# Kiberbiztonsági kihívások a 21. században

CSUTAK ZSOLT

Napjainkban a 21. század ipari forradalma zajlik, ahol a digitális adatok és a számítógépes rendszerek virtuális világa elsődleges realitássá vált több milliárd ember számára, ugyanakkor posztmodern világunkra jellemző aszimmetrikus módon a világ lakosságának másik harmada még elektromos áramhoz és ivóvízhez sem jut, nemhogy a világháló nyújtotta szolgáltatások előnyét vagy hátrányait élvezhetné. Az emberiség, a fejlett Nyugati világ vezetésével létrehozta a valaha alkotott legkomplexebb rendszert, az internetes kiber világot. Az okos számítógépes rendszerek alkotta internet, illetve kiber világ negyedszázad alatt rohamtempóban meghódította a világot és átvette az irányítást életünk számtalan szegmense felett, annak minden pozitív és negatív hozadékával egyetemben. Mint minden technológiai újítás, technikai találmány a történelem során, az internetes kiber világ és a mesterséges intelligencia szolgáltatásai is felhasználhatóak jó és rossz célra egyaránt. Ebben a közegben, sajnálatos, ellenben az emberi természetnek megfelelő módon a virtuális polgárok és szervezetek nemcsak a tudomány és a civilizáció előmozdításán dolgoznak, hanem pusztító és igen ártalmas kiber eszközök, illetve szolgáltatások is eluralkodtak, amelyek elhárítása, kiiktatása még egy ideig komoly fejtörést és kihívást okoz minden felhasználó számára.

## Alapvetések

„*lesz majd egy világméretű számítógépes könyvtár,*
*amelyhez bárki bárhonnan csatlakozhat*”
/Isaac Asimov, 1964/

A tech-világ trend-diktáló magazinjának számító Wired magazin 2014. júliusi számában megjelent Joris Toonders cikke szerint a 21. század újabb ipari forradalmának korában az új világ olaja nem más, mint az adat.[1] A holland web marketing szakértő nagyon találó megállapítása ─ Mark Getty[2] internet guru elhíresült *bon mot*-jának parafrázisaként ─ a 21. századot leíró metaforák mesterpéldája lehetne, hiszen amennyiben körbetekintünk a dolgok/tárgyak internete uralta posztmodern világunkban, mindenfelé információ-felhőkbe burkolózó embereket és adatokat feldolgozó okos kütyüket láthatunk. Az előbb említett dolgok internete – avagy *Internet of Things* (továbbiakban IoT) – a 2017-es állapotok alapján közel 25 milliárd okos eszköz web-alapú összekapcsoltságát jelenti az önvezető elektromos autóktól, az önjáró 4-es metrón, az automata teherhajókon keresztül az okos szemüvegekig, továbbá ez a szám a megbízható trendkövető előrejelzések szerint 2025-re elérheti a döbbenetes 75 milliárd

[1] TOONDERS 2014.
[2] Marc Getty, a híres Getty Images vállalat alapítója szerint a 21. század olaja a szellemi tulajdon védelme (GETTY 2000).

interneten összekapcsolt okos eszközt is.[3] Rögtön adódik a jogos kérdés, miszerint ki vagy mi képes felügyelni, irányítani illetve biztonságos ember-barát működést biztosítani e milliárdnyi okos eszköz számára egy olyan fékezhetetlenül fejlődő számítógépek uralta világban, ahol a web-alapú bűncselekmények és visszaélések száma 2015-ben az USA-ban és az Egyesült Királyságban[4] már letaszította trónjáról a szervezett bűnözést és a drogkereskedelmet?

E rövid terjedelmű dolgozat keretei között kísérletet teszünk ilyen és ehhez hasonló kérdések végig gondolására, felvetésére, amelyek tulajdonképpen a nemzetközi rendszer globális biztonságérzetével és meghatározó szakirányú felfogásával foglalkoznak. Lehetőségeink szerint a következő átfogó kérdéseket szeretnénk körbejárni, megvizsgálni: hol tart az emberiség a számítógép-alapú vagy kiber társadalom és gazdaság tekintetében; milyen fő veszélyforrások, kiberbiztonsági kockázatok, kihívások léteznek és fejlődhetnek ki a jövőben; illetve a lendületesen fejlődő mesterséges intelligencia (továbbiakban MI) milyen optimista vagy talán disztópikus forgatókönyveket rejthet az emberiség számára?

Mielőtt belevágnánk a lehetséges válasz-kísérletek taglalásába, fontosnak tartjuk meghatározni a sokat használt, ellenben annál nehezebben megragadható *kiber* és *kibertér* fogalom tartalmi jelentését és használatának kontextusát. Az angol *cyber* megfelelőjeként a magyar nyelv is honosította a görög eredetű *kiber* kifejezést,[5] amely köznapi használatban tulajdonképpen nem egyéb, mint egy tudományos-fantasztikus irodalomból származó *metafora*, amelyet a híres kanadai-amerikai író, William Gibson használt először 1982-ben a számítógép-alapú hálózatok és az ember interaktív virtuális kapcsolatrendszerének leírására.[6] Napjainkra ez a szimbolikus vagy metaforikus tér szélsebesen digitalizálódott világunk másodlagos valóságává vált, sőt, mondhatjuk, hogy az utóbbi évtizedek Z és alfa-generációi számára inkább már az elsődleges realitás tapasztalatát nyújtja, annak minden elképzelhető előnyével és tragikomikus hátrányával együtt. A későbbiekben még szeretnénk behatóbban foglalkozni az emberi mértékkel már szinte követhetetlen sebességgel alakuló, fejlődő kibervilág kihívásaival, illetve a számítógép-alapú mesterséges intelligencia lehetséges forgatókönyveivel és potenciális veszélyforrásaival, a dolgozat terjedelmi keretein belül.

Gibson, akárcsak művelt természettudós és neves sci-fi író társai, mint Clarke, Vinge, vagy legfőképp Isaac Asimov, a számítógépek uralta világról

[3] STATISTA 1. 2018.
[4] THE TELEGRAPH 2017.
[5] *Kübernétész* – görögül hajó kormányosa (KIS 1809, 142), átértelmezve az információ irányításának, kormányzásának készségére utalva.
[6] Gibson 1982-ben megjelent *Burning Chrome* c. novellájában utal erre az összefüggésre, habár a sci-fi brit nagymestere Arthur C. Clarke 1956-os a *Város és a Csillagok című* regényében már használt teljesen hasonló leírást, de nem ezzel a kifejezéssel, hanem „virtuális mátrix" illetve a „virtuális valóság" használatával. Lásd GIBSON 2018.

alkotott elképzeléseiket, illetve a számítástechnika alapját képező adat, információ-feldolgozás, áramlás és rendszerbe szervezés ötletét, természetesen a *kibernetika* nevű új tudományágból merítették, amely a II. világháborút követően forradalmasította a matematika, számítástechnika irányvonalát, és egyben a megváltozott paradigmájú világról szóló filozófiai gondolkodást is. Norbert Wiener 1948-ban közzétett *Cybernetics* c. műve útjára indította a 20–21. század új alaptudományát, amelyben sajátosan ötvözte a természettudományos matematikai éleslátását, illetve mestere, a híres angol matematikus-filozófus, Bertrand Russell mély bölcseleti hatását. Ezen a ponton fontos lehet megjegyeznünk, hogy a II. világháború idején és különösképpen az azt követő hidegháború évtizedeiben, szinte minden jelentős tudományos-műszaki felfedezésnek vagy áttörésnek kapcsolódnia kellett a haditechnikához, illetve a gyakorlatiasabb katonai stratégiákhoz, – egyrészt biztonságpolitikai, másrészt az elérhető pénzügyi és humán erőforrások szempontjából – úgy az Egyesült Államokban, mint a Szovjetunió globális érdekszférájában egyaránt. Természetesen ez alól nem volt kivétel az atom-, vagy kvantumfizika és a kibernetika új tudománya, vagyis Wiener sem, aki többek között a légvédelmi rendszerek működési optimalizálásának számításain is dolgozott Amerikában.[7] A híres Manhattan terv, a SAGE program és az ős-internetet jelentő ARPANET szintén kapcsolódási pontokkal rendelkezhet ehhez a témához és a kibernetika tudományágához, az okos hálózatok, az ember és a számítógép interakciójának úttörő momentumainak leírásával. Jól látható, hogy a kiber elnevezés és a Wiener-féle kibernetika a fogalmi kölcsönzésen túl is rokonítható eszmeiségű, hiszen a kibernetika tudományából, illetve az általa kialakuló újabb tudományágak – mint a játék-, rendszer- és hálózatelmélet elképzelései és alapvetései – tartalmilag is összekapcsolhatóak. Az említett, új paradigmát képviselő kibernetikai tudományágakban felettébb komoly hozzájárulással büszkélkedhetünk magyar tudós gondolkodóink részéről, hiszen gondoljunk csak Neumann Jánosra, Erdős Pálra, von Bertalanffyra, Hunfalvy Jánosra, vagy újabban az erdélyi származású harvardi-budapesti kutató fizikusra, Barabási Albert-Lászlóra, a hálózatok új tudományának vezető kutatójára. Barabási, felhasználva elődjei nagyszerű halmaz- és játékelméleti alapjait, bostoni kutatócsoportjával megpróbálta lemodellezni az emberiség által valaha létrehozott legnagyobb, legösszetettebb és legdinamikusabban fejlődő hálózati rendszert, vagyis az internetet.[8] Megállapításai szerint az internetes hálózat-topológia is hasonló szabályszerűséget mutat, mint a legtöbb ember alkotta óriás-szervezet: kapcsolódási csomópontok és redundáns hálózatok giga-hálózata, akárcsak a mikrokozmosz a makrokozmosz tükörképe. E hálózat-modell segítségével sokkal könnyebben megérthető és áttekinthető a világháló működése és kapcsolódási algoritmusa, amely nyilvánvalóan már rég túlnőtte

[7] WIENER 2018.
[8] BARABÁSI 2013.

eredeti 1970-es évekbeli ARPANET-es[9] alkotóinak legvakmerőbb elképzeléseit is. Kifejezetten izgalmas és érdekfeszítő fejlemény Barabási szerint is, hogy híres magyar írónk, Karinthy Frigyes nem túl közismert „hat lépés távolság szabály" elmélete[10] újból bizonyítást nyert az internet és a közösségi hálózatok működésének vizsgálata során.[11]

Ismert közhelyszerű kijelentés szerint, az Amerikából induló információs szupersztráda, vagy internet az utóbbi három évtizedben meghódította az egész világot, amely ugyanakkor sajnálatosan egy torz, hamis tükörképet mutat nagyon egyenetlen és aránytalan módon fejlődő világunkról, ahol a közel 8 milliárd földlakó fele egyáltalán nem használ számítógépet és nincs internet hozzáférése,[12] sőt, kb. 1,5 milliárd emberhez a villanyáram sem jutott még el. A hadtudomány új kedvenc kifejezésével élve, *aszimmetrikus*, mondhatni párhuzamos tér-idősíkú világokban él az emberiség nagy része, ha például összehasonlítjuk a kaliforniai Szilikon-völgy magasan képzett lakóit az afrikai megaváros Lagos szeméttelepén élő milliókkal vagy akár Indonézia, Kongó, Brazília dzsungel-lakóinak életmódjával, amely sem tudomány-technológiai, sem antropológiai szempontból nem sokat változott az utóbbi évezredben. A világ egyik fele már nem tudja elképzelni hétköznapi életét az internet virtuális valósága és a zsebében lapuló több ezer alkalmazást nyújtó okos eszközök nélkül, amely ugyanakkor nem kevés veszélyforrást is jelent életükre. A számítógépes rendszerek és az azokat összekötő optikai és tengeralatti kábelek globális hálózata segítségével megvalósult az Isaac Asimov által 1964-ben vizionált globális számítógépes információs adatbázis és tudáskönyvtár,[13] az önvezető autókkal és a mesterséges intelligencia hétköznapi alkalmazásával együtt. A döbbenetes mértékű napi kb. 15 Yottabyte adatforgalmat[14] generáló számítógépes világháló eléréséhez csupán két dologra van szüksége egy potenciális felhasználónak: web-kapcsolatú számítógépre vagy okos eszközre (*hardware)* és a kezeléshez szükséges alap készségekre, ún. digitális írástudásra (*software skill*). A világ legnagyobb közkönyvtáraként is működő washingtoni Kongresszusi Könyvtár 15 millió önálló könyves állományának többszörösét kitevő napi globális internetes adatforgalom figyelésére, ellenőrzésére, szűrésére gyakorlatilag nincs lehetőség vagy mód, csak regionális vagy országos szinten – lásd É-Korea esetét vagy a Nagy Kínai Tűzfalat. Az internet és a rajta futó

[9] ARPANET – vagyis *Advanced Research Project Agency's Network*, az amerikai Haditengerészet tudományos kutató ügynöksége, a DARPA által létrehozott egyetemi és katonai számítógépes hálózat az USA keleti és nyugati parti számítógépközpontjai között. 1969-től 1983-ig létezett, amikor különvált és létrejött a polgári hálózat, az ős-internet és a katonai hálózat, a MILNET.

[10] Karinthy írta 1929-ben a *Láncszemek* c. novellájában látnoki módon, miszerint bárkit ismerhetünk a világban, hiszen ismerőseink kapcsolatrendszere exponenciálisan behálózhatja az egész világot. A globális internet *DNS Root Node* csomópontjai illetve a közösségi háló világhíres celebjei is ugyanígy viselkednek tulajdonképpen, amint Barabási A. László bebizonyította 70 évvel később.

[11] BARABÁSI 2013, 34–45.

[12] STATISTA 2. 2018.

[13] ASIMOV 1964.

[14] STATISTA 3. 2018.

népszerű kezelőprogram a *worldwide web* (világháló) atyjai, nevezetesen Vinton Cerf és Tim Berners-Lee sokáig megvalósulni látták nagy álmukat, hogy létrejöhetett a gondolatok, és a tudásmegosztás világméretű szabad, semleges és korlátlan fóruma. Ám a 21. század elején bekövetkezett radikális internetes átalakulások, a közösségi hálózatok mindent elsöprő ereje, a hamis hírek, áltudományos sarlatánságok özöne – nem beszélve a kiberbűnözés, kiber-hadseregek, trollok és zsarolóvírusok elterjedéséről – csúnyán szétzúzták és beárnyékolták az alapítóatyák jóhiszemű idealista elképeléseit.[15]

Az internet világa mindössze bő három évtized alatt létrehozta a több száz milliárd dollár forgalmat bonyolító web alapú kereskedelmet, a globális adathalász és kereső szoftvereket, digitális oktatási platformokat és a világ népességének harmadát elérő közösségi hálózatokat, amelyek napjainkra az elsődleges információforrásokká és véleményformáló, vagy akár forradalom-előkészítő tényezőkké váltak emberek százmillióinak életében. Természetesen a napos oldal mellett ugyancsak megjelent az online kibertér alvilága, a TOR[16] programmal elérhető mély web (*deep web*), és annak a legvisszataszítóbb, illegális bűntanyája, a sötét web (*dark web*), amelynek oldalain, az elemzések szerint mintegy 80%-ban gyomorforgató *hardcore* pedofil tartalmak, továbbá drog-, fegyver- és emberi szervkereskedelem, vagy felforgató politikai agitáció, állam- és társadalomellenes terror-propaganda zajlik (*1. kép*).[17]


**1.kép: A web népszerű modellje**

[15] BERNERS – LEE 2017.
[16] *The Onion Router (TOR)* – (a hagyma 3x titkosítású 2. generációs elosztó program) az amerikai tengerészgyalogság kutatólaboratóriuma által 1997-ben kifejlesztett, és ma már az *Electronic Frontier Foundation* által kezelt nyílt forrás-kódú szoftver a mély webes platformok, tartalmak eléréséhez.
[17] CHEN 2012 – alapos feltáró tudományos elemzés a mély webről.

## A *Szingularitás* hajnalán

A tudományos elméletet a napi valóság gyakorlatába vetítve, a 21. századi okos tárgyak internetes világhálózatának témája, továbbá a mesterséges intelligenciát hordozó ember-nélküli okos eszközök hadászati vagy polgári alkalmazásának kérdésköre igencsak komoly vitatéma a világ vezető hatalmai, illetve a politikai és a tudományos közvélemény számára egyaránt. Ezen a ponton különösen tetten érhető témaválasztásunk interdiszciplináris jellege és össztársadalmi fontossága, hiszen a kibertér és az összekapcsolt okos eszközök sokasága a modern társadalmi és gazdasági létünk minden szegmensét meghatározza és áthatja, következésképpen a kibertérben zajló folyamatok, jelenségek, lehetőségek és veszélyforrások biztonságpolitikai, gazdaságpolitikai és sok más egyéb vonatkozással bírnak. Ebből a nézőpontból elutasítandó és nehezen érthető a természettudósok és számítástechnikai szakemberek gyakori neheztelése az egyéb tudományterületek képviselői irányába – vagy különösebben a hadtudományi és biztonságpolitikai szakértők felé, – hiszen a kibertérben zajló számítógép-alapú történések már évtizedek óta nem csupán a rendszerfelügyelő mérnökök, új alkalmazásokat kialakító szoftverfejlesztő vagy károkozó programok vírus-irtásával foglalkozó kiberbiztonsági szakemberek szakmai privilégiumát képezik.

A társadalmi, gazdasági és katonai vonatkozások tekintetében a kibertér és a mesterséges intelligencia fejlődése hadtudományi, közgazdaságtani és nem utolsó sorban filozófiai probléma is egyben, hacsak pusztán azokra az egyszerű, ellenben megválaszolatlan kérdésekre gondolunk, hogy az emberiség javára vagy inkább kárára válik a virtuális világ eszközeinek általános használata? Mi történik majd az emberiséggel, amennyiben bekövetkezik az MI s*zingularitása,* azaz egyszerűen fogalmazva, az emberi elme és a mesterséges elme egy szintre kerülése? Vajon igaza lesz a számítógép-tervező matematikus Neumann Jánosnak, illetve sci-fi írással is foglalkozó kollégájának, Vernor Vinge-nek, akik már az 1950-es években a technológiai és számítógépes forradalmi paradigmaváltásról – technológiai szingularitásról – értekeztek, amely ha bekövetkezik, várhatóan a 21. század közepe táján, akkor az emberiség által ismert történelem véget érhet?[18] E kérdések a hideg háború éveiben még nem váltottak ki túl nagy intellektuális vagy biztonságpolitikai érdeklődést, többnyire túl elméletinek, hipotetikusnak, illetve fantasztikusnak tartották a problémafelvetést. Nem úgy, mint napjainkban, amikor már a mesterséges intelligencia és a kibertér gazdasági, tudományos, valamint katonai, politikai fontossága megkerülhetetlen tényezővé vált. Gondoljunk csak az IBM *Watson*jára, a Google *DeepMind*-jára, az Apple *Siri*-jére, a hírhedt kiber troll seregekre, a világhíres Sophie-ra az első – szaúd-arábiai – humanoid robot állampolgárra (*2. kép*), nem is beszélve a takarító, felszolgáló, segítő japán háztartási robotokról, valamint az amerikai gyilkos drón repülőgépekről, harci robotkutyákról és mini-robotaknakeresők seregéről. Itt érdemes megjegyeznünk,

[18] VINGE 1993.

hogy a Sophie-hoz hasonlóan a közeljövőben tömegesen előállított értelmes robotok, kiborgok léte nem várt jogi, nyelvészeti és filozófiai kérdéseket is felvet. Nevezetesen, hogy milyen jogokkal, státussal bír majd egy intelligens robot, illetve milyen névmással, jelzővel lehet vagy kell majd őt/azt illetni? Az MI és a robot-munkaerő elterjedésének munkaerő-piaci és szociálpszichológiai hatásairól még talán korai következtetéseket levonni, mindenesetre nagyon drasztikus következményekkel és feszültségekkel fog járni a 21. század társadalmaiban, egy újabb okos eszköz-pusztító, géppromboló *neoluddita*[19] mozgalom kibontakozásának esélyeivel. A robotika és az MI társadalmi, munkaerő-piaci következményeiről számos és sokféle elképzelés született már, Martin Ford szerint az általános alapjövedelem bevezetése az állampolgárok számára megoldást jelenthetne a közeljövőben az általános társadalmi feszültséget generáló helyzet feloldására.[20]

**2. kép: Sophie, az első igazi humanoid robot**

A mesterséges intelligencia és a szingularitás témakörének talán legismertebb képviselője és internetes guruja, az amerikai Ray Kurtzweil szerint – aki amúgy a Google műszaki igazgatója és a Szilikon-völgybéli Szingularitás Egyetem[21] társ-alapítója is egyben – a jelenlegi fejlődési trendeket tekintetbe véve 2029-re várható, amikor az első MI-eszköz sikeresen teljesíti a híres Turing-tesztet.[22] Továbbá 2045-re ez már tömegesen is bekövetkezhet, ami egyenértékű lesz a technológiai MI-áttöréssel, vagyis a sokat említett szingularitással, s annak egyelőre még beláthatatlan következményeivel.[23]

[19] Az 1810-es évek angol textilipari gyári munkás géprombolók modern megfelelői, az okos robotok ellen lázadva munkahelyeik védelmében.
[20] FORD 2017.
[21] Lásd *Singularity University (Szingularitás Egyeteme)* honlapját: https://su.org/about/ (Letöltés: 2018.03.01.)
[22] Alan Turing, a híres angol kódfejtő matematikus, 1950-ben megalkotta az ember-gép 5 perces kérdés-alapú intelligencia-tesztjét.
[23] FUTURE SOCIETY 2017.

A humánum elvesztése miatt jogosan aggodalmaskodó, többnyire konzervatív gondolkodók szerint az emberiség önpusztító módon veszélyes és etikátlan kísérletbe kezdett, amikor tulajdonképpen önmagunkat akarjuk lélektelen, ellenben nagyon intelligens, tökéletes gépekben reprodukálni, újrateremteni.[24] Létre kívánjuk hozni a tökéletes egydimenziós mű-embert, amely lélektelen mechanikus módon gondolkodva végrehajtja parancsainkat az asimovi robotika alaptörvényei szerint, de rögtön adódik a kérdés, hogy mi történik, ha – akarva-akaratlanul – porszem vagy programozási logikai hiba (szakszóval *bug*) kerül a vezérlőprogramba, az MI-rendszerbe, és mondhatni prométheuszi módon, a tökéletes gép-ember az alkotója ellen fordul? Habár e felvetés jelenleg még túl hipotetikusnak tűnhet, ellenben az öntanuló gépek és az MI robbanás-szerű exponenciális fejlődésével a probléma valószínűsége és realitása egyre növekszik. Gondolhatjuk, hogy a kibertérben történő folyamatokkal és a potenciális MI-alapú veszélyforrásokkal maguk a tervezők, és a jövőbe látó filozófus-mérnökök lehetnek leginkább tisztában. Ezt a felvetést látszik erősíteni az a nyílt levél is, amit 2015 júliusában 26 ország 120 kimagasló globális tech-cég vezetője, főmérnöke, szoftverfejlesztője közzétett – köztük Elon Muskkal, a Space X-Teslától és Mustafa Suleymannal, az Alphabet, a Google-t is birtokló anyacég elnökével – a világ vezetői és az ENSZ részére címezve az önjáró, ember-nélküli gyilkos robotok és MI-hordozó pusztító eszközök betiltása érdekében.[25] Ismerve a vérzivataros emberi történelmet és az immanensen bennünk lévő teremtő és pusztító hajlamot, a fenti számítógépes guruk és MI-fejlesztő cégvezetők rettentő veszélyt és jövőbeli konfliktus-forrást látnak ezen eszközök hadászati fejlesztésében és tömeges alkalmazásában, különösképpen emberek ellen. Nyilvánvalóan a versengő államok, és legfőképp a terrorista csoportok minden létező, beszerezhető eszközt hajlandóak fegyverként felhasználni céljaik elérése, érdekeik érvényesítése érdekében, vállalva a kockázatát, hogy az új halálos okos eszköz akár saját pusztulásukat is eredményezheti, amint azt szemléletesen bemutatja a Terminátor 5 című világhírű film Arnold Schwarzenegger és az öntudatra ébredő *Skynet* harcában. Sajnálatos módon, ez az igencsak disztópikus forgatókönyv már nem csupán a valóságtól elrugaszkodott sci-fi filmek világába tartozik, hanem, amint már sokan – Neumann János, Vernor Vinge vagy Molnár Tamás mellett – közvetve utaltak rá, a holnaputáni valóságunk egyik lehetséges verziója. Ezért mindenképp szükséges és fontos döntés lenne az emberiség politikai és technológiai vezetői részéről a megfelelő technológiai óvintézkedések, elővigyázatos jogi és egyéb lépések foganatosítása a mesterséges intelligencia és a milliárdnyi összekapcsolt okos eszköz ellenőrzése, irányítása és kizárólag békés célú felhasználása érdekében. Természetesen nemcsak a kifinomult gondolkodású filozófusok és a humanitást is értékelő, megszállott kiber szakértők, hanem a döntéshozó

[24] Lásd Molnár Tamás amerikai magyar konzervatív filozófus jövőbe mutató *Lélek és Gép* c. esszéjét (MOLNÁR 2000, 194–199).
[25] Angol eredetiben *UAK: unmanned autonomous killer robots* (GIBBS 2017).

politikusok, és a világ-trendekre odafigyelő államfők is érzékelik az idők változását, valamint az új ipari forradalom kihívásait, ezért nem meglepő, hogy Vladimir Putyin, az Orosz Föderáció elnöke 2017 októberében Szocsiban a 14. Valdaj nemzetközi üzleti fórumon a kibontakozó új világrendről tartott előadásában kifejtette, hogy az az ország fogja uralni és irányítani a globális folyamatokat a 21. században, amelyik képes maximálisan kihasználni és irányítani a mesterséges intelligenciát.[26]

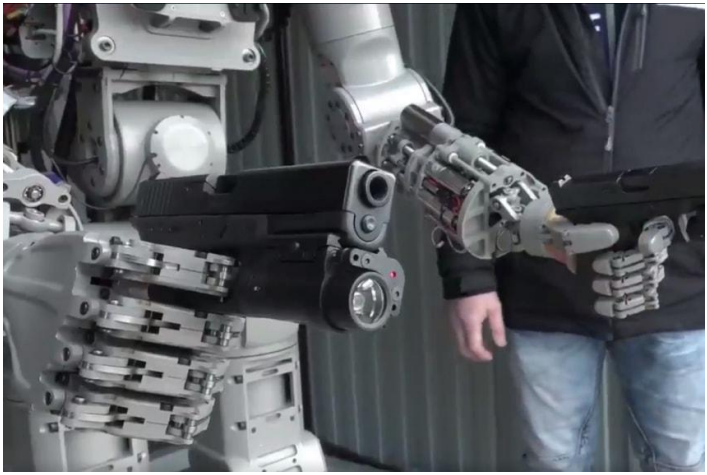
A globális versengés és geopolitikai érdekszféra-konfliktus felfűzhető a Kína, Egyesült Államok, Oroszország és az Európai Unió főtengelyre, amely leginkább a fentebb hangoztatott békés célú és tudományos elvekkel ellentétben az új MI-alapú technológiák hadászati, kibervédelmi és gazdasági előnyszerzés céljából való hasznosításában mutatkozik meg. Az MI-kutatás-fejlesztésbe fektetett humán és pénzügyi tőke polgári és kormányzati célú felhasználása igencsak éles versengést mutat elsősorban a robotika, kibernetika és MI-kutatásban úttörő Egyesült Államokban a szilikon-völgyi agytrösztök, és kutatóközpontok, valamint a NASA és a hadügyminisztérium első számú kutató-fejlesztő ügynöksége, a híres-neves DARPA[27] között. Az orosz és kínai MI-kutatás elsősorban hadászati, védelmi célú tudományos kutatóműhelyekben zajlik, míg Európában sajátos módon többnyire kisebb önálló, koordinálatlan egyetemi kutatócsoportok végzik ezt a fontos tudományos kutató-fejlesztő tevékenységet, jócskán elmaradva az amerikai társaiktól. A fél milliárd lakossal rendelkező Európai Unió, amely deklaráltan 2020-ra a világ legfejlettebb tudás-alapú társadalmát szeretné létrehozni (sajnos egyre kevesebb eséllyel), az Európai Kutatási Övezet (*European Research Area*) és a SPARC robotika-fejlesztési programjában,[28] a 7 éves pénzügyi ciklusban évente mindössze 11 milliárd eurót szán interdiszciplináris tudományos kutatásra, amiből kb. 2 milliárd euró jut a mesterséges intelligenciát célzó projektekre. Mindeközben a 340 milliós lélekszámú, ellenben nagyon innovatív és kevésbé bürokratikus Egyesült Államokban évente 180–250 milliárd dollárt költenek állami és magán vállalkozói forrásokból ugyanerre a kiemelt tudományos-technológiai területre, amit az Országos Tudományos és Műszaki Tanács (*NSTC*) 2016 májusában létrehozott Hálózat és Információs Technológiák Kutatás-Fejlesztési Albizottsága (*NITRDSC*) koordinál.[29] Európában a legtöbb egy főre jutó MI-alkalmazást használó vagy kutató cég érdekes módon az EU-n kívüli államban, ugyanakkor a legnagyobb európai tudományos központnak, a CERN-nek is helyet adó Svájcban található.[30]

A feltörekvő Kínában a 2015-ös évvel kezdődően évente 7–10 milliárd dollárnyi keretösszeget fordítanak MI-alapú kutatás-fejlesztési projektekre, de a valóságban a hadászati célú titkos projektekkel kiegészülve ez a keretszám jóval

[26] VALDAJ 2017.
[27] *Defense Advanced Research Projects' Agency* – Fejlett Védelmi Kutatási Projektek Ügynöksége.
[28] EC 2014.
[29] NSTC NITRC 2016.
[30] CITY AI 2017.

magasabb lehet. Kína kinyilvánított ambiciózus célja, hogy 2030-ra az Egyesült Államokat megelőzve a világ vezető MI-kutató és -alkalmazó országa legyen, ezért Peking mellett létrehozzák Ázsia legnagyobb, 55 hektáros MI kutatóbázisát 2,2 milliárd dollárból,[31] ahol elsősorban a gépi tanulási (*deep/machine learning*) folyamatokat, felhő szolgáltatásokat (*cloud computing*) és nagybani adatelemzést (*big data*) fogják kutatni, fejleszteni több tízezer válogatott szakemberrel.

Az új okos technológiák hadászati célú felhasználását vizsgáló szakemberek, valamint a kiberbiztonsággal foglalkozók érdeklődését is igencsak izgatja a nagyfokú orosz titkolózás ebben a tekintetben, hiszen nyilvánosan csak a Yandex nevű internetes óriás-cég kutatócsoportja és a Kazanyi Állami Tudományegyetem Gépi Tudatosság Kutatólaboratóriuma foglalkozik tudományos jellegű MI kutatással Oroszországban. Ahogy Elon Musk, az úttörő technológiák világszerte ismert magánvállalkozója megjegyezte,[32] a nagyon fejlett és kifinomult technológiákat alkalmazó orosz hadiipart ismeretében, gyanakvásra és aggodalomra adhat okot – különösen Putyin elnök célzott kijelentéseinek fényében –, hogy az orosz MI-kutatásról nem sok megbízható információval rendelkezünk. Mindez arra enged következtetni, hogy valójában az oroszok gőzerővel folytatnak ezirányú titkos fejlesztéseket, kutatásokat. Erre példa a büszkén bemutatott híressé vált FEDOR robot,[33] amely nemcsak autót, de akár az új orosz űrkompot is képes lesz elvezetni, azonban sajátosan orosz módra, mintegy Terminator-szerűen pisztollyal a kezében jelent meg 2017-ben (*3.kép*).



**3. kép: FEDOR – az első orosz robot**

[31] CYRANOSKI 2018.
[32] MUSK 2017.
[33] FEDOR 2017.

Nyilvánvaló stratégiai okokból egyetlen nagyhatalom sem engedheti meg magának, hogy lemaradjon a fentiekhez hasonló, forradalmian új technológiák és korszerű nem-konvencionális fegyvernemek kifejlesztéséből és gyakorlati alkalmazásából.

Sokak szerint a globális méretű világháború már 2007. április 27-én elkezdődött az Észtország elleni összehangolt túlterheléses botnet kiber támadással,[34] amelyet a szakírók már csak *Web War I*-nak vagyis Első Kiber-háborúnak neveznek.[35] A közel egy héten keresztül zajló kiber támadás a kis 1,5 millió lakosú, ellenben a legdigitalizáltabb európai államnak számító balti ország életét teljesen megbénította, leállítva a távközlési, banki, valamint közlekedési informatikai rendszereket. A „szovjet bronz-katona éjszakáját" követő példátlan erejű, demonstratív kibertámadás-sorozat digitális lábnyomai oroszországi szerverekhez vezettek, habár természetesen az orosz kormányzat mindenféle érintettséget és beavatkozást hevesen és indulatosan tagadott a szomszédos parányi EU-s és NATO-tagállammal szemben.

Az utóbbi évtizedben nagyon elszaporodtak a hasonló jellegű, de kisebb intenzitású kibertámadások a világban, és nem túlzás kijelenteni, hogy tulajdonképpen egy „mindenki mindenki ellen" jellegű háború zajlik a kibertérben. Államok és óriás üzleti társaságok próbálnak előnyös pozíciókat, lehetőségeket kiharcolni saját maguk részére a kibertér szabályok és határok nélküli harcmezején. Talán ezért is mondta Toomas H. Ilves volt észt elnök kiberbiztonságot is érintő beszédében, hogy az európai döntéshozó politikusok még mindig nem nagyon értik, vagy nem akarják tudomásul venni a kibertér biztonságpolitikai, gazdasági és katonai jelentőségét, például az amerikaiakkal vagy oroszokkal ellentétben.[36] A digitalizáció gyors előretörése előtti korban szocializálódott politikai és katonai, illetve hírszerzési döntéshozók hajlamosak lebecsülni, vagy nem megfelelő súllyal és fontossággal kezelni a kiber és MI-alapú technológiákat, alkalmazásokat, aminek nagyon komoly és akár tragikus következményei is lehetnek. Elég, hacsak az őrült norvég tömeggyilkos Breivikre, vagy a párizsi Bataclan-klubban vérontást rendező belga terroristákra gondolunk, akik mindannyian a többszereplős online stratégiai harci játékok[37] belső, zárt, titkosított kommunikációs csatornáin keresztül egyeztették akcióikat, illetve könnyedén szerezték be illegálisan lőfegyvereiket.[38]

[34] DDOS-attack avagy túlterheléses parancsmegtagadáson alapuló kibertámadás több tíz vagy százezer számítógép (zombi-gépek) összehangolt másodlagos háttér-irányításával egy célpont ellen.
[35] WW I 2007.
[36] SCHULTZ 2017.
[37] Massive Multi-Player Online Battle Arena, First Person Shooter, Role Play Games mint LoL, WoW, WoT.
[38] KIS-BENEDEK 2016, 150.

## Összegzés

Napóleon, a modern történelem egyik legnagyobb hadvezére is felismerte, hogy az eszmék és a szellem erejét nem szabad alábecsülni, mert hosszú távon legyőzik a kardot is, s később még ehhez hozzátette, hogy tulajdonképpen a háború oroszlánrészt információból áll.[39] Mindkét gondolat – különösképpen két évszázad távlatából – szembetűnő relevanciával rendelkezik és kimagasló helyzetfelismerésről, intellektuális éleslátásról tesz tanúbizonyságot, amelyek meghatározóak lehetnek egy ország vagy haderő sikeressége szempontjából. Napjainkban a kardnál erősebb eszme az évezredek óta újragondolt vallásos hit feltámadásában, és a lehengerlő tudományos technikai felfedezések formájában jelentkezik. Az információ pedig a bennünket körülvevő fizikai, és immár virtuális valóságból származó adatok, jelzések összessége. A modern számítógép-alapú technológiák meghatározzák életünket és minél jobban kötődünk hozzájuk, annál inkább sérülékennyé, kiszolgáltatottabbá teszik a civilizációnkat és a globális gazdaságot egyaránt. Olyan új kommunikációs eszközök és csatornák jöttek létre, amelyekre az emberiség nem igazán tudott felkészülni egy-két emberöltő rövid idősávja alatt, miként hasonló módon az információs technológiák szélsebes fejlődésével sem képesek lépést tartani az információ-biztonságot szolgáló elhárító, védekező technikák és alkalmazások. Ez a biztonsági és információs rés (*security and intelligence gap*) a felhasználó szándékától függően komoly előnyt vagy éppen hátrányt jelent akár egy nagy szuverén állam, egy multinacionális, stratégiai gerinc-hálózatot működtető vállalat, vagy egy kiber fegyvernemhez tartozó katonai egység számára, amelynek pusztító hatását már megtapasztalhatták az észtek, grúzok vagy dél-koreaiak az országuk ellen indított 2007-es, 2008-as, illetve a 2009-es összehangolt kibertámadás-sorozat idején.

**4. kép: Robot jövő?**

[39] CITATUM 2018.

Aszimmetrikus világunk súlypontja visszafordíthatatlanul eltolódni látszik a virtuális kiber világ irányába, annak minden pozitív és negatív hozadékával egyetemben, és láthatóan ezt a folyamatot megállítani már nem, csupán lassítani lehet. A kibernetika, robotika és mesterséges intelligencia új felfedezései sokkal jobbá, élhetőbbé és könnyebbé tehetik az emberek millióinak életét. Ugyanakkor mindezek a folyamatok ártó szándékú, rövidlátó, önző célú vezetők és csoportosulások kezében akár egész civilizációnk vesztét is okozhatják. Az infokommunikációs és MI-kutató szakemberek, valamint a döntéshozók a megfelelő szakértelemmel és a régi bölcsek megfontolt óvatosságának (*prudencia*) és mértékletességének alkalmazásával az emberiség javára fordíthatják a páratlanul új forradalmi technológiákat. Csupán az ősrégi filozofikus senecai kérdést kell felidéznünk és folyamatosan megválaszolnunk, hogy *cui prodest, cui bono*? Valójában, kinek használ és kinek jó a sok új műszaki eszköz, robot és kiber alkalmazás (*4.kép*)?

Ezekre a kérdésekre a jövő történései és társadalmi folyamatai fognak remélhetőleg hamarosan válaszokat adni.

## Irodalom


BARABÁSI 2013 = Barabási A. L.: *Behálózva – a hálózatok új tudománya*. Budapest 2013.

CHEN 2012 = Chen, Hsinchun: *Dark Web – exploring and data mining the dark side of the web*. New York 2012.

FORD 2017 = Ford, M.: *Robotok kora*. (HVG Könyvek) Budapest 2017.

KAPLAN 2016 = Kaplan, J.: *Artificial Intelligence*. New York 2016.

KIS 1809 = Kis J.: *A régi görögök erköltseinek és szokásainak vagy vallásbéli, polgári, hadi és házi rendtartásainak leírása Eschenburg szerint*. Pozsony 1809. (Google e-könyv verzió)

KIS-BENEDEK 2017 = Kis-Benedek J.: *Dzsihadizmus, Radikalizmus, Terrorizmus*. Budapest 2017.

KURTZWEIL 2005 = Kurtzweil, R.: *Singularity is Near*. New York 2005.

MOLNÁR 2000 = Molnár T.: *Lélek és Gép*. Budapest 2000.


## Internetes források


ASIMOV 1964 = Asimov, I.: „Visit to the world fair of 2014.” *The New York Times* 1964.10.14.; http://www.nytimes.com/books/97/03/23/lifetimes/asi-v-fair.html (Letöltés: 2018.03.02.)

BERNERS-LEE 2017 = Berners-Lee, T.: „The system is failing" *The Guardian* 2017.11.15.; https://www.theguardian.com/technology/2017/nov/15/tim-berners-lee-world-wide-web-net-neutrality (Letöltés: 2018.01.29.)

CITATUM 2018 = *Bonaparte Napoleon idézetek*. https://www.citatum.hu/szerzo/Bonaparte_Napoleon (Letöltés: 2018.03.02.)

CITY AI 2017 ="The European AI Landscape" *Medium City AI*. 2017.07.31.; https://medium.com/cityai/the-european-artificial-intelligence-landscape-more-than-400-ai-companies-build-in-europe-bd17a3d499b (Letöltés:2018.03.05.)

CYRANOSKI 2018 = Cyranoski, D.: „China enters the batte for AI talent" *Nature* 2018.01.15.; https://www.nature.com/articles/d41586-018-00604-6 (Letöltés: 2018.03.07.)

EC 2014 = „Making the most of robotics and AI in Europe" *Európai Bizottság Andrus Ansip biztos blogja*. https://ec.europa.eu/commission/commissioners/2014-2019/ansip/blog/making-most-robotics-and-artificial-intelligence-europe_en (Letöltés: 2018.03.07.)

FEDOR 2017 = Final Experimental Demonstration Object Research; http://www.newsweek.com/us-could-lose-russia-china-war-artificial-intelligence-726603; http://www.independent.co.uk/life-style/gadgets-and-tech/news/terminator-robot-fedor-guns-russia-shooting-dmitry-rogozin-a7684406.html (Letöltés: 2018.02.28.)

FUTURE SOCIETY 2017 = https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045/ (Letöltés: 2018.02.22.)

GETTY 2000 = Getty, M.: „Blood and Oil" *Newsweek* 2000.03.04. (2000) 68o.

GIBBS 2017 = Gibbs, S.: „Elon Musk leads 116 experts calling for outright ban of killer robots" *The Guardian* 2017.08.20.; https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war (Letöltés: 2018.03.10.)

GIBSON 2018 = http://www.technovelgy.com/ct/content.asp?Bnum=53 (Letöltés: 2018.02.25.)

MUSK 2017 = https://twitter.com/elonmusk/status/904638455761612800?ref_src=twsrc%5Etfw&ref_url=https%3A%2F%2Fwww.bloomberg.com%2Fview%2Farticles%2F2017-09-05%2Ftake-elon-musk-seriously-on-the-russian-ai-threat&tfw_site=bopinion (Letöltés: 2018.03.01.)

NSTC NITRC 2016 = https://www.nitrd.gov/news/national_ai_rd_strategic_plan.aspx (Letöltés: 2018.02.28.)

SCHULTZ 2017 = Schultz, T.: 'A Decade after „Web War 1"' *The Atlantic Council* 2017.04.26.; http://www.atlanticcouncil.org/blogs/new-atlanticist/a-decade-after-web-war-1-former-estonian-president-blasts-eu-cyber-inertia (Letöltés: 2018.03.02.)

STATISTA 1. 2018 = https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (Letöltés: 2018.01.28.)

STATISTA 2. 2018 = https://www.statista.com/statistics/617136/digital-population-worldwide/ (Letöltés: 2018.02.25.)

STATISTA 3. 2018 = https://www.statista.com/statistics/267202/global-data-volume-of-consumer-ip-traffic/ (Letöltés: 2018.01.26.)

THE TELEGRAPH 2017 = „Fraud and cyber crime" *The Telegraph* 2017.01.19.; https://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/ (Letöltés: 2018.01.29.)

TOONDERS 2014 = Toonders, J.: „Data is the new oil of the digital economy" *Wired* 2014. July; https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (Letöltés: 2018.01.25.)

VALDAJ 2017 = http://en.kremlin.ru/events/president/news/55882 (Letöltés: 2018.02.22.)

VINGE 1993 = Vinge, V.: Technological Singularity. *Whole Earth Review* 1993. Winter; http://cmm.cenart.gob.mx/delanda/textos/tech_sing.pdf (Letöltés: 2018.02.26.)

W.W. I. 2007 = „On Web War I."; https://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/ (Letöltés: 2018.03.08.)

WIENER 2018 = *Norbert Wiener – Wikipédia szócikk*; https://hu.wikipedia.org/wiki/Norbert_Wiener (Letöltés: 2018.01.19)

**Képek forrása**

**1. kép**:Wikipedia.commons

**2. kép**: Reuters

**3. kép**:Advanced Research Fund/Newsweek

**4. kép**: Yahoo Flickr!

## Cyber security challenges in the 21st century

ZSOLT CSUTAK

Nowadays, a new industrial revolution of the 21st century is taking place with the computerized virtual cyber-world turning into primary reality for billions of people, all the same almost a quarter of the world's population has basically no access to electricity or daily fresh water, not to mention the missing benefits or drawbacks of web-based services. The human race, with the leadership of the highly developed Western powers, has created the most complex system or network ever developed in history: the cyber world of the internet. This smart computerized virtual world, basically has taken over the control of many parts of our lives within the relatively short time of a quarter of a century, with all its bright and dark consequences. Similarly to all the technical inventions and technological innovations through human history, the internet-based cyber-world as well as the artificial intelligence might have their positive and negative usage and impacts, too. In this virtual medium, the human users and organisations – sadly yet understandably – act according to the basic human features, namely they tend to use the new applications, softwares and gadgets for various purposes: for promoting science and civilization as well as for creating new destructive cyber weapons and services. This latter, evidently causes serious headaches and challenges for all the cyber security experts and common users worldwide with unpredictable consequences, for the time being.