefüggések, kapcsolatok felderítése, legyen szó attribútomok (azaz tulajdonságok) közötti kapcsolatorkól, eltéréselemzésről (*különcpontok* keresése, az adatbázishoz képest nagyban eltérő elemek) vagy webes adatbányasztról (azaz az interneten alapuló információ-kinyerő algoritmusok) [5].

Ez a fajta feltárás több lépést magába foglal: adat – forrásadat (kiválasztott adat) – tisztított adat – transzformált adat (csökkentés és transzformáció) – adatbányászat – minták – értelmezés és értékelés – tudás. [5] Feltárás tekintetében két fő tevékenységet különítünk el: a feltárást és előrejelzést.

Az adatbányászat szakterületéről ki kell emelni Abonyi János Adatbányászat kötetét [6] amely részletesen bemutatja az adatbányászat és tudásmenedzsment összefüggéseit, a tudásfeltárás módszertanát lépésről lépésre. Emellett gyakorlati oldalról bemutatja azon adatelemző eszközöket, amelyek a legelérhetőbbek, pl. a weka, az excel. Az adatok kezelésével kapcsolatosan bemutatja az adatok elő feldolgozását, a felkészítését, megjelenítését, elemzését - vagyis az egész adat életciklusát. Az elemzések és azok

[1] preskriptív: minták alapján trendek, szokások felfedése
[2] prediktív: a feltárt minták alapján próbálunk következtetni a jövőre

felhasználási területét is érintve egy teljes képet ad az adatbányászat elméleti és gyakorlati oldaláról.

Bodon Ferenc [5], az Adatbányászat algoritmusokban bemutatja az adatbányászat fogalmát, feladatait, összehasonlítását a statisztikával, valamint alkalmazási területeit, erős matematika-orientáltság mellett. A témámhoz kiemelten kapcsolódik a mesterséges neurális hálózatokról, valamint a webes adatbányászatról szóló fejezetei.

Nemzetközi szinten Leskovec - Rajaraman - Ullmann féle Mining of Massive Datasets [7] kötetet kell kiemelni, mely az előzőeken túl foglalkozik az internetes marketinggel, az weboldalak ajánlási algoritmusaival, a szociális médiából kinyerhető adatokkal és a nagy-méretű gépi tanulással.

Mindezek katonai alkalmazása valósul meg az információs műveletekben, az információs fölény elérésében. Ehhez, ahogyan Haig Zsolt [8] *Az információs hadviselés kialakulása, katonai értelmezésében* cikkében kifejti, szükség van egy új típusú, összehangolt, szinkronizált, információalapú tevékenységre (információs műveletek), melynek alapja többek között az összadat-forrású felderítés. Az általa említett három dimenzió közül kiemelendő az *információs dimenziót* (amelyet általában kibertérnek is neveznek), ahol az információs folyamatok (adatszerzés, tárolás, feldolgozás, stb.) zajlanak, a kibertámadások és kibervédelem mellett.

ADATOK ELEMZÉSE: OPEN SOURCE INTELLIGENCE (OSINT), HUMAN INTELLIGENCE (HUMINT) VAGY VALAMI ÚJ? CROWDSOURCED INTEL

Az adatelemzési módszerek folyamatosan fejlődnek, melynek az utóbbi évek egyik új eleme a crowdsourcing, mely kifejezést úgy foglalhatnánk össze, hogy „crowdsourcing azt a tevékenységet fedi, mikor egy szervezet egy addig az alkalmazottai által ellátott funkciót vagy feladatot kiszervez egy előre nem pontosan definiált (jellemzően nagy) csoportnak egy nyílt felhívás formájában. Az elengedhetetlen feltételek a nyílt felhívás és a potenciális résztvevők nagy hálózata.” [9]

Ahogyan azt Kovács László doktori értekezésében [13] is kifejtette, az itthoni terminológia a felderítést használja az információszerzési eljárásokra, mely jelentés azonban magába foglalja - az adatok, információk megszerzésén túl - azok feldolgozását, elemzését, értékelését és az eredmény felhasználókhoz való eljuttatását. A közösségi hálókon való információszerzés - így a crowdsourcing is - egyfelől tartozik az emberi erővel folytatott felderítéshez (HUMINT), másfelől a nyílt források felhasználásával folytatott felderítéshez (OSINT).

A crowdsourcing felderítés-elemzési kihívásai jelenleg többek között a forrás anonimizálása (azaz az adatok adaptálásának folyamata, amely során meggátoljuk az egyes személyek azonosítását) a dezinformáció szűrése és a kommunikációs hálózatok hozzáférhetőségében rejlenek. Mindamellett a crowdsourcing, a big data és a mesterséges intelligencia közös felhasználásának egyik sikeres példája a humanitárius krízisek feltérképezése, mint amilyen a Carter Center for Peace [10] szíriai konfliktus feltérképezési projektje (Syrian Conflict Mapping Project). Ez a projekt 2012 óta elemzi az OSINT adatokat (beleértve a közösségi médián feltöltötteket, mint youtube, twitter, stb.) a konfliktushoz kapcsolódóan, amelyeket (hitelesség ellenőrzés után) egy közel valós-idejű konfliktus térképre feltöltenek.

Az előző fejezetben említett *Mining of Massive Datasets [7]* külön fejezetben foglalkozik a közösségi médiából nyerhető adatokkal, a Facebook-adta baráti hálón túl foglalkozik a „közösségek"” azonosításával, melyben segítségünkre lehet az adatbányászatban használatos csoportosítási algoritmusok. Mivel a csoportok gyakran átfedésben vannak, így kibővítik az értelmezési lehetőségeket a hasonlósági mértékkel (simrank), mellyel lemodellezhető nem csak a baráti háló, hanem akár a telefon, email, érdeklődési körből fakadó meglévő vagy potenciális kapcsolati hálózat.

A témában jelenleg Grad-Gyenge László a közösségi média és mesterséges intelligencia kapcsolatát kutatja. Filzmoser-rel és Werthner-rel írt közös tanulmányában [11] bemutatnak egy adaptív értékelési módszert, amely képes feldolgozni heterogén információforrásokat, ezzel javítva az ajánlás minőségét. Ez az adaptív módszer lenne egy tudás-alapú gráf modell, ahol többek között súlyozva lennének az ajánlók közelsége (azaz mennyire valószínű, hogy az ajánlását megfogadja). Ez a tudás-alapú modell jövőbeni felhasználhatósága az adatok és információk megbízhatósági szűrésénél érdekes lehet.

Az adatok összekapcsolásánál egy külön problémát jelent az adatok és meta adatok standardizálása, amelyre egy megoldási lehetőség a szemantikus web, melynek lényege, hogy az interneten található információkat a keresőrendszerek mélyen, valódi tartalomként kezeljék. [12]

Kovács László doktori értekezésében kifejti a felderítési ciklus technikai és technológiai követelményeit - melynek része az integrált összadatforrással dolgozó berendezések és hálózatok, mint amilyen az ISTAR vagy a C4I rendszerek. Következtetése az idő és az információ összefüggéséről - hogy a saját oldali döntésnél és végrehajtásnál az időciklust rövidíteni lehessen - és hogy a döntéshez meglegyen az *optimális* mennyiségű információ, egybecseng a korábban kifejtett mennyiségi adat (big data) és minőségi adat (rich data) közötti követelményekkel. Ahogy a piacnak, úgy a katonai vezetésnek sem *több,* hanem *jobb* adatra van szüksége. Ezt mutatja be az adatfúzió folyamatainak ismertetésével, valamint az összadatforrású felderítéssel (ASAS - all source analysis system), valamint a részrendszereit (felderítő szenzorok, felderítő szervek, külső adatbázisok, fúziós adatfeldolgozó központ, adatelosztó rendszer). A különböző adatforrások (szöveg, fénykép, mozgókép, hang, lokációs adatok) együttes elemzése továbbra is kihívást jelent, történtek előrelépések.

A DEEP LEARNING

A deep learning a gépi tanulás módszereihez tartozik, melynek segítségével a korábbiaknál pontosabb modellek létrehozhatóak.

Ahogyan a Neurális Hálózatokban [14] kifejtik, az élő szervezetek tanulásának analógiája alapján létezik gépi tanulás, illetve léteznek olyan gépek, melyek tanulásra képesek. A gépi tanulás során egy gép – a tanuló rendszer – a környezetéből nyert ismeretek alapján javítja a teljesítőképességét. A *deep learning* könyv idén jelenik meg az MIT Press gondozásában, és több évnyi oktatási anyagot tartalmaz példákkal együtt. Három nagyobb részre tagolódik, az első - alkalmazott matematika - és a gépi tanulás alapjain túl a második és harmadik fejezetek nyújtanak praktikus információkat a hálózatokban történő felhasználásra és a mély tanulási kutatás tekintetében - például különböző modellek alkotásában és építésében.

Egy megfigyelés (például egy kép) többféleképpen reprezentálható, akár vektorként (intenzitás érték pixelenként), akár körvonalakként, akár más értékek mentén. Egyes reprezentációk alkalmasabbak a tanulás megkönnyítésére (ilyen például az arcfelismerés) [15].

A deep learning egyik ígérete az egyszerűbb feladatok kiváltása hatékony algoritmusok segítségével a felügyelt (ellenőrzött) tanulással (az ellenőrzött tanulás során, ahol adva vannak bizonyos tanítópontok, melyekhez tároljuk a rendszertől elvárt kimenetet [16]), a nem- és félig felügyelt tanulással (nem felügyelt tanulásnál nem állnak rendelkezésünkre adott bemenetekhez tartozó kívánt válaszok, a félig felügyelt tanulásnál a felhasználható adatoknak csak egy része van biztosítva a tanuláshoz).

A neurális hálózatok - ahogyan azt bemutatja Altrichter M. - Horváth G. - Pataki B.- Strausz G. - Takács G. -Valyon J.: *Neurális Hálózatok* c. kötete, az egyik kutatási terület [a deep learning / gépi tanulás / mesterséges intelligencia területén belül], amely megpróbálja jobban reprezentálni és modellezni nagymennyiségű jelöletlen adatokat. A neurális hálózatok alapja a biológiai neurális hálózatok, a neuronok kommunikáció mintáit és információ

feldolgozását veszi alapul. A neurális hálózatok alkalmasak olyan feladatok megoldására, amelyekre hagyományos algoritmusokkal vagy szabályrendszerekkel nehezen vagy nem megoldhatóak.[17] A kötet bemutatja a neurális hálózatok felépítését és képességeit, a hálózat típusokat, az ellenőrzött tanítású hálók alkalmazásainak lehetőségeit.

A Microsoft két kutatója, Li Deng és Dong Yu által 2014-ben publikált Deep Learning - Methods and Applications [18] az alap lefektetésén túl bemutatják a technikai felhasználhatóságát a gépi tanulásnak, felügyelet nélkül automatikus jeladóként (autoencoders) és feldolgozóként, beszéd és egyéb hangfelismerőként, nyelvfeldolgozóként, információ lehívóként és visszakeresőként, számítógépes látás valamint a kutatásom szempontjából legérdekesebb része a tanulmánynak a többcélú tanulás (multi-task learning). A bemutatott modellek további felhasználási lehetőségként említik a különböző malware-k osztályozását a kibervédelemben.

A neurális hálózatok tehát nagyfokú hasonlóságot mutatnak az emberi aggyal. Nagy mennyiségű digitális adatot elemezve, ezek a neuronhálók megtanulják különböző feladatok ellátását, mint amilyen a fénykép felismerés, parancsfelismerés vagy internet keresési lekérdezések. Ilyen a Google mesterséges intelligencián alapuló deep learning rendszere, a RankBrain, mely segít keresési kérdések megválaszolásában. A rendszer része a Google keresési algoritmusának, a Hummingbirdnek. A Google keresési találatainak rangsorolásánál a linkek az elsődleges faktorok, a szavak másodlagosak, és a harmadik a RankBrain, amely nem pontosan leírható keresések megtalálásában segít. [19] Azonban – ahogy a biológiai neuronhálók esetében is – a szakértők nem mindig biztosak abban, hogy miért viselkedett (ebben az esetben rangsorolt) ahogyan azt tette. Ettől függetlenül úgy tűnik, a rendszer működik: amennyiben elég adatot szolgáltatunk a mesterséges neuronhálózatoknak, egyre hatékonyabban képes helyes válaszokat találni komplex kérdésekre.

A képfelismerés – másik nevén számítógépes látás – a képek megszerzésének, elemzésének és megértésének módszere, hogy azokból számbeli adat keletkezzen. A képfelismerés három nagy területe, az arcfelismerés (mint amilyen a Facebook automatikus arcfelismerése), az optikai karakter felismerés (betűk / nyelvdetektálás) és a minta felismerés (pattern recognition).

A fényképek automatikus leírása (azaz hogy mesterséges intelligencia segítségével létrejöjjenek a kereshető metaadatok) egyike a meghatározó problémáknak, amelyre megoldást kínálhat a képfelismerés és a természetes nyelvi feldolgozás összekapcsolása.[20] Egyik jelentős területe ennek a nagyfokú képfelismerő képességeknek fejlesztése a deep learning segítségével az önvezető gépjárművek és a fedélzeti rendszerük – például a 360° kamera képfelismerésében és értelmezésében.[21]

Az egyre növekvő adatforgalomhoz és a big data gondolatához lassan hozzászokva nem nehéz elképzelni, hogy a jelenleg valószínűleg a legnagyobb adatforgalom generáló piaci szereplő az önvezető autók lesznek. Mindamellett, hogy a mobilhálózatok sincsenek jelenleg felkészülve ekkora forgalomra a 4G rendszerben, a mesterséges intelligencia a szoftverek mellett a hardverekben is megjelent, mégpedig a mesterséges intelligencia gyorsítókkal (AI accelerator), melyek a mesterséges neuronhálózatok, a számítógépes látás, és egyéb deep learning algoritmusokra fejlesztett mikroprocesszorok a robotikához, dolgok internetéhez (Internet of Things, IoT) és egyéb érzékelés vezérelt feladatokhoz. [22]

Egy képfeldolgozó egység az MI gyorsítókon belül külön fejlesztés alatt áll, melynek feladata a számítógépes látás feladatainak gyorsítása. [23] A képfeldolgozó egység abban különbözik a videó feldolgozó egységtől, hogy a gépi látás algoritmusai képesek több fajta neuronhálózatot is felismerni.

A bemutatott területeken keresztül látható, hogy nem csak a felhasználói oldalon jelent kihívás a nagy mennyiségű adatok (big data) megjelenése és használata, hanem a fejlesztői oldalon is, hiszen a jelenlegi hálózati rendszerek nincsenek felkészülve ekkora

adatmennyiségek forgalmazására. Az egyre növekvő adatmennyiség mellett kihívás a minőségi adatok szűrése, ami elengededhetetlen a hatékony és működőképes modellek megépítéséhez. Mindamellett ahogyan egyre inkább teret nyernek a mély algoritmusok / deep learning rendszerek a mindennapi életben egyre fontosabbá válnak ezek emberekhez fűződő viszonya, amelyet kilépve a sci-fi világából érdemes lenne azelőtt tisztázni (morális, jogi szempontból) hogy ténylegesen kiengedjük a szellemet a palackból.

KIBERVÉDELEM

A kibertérből származó fenyegetések kivédésre a NATO a 2016-os varsói csúcstalálkozó záródokumentumában a hadviselés területét kiterjesztették a kibertérre is. [24] Ezzel majdhogynem egyidejűleg megszületett az EU 2016/1148-as irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, amelyet NIS irányelvként használ a szakma. [25] Az irányelv az első átfogó uniós szabályozás, amely közösségi és nemzeti szinteken egyaránt meghatározza a kibervédelem kialakítandó intézményi rendszerét.

A kibertér - ahogyan a Magyarország Nemzeti Kiberbiztonsági Stratégiája fogalmaz - globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint e rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.

Az EU és a NATO stratégiaalkotási folyamatába illeszkedve a Kormány 2013-ban elfogadta Magyarország Nemzeti Kiberbiztonsági Stratégiáját (1139/2013. (III. 21.) Korm. határozat) [26], majd az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt (Ibtv.) [27] is, melynek végrehajtása során kialakult az információbiztonság magyarországi szervezeti rendszere, mely 2015-ben a Nemzeti Kibervédelmi Intézetben központosul (a Nemzetbiztonsági Szolgálat alárendeltségében).

A jelen cikkben a két legújabb kiberbiztonsági stratégiára térnék még ki, a britre és a németre, melyek előremutatóak az európai kiberbiztonság jövőbeni trendjeit illetően.

A brit Kormány 2016. november 1-án nyilvánosságra hozta a Nemzeti Kiberbiztonsági Stratégia 2016-2021 dokumentumot [30] mely három fő területet határoz meg kibervédelmi szempontból:

1. Megvédeni a lakosságát, vállalatait, valamint a magán- és közszféra különböző vagyontárgyait - beleértve az általa szorgalmazott értékeket.
2. Elrettenteni és megzavarni az ellenfeleket (országokat, bűnözőket, hackereket)
3. Fejleszteni a kritikus képességeket és növelni a saját kiberbiztonsági szektort, elsősorban az oktatás és technológiai fejlesztések területén. Integrálják az oktatási rendszerbe a kiberbiztonságot, létrehoznak két új innovációs központot és egy Kiber Innovációs Alapot.

Az előző stratégiához képest egy aktívabb és beavatkozóbb megközelítést kíván alkalmazni. A kiberbiztonság nemzetközi jellege miatt a következő öt évben szeretnének nemzetközi operatív együttműködést, tisztázni és egyetértésre jutni, hogy mit jelent a felelősségteljes állami magatartás a kibertérben, fejleszteni a nemzetközi partnerek kiberbiztonsági képességeit.

A német szövetségi kormány a 2016. november 9-i kabinetdöntéssel [31] a 2011-ben készült kiberbiztonsági stratégiát egészítették ki, megtartva az egyensúlyt a szabadság és a biztonság garantálása között a digitális világban. A főbb cselekvési irányok a következők:

1. erősíteni a biztonságos és magabiztos cselekvést a digitális világban
2. szélesíteni az állami és gazdasági szféra közötti együttműködést a kiberbiztonság területén

3. jól működő és fenntartható, egész országra kiterjedő kiberbiztonsági rendszer kiépítése
4. aktív szerep az európai és nemzetközi kiberbiztonságpolitika területén.

Ehhez közös kibervédelmi központot kívánnak létrehozni a Szövetségi Belügyminisztérium alatt, valamint egy gyorsan mozgósítható és bevethető kibervédelmi csoport létrehozását az Információs Technológiai Biztonságért felelős Szövetségi Hivatalban, a Szövetségi Bűnügyi Hivatalban és a Szövetségi Alkotmányvédelmi Hivatalban.

Az oktatás területén tudatosítani kell a kiberbiztonság fontosságát és a digitális oktatásnak a köznevelési, szakképzési és felsőoktatási rendszer alkotóelemévé kell válnia.

Mindkét új stratégiából kiolvasható egyfelől, hogy az államok passzív szerepükből aktív szereplőkké kívánnak válni a kibertérben, és ehhez egy részről a gazdasági szektorral történő együttműködés erősítése révén, másfelől a kiberbiztonsági tudatosság növelésével kívánják elérni, végezetül pedig speciális kibervédelmi csoportok létrehozásával.

Az Országgyűlés Hivatalának 2016. szeptember 29-i (2016/44.) Infojegyzetéből [32] kiderül, hogy a kiberbűnözés által okozott kár a világgazdaságban 2014-ben elérte a 445 milliárd dollárt. A kritikus infrastruktúrák elleni támadások 2014/15 között 43%-al nőtt a célzott támadások száma, elsősorban a kormányzati és energetikai szektorban. Mind az Egyesült Királyság, mind Németország növekvő kiberkémkedési aktivitást jelzett.

A 2010-ben Kovács László és Krasznay Csaba közös munkájaként megjelent Digitális Mohács - egy kibertámadási forgatókönyv Magyarország ellen [33] bemutatta egy magyarországi kritikus infrastruktúra elleni támadás forgatókönyvét és annak következményeit. A támadást három részre osztották: egy felderítési és információszerzési szakaszra, melyet nagy részben nyíltforrású hírszerzési adatokkal megoldhatnak a támadók. A második szakasz a pszichológiai műveletek szakasza, az információs támadásoké. A harmadik, végső szakasz pedig maga a támadás megszervezése és végrehajtása. A magyarországi különböző infrastruktúrák üzemeltetői fel vannak készülve egy bizonyos fokig a támadásokra, de az Infojegyzetből [32] kiderül, hogy míg az EU átlagos szintjén 32%-os az infokommunikációs biztonsági stratégiával rendelkező vállalatok aránya, Magyarországon ez az arány 10%, ami igen nagy biztonsági kitettséget jelent.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

Ahogyan azt korábban is megfogalmazták [28] a hadviselés állandó változásban van, melynek következménye, hogy a résztvevők nézeteiket felülvizsgálják, azért, hogy az újabb kihívásokra újabb válaszokat legyenek képesek adni. A cikk elején megfogalmazott adat-technológia fejlődésének üteme és lehetőségei optimizmusra adnak okot, azonban kétségtelen, hogy az információbiztonság, az adatok védelme is kiemelt fontosságú kell, hogy legyen.

A világháló adta (szólás) szabadság olyan információkat és adatokat is illetéktelen kezekbe juttathat, amelyek kárt okozhatnak számunkra. A nyílt információszerzés internet-adta lehetősége oda-vissza működnek [29].

A személyes, mindennapos internethasználatunk (és függőségünk) mellett az államok szervezeti szintjén is kulcsfontosságú lett az információbiztonság, hiszen ki vannak szolgáltatva ezeknek az információs rendszereknek. [28] E kitettséget felismerve született meg a kibervédelmi stratégia Magyarországon [26] [27] mely a jogi hátteret biztosítja.

A deeplearning rendszerek, algoritmusok és mesterséges intelligencia felhasználását tekintve a lehetőségek bővülnek és összekapcsolódnak és a szervezeteknek érdekük a kereskedelmi szektor technológiai fejlesztések nyomon követese és felhasználása, hogy előnybe kerülhessenek a további fejlesztések alkalmazásában.

FELHASZNÁLT IRODALOM

[1] HAIG Zs., KOVÁCS L., MUNK S., VÁNYA L. (szerk.): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* Budapest, Nemzeti Közszolgálati Egyetem, 2012.

[2] HAIG Zs., KOVÁCS L., VÁNYA L., VASS S., NÉMETH A. (szerk.): *Elektronikai hadviselés.* Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[3] FÜLÖP, G.: *Az információ*. Budapest: Eötvös Loránd Tudományegyetem Könyvtártudományi - Informatikai Tanszék, 1996.

[4] BIEHN, N.: *The missing V's in Big Data: viability and value*. Wired Magazine, https://www.wired.com/insights/2013/05/the-missing-vs-in-big-data-viability-and-value/ (A letöltés dátuma: 2016. október 30)

[5] BODON F.: *Adatbányászati algortimusok*. BME, http://www.cs.bme.hu/~bodon/magyar/adatbanyaszat/tanulmany/adatbanyaszat.pdf (A letöltés dátuma: 2016. november 27.)

[6] ABONYI, J.: *Adatbányászat: a hatékonyság eszköze.* Budapest: Computerbooks, 2016.

[7] LESKOVEC, J., RAJARAMAN, A., ULLMAN, J.:*Mining of Massive Datasets.* Stanford University Press, 2014.

[8] HAIG, Zs.: *Az információs hadviselés kialakulása, katonai értelmezése.* MHTT-konferencia. http://www.mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_4.pdf (A letöltés dátuma 2016. november 28.)

[9] HOWE, J.: *Crowdsourcing: A Definition.* June 02, 2006. http://crowdsourcing.typepad.com/cs/2006/06/crowdsourcing_a.html (A letöltés dátuma: 2016. 11. 02.)

[10] The Carter Center: *Syria Conflict Resolution.* www.cartercenter.org/peace/conflict_resolution/syria-conflict-resolution.html (A letöltés dátuma: 2016. 10. 31.)

[11] GRAD-GYENGE, L., FILZMOSER, P., WERTHNER, H.:*Recommendations on a Knowledge Graph.* http://mlrec.org/2015/papers/grad2015recommendation.pdf (A letöltés datum: 2016. november 28.)

[12] GOTTDANK T.: *Szemantikus web.* Budapest: Computerbooks Kiadó, 2005.

[13] KOVÁCS L.: *Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmzhatósága a Magyar Honvédségben.* Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem, 2003.

[14] GOODFELLOW, I., BENGIO, Y., COURVILLE, A. *Deep Learning.* Massachusettes: MIT Press. 2016. Online elérhető: http://www.deeplearningbook.org/ (A látogatás dátuma: 2016.11.13.)

[15] GLAUNER, P.: *Deep Convolutional Neural Networks for Smile Recognition (MSc Thesis).* Imperial College London, *(2015).*.https://arxiv.org/abs/1508.06535 (A letöltés dátuma: 2016.11.05)

[16] *Mesterséges Intelligencia Fogalomtár:* https://mialmanach.mit.bme.hu/fogalomtar/ellenorzott_tanulas (A letöltés dátuma: 2016.11.12)

[17] ALTRICHTER M., HORVÁTH G., PATAKI B., STRAUSZ G., TAKÁCS G., VALYON J.: *Neurális Hálózatok*, Budapest: Panem Könyvkiadó Kft. 2006.

[18] LI, D., DONG Y.: *Deep learning - Methods and applications*. Foundations and Trends in Signal Processing (Vol.7) 2013.

[19] METZ, C.: *AI is transforming google search. The rest of the web is next.*. https://www.wired.com/2016/02/ai-is-changing-the-technology-behind-google-searches/ (A letöltés dátuma: 2016. 11.06)

[20] VINYALS, O., TOSHEV A., BENGIO, S., ERHAN, D.: *Show and Tell: A Neural Image Caption Generator*, https://arxiv.org/abs/1411.4555 (A látogatás dátuma: 2016.11.10)

[21] TALBOT, D.: *CES 2015: Nvidia Demos a Car Computer Trained with "Deep Learning"* MIT Technology Review, https://www.technologyreview.com/s/533936/ces-2015-nvidia-demos-a-car-computer-trained-with-deep-learning/ (A letöltés dátuma: 2016.11.06)

[22] MERRIT, R.: *Google designing AI processors*, http://www.eetimes.com/document.asp?doc_id=1329715 (A letöltés dátuma: 2016.11.15)

[23] HANLEY, S.: *NVIDIA introduces „supercomputer" for self driving cars.* http://gas2.org/2016/01/06/nvidia-introduces-supercomputer-for-self-driving-cars/ (A letöltés dátuma: 2016.11.15)

[24] http://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber (A letöltés datuma 2016.11.28.)

[25] http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU

[26] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

[27] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

[28] Kovács L.: *Terrorizmus a digitális hadszíntéren*, Bolyai Szemle (2006) ?

[29] Haig Zs., Kovács L., Ványa L.: Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata, Budapest: FELDERÍTŐ SZEMLE 10.évf.: (1-2. sz.) p.183

[30] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (A letöltés datum: 2016.11.28.)

[31] http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cybersicherheitsstrategie/cybersicherheitsstrategie_node.html (A letöltés datuma: 2016.11.28.)

[32] MÜLLER T., *Információs Szolgálat Infojegyzet* (2016/44.), Országgyűlés Hivatala, Képviselői Információs Szolgálat 2016. http://www.parlament.hu/documents/10181/595001/Infojegyzet_2016_44_kibervedelem.pdf/d1ca0029-dc3f-4cb3-8d5c-9ed0592d2f1d (A letöltés dátuma: 2016.11.28.)

[33] KOVÁCS L., KRASZNAY Cs.: *Digitális Mohács - egy kibertámadási forgatókönyv Magyarország ellen.* Nemzet és Biztonság, 2010. http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf (A letöltés dátuma: 2016.11.28.)