GEOPOLITIKAI TANÁCS KÖZHASZNÚ ALAPÍTVÁNY

www.cgeopol.hu

dr. Dornfeld László – Keleti Arthur – Barsy Miklós
– Kilin Józsefné – Berki Gábor – dr. Pintér István

Műhelymunkák

A virtuális tér geopolitikája

2016/1. szám

Műhelymunkák

A virtuális tér geopolitikája

2016/1. szám

In memoriam
Rémy Leveau

PAGEO | PALLAS ATHÉNÉ GEOPOLITIKAI ALAPÍTVÁNY

Készült a Pallas Athéné Geopolitikai Alapítvány támogatásával.

dr. Dornfeld László – Keleti Arthur – Barsy Miklós – Kilin Józsefné – Berki Gábor – dr. Pintér István

Műhelymunkák

A virtuális tér geopolitikája

Tanulmánykötet

2016/1. szám

Geopolitikai Tanács Közhasznú Alapítvány – Budapest, 2016
w w w . c g e o p o l . h u

Szerkesztette: Pintér István

A kötetben publikált tanulmányok
a szerzők önálló véleményét tartalmazzák,
így az abban foglaltak nem tekinthetők
a Geopolitikai Tanács hivatalos álláspontjának.

Idézés: Szerző neve (2016) A cikk címe. In: PINTÉR, István: A virtuális tér geopolitikája. Geopolitikai Tanács Műhelytanulmányok, 2016/1. p. oldalszám.HU ISSN 1788-7895. ISBN 978-963-9816-34-3.

Citation: Name of the author (2016) Name of the article. In: PINTER, Istvan: Geopolitics of the Virtual Space. Council on Geopolitics Working Papers, 2016/1. pp.
HU ISSN 1788-7895. ISBN 978-963-9816-34-3.

Tartalom

A kötet szerzői

Barsy Miklós

Hivatásos katonai szolgálatot 25 évig teljesített, ez idő alatt pénzügyi vezető, felügyeleti belső ellenőrzési vezető, majd gazdasági tervező munkakört töltött be és fejlesztőként részt vett a Közgazdasági Informatikai Rendszer kidolgozásában. Szolgálati nyugállományba helyezését követően a polgári életben – egy szállodákat és kulturális intézeteket üzemeltető – gazdasági szervezetnél volt kontrolling vezető. Jelenleg az OTP Bank csoport egy leányvállalatánál dolgozik, ahol szakterületei a gazdasági tervezés, a riporting, a vállalatok piaci megítélésének értékelése, elemzése, az operatív kockázatkezelés és a vállalatirányítási rendszerek szervezése, üzemeltetése, valamint a digitális gazdasági technológia fejlesztése. Résztvevője a digitális bank projektnek és a vállalati adattárház és információs rendszer kialakításának. Végzettségei: Budapesti Műszaki és Gazdasági Egyetem Okleveles Közgazdász, Budapesti Közgazdaságtudományi Egyetem Védelemgazdasági Szakértő, DRMI Naval Postgraduate School Risk Management course. Szakirányú végzettsége: okleveles könyvvizsgáló és regisztrált tagja a Magyar Könyvvizsgáló Kamarának. 2004-ben csatlakozott a Geopolitikai Tanács Alapítványhoz és azóta vezeti az alapítvány Alkalmazott Kockázatkezelési Egységét.

Berki Gábor

Nyugállományú rendőr százados közel 25 évet dolgozott a Belügyminisztérium, a Pest megyei Rendőr-főkapitányság és a Budapesti Rendőr-főkapitányság kötelékében különböző híradó-informatikai beosztásokban. A Gábor Dénes Főiskolán szerzett informatikus-mérnöki diplomát, majd elvégezte a Rendőrtiszti Főiskola tiszti átképző kurzusát. Mesterdiplomát a Zrínyi Miklós Nem-

zetvédelmi Egyetem Védelmi vezetéstechnikai rendszerszervező (C3 system manager) szakán szerzett. A doktori képzést a Nemzeti Közszolgálati Egyetem Katonai-Műszaki Doktori Iskolájában folytatja. Témája a számítógép-hálózati hadviselés. Budapesten él, nős, egy kislány édesapja.

dr. Dornfeld László

Miskolcon született, tanulmányait a Miskolci Egyetem Állam- és Jogtudományi karán folytatta jogász szakon. Már graduális hallgató korában bekapcsolódott a tudományos életbe, négy helyi és két országos TDK-n vett rész, amiből a 2016-os két első helyezést sikerült elérnie. Cum laude minősítéssel szerzett diplomát, majd a Deák Ferenc Állam- és Jogtudományi Doktori Iskolában kezdte meg tanulmányait mint doktorandusz. Kutatási területe a kiberbűnözés elleni fellépés, különös tekintettel a nyomozásra. Munkáiban és előadásaiban a büntető-eljárásjog és büntető anyagi jog mellett a nemzetközi jog és alkotmányjog egyes kérdéseivel is foglalkozik.

Keleti Arthur

Keleti Arthur 1999 óta dolgozik a T-Systems Magyarország Zrt.-ben, jelenleg az IT biztonsági stratéga pozíciójában. Az Informatikai Biztonság Napja (ITBN) konferencia ötletgazdájaként és szervezőjeként átfogó képpel rendelkezik a teljes magyar IT biztonsági piacról és igyekszik annak fejlődését aktívan segíteni. Piaci tevékenységét tekintve a Magyar Külkereskedelmi Bank munkatársaként eltöltött idő után csatlakozott az EasyCall majd az Euróhívó csapatához, ahonnan az ICON (Biztos.Pont vezető, üzletágigazgató, kommunikációs és üzletfejlesztési igazgató), majd a KFKI soraiba lépett át. A kritikus infrastruktúrák és az informatikai rendszerek kiberbiztonságáért tenni akaró szakértő civil ernyőjét képező Önkéntes Kibervédelmi Összefogás alapítója és elnöke. Korábban számítógépes játékok fejlesztésével, tervezésével és játékzenék komponálásával, valamint újságírással is foglalkozott.

„Mélyen hiszek a kreatív innovációban és az emberek közti kommunikáció lehetőségeinek kihasználásában. Vallom, hogy a biztonságra való törekvés segít átgondoltnak, összeszedettnek és megfontoltnak lennünk. A biztonság erőt, stabilitást, megbízhatóságot ad, amely alapja minden kiszámítható gazdasági és emberi rendszernek."

Kilin Józsefné

A szerző rendszerszervező, szakigazgatás-szervező, statisztikus, közszolgálati menedzser. Szolgálati idejének közel felét a Központi Statisztikai Hivatalban statisztikusi munkakörben töltötte. Munkaviszonyának nagyobb részében a Parlamenti Információs (informatikai) Rendszer kialakításában és fejlesztésében vállalt jelentős szerepet, majd törvényalkotási szakmai koordinátori feladatkört látott el. Irányítása alatt épült ki az országgyűlési képviselők tájékoztatásának eljárási rendje és információs rendszere, beleértve a törvényalkotási statisztikai rendszert is. Nyugdíjba vonulása előtt közel 10 évig irányította az éves költségvetési törvényjavaslatok és az azokhoz benyújtott módosító indítványok informatikai rendszerben történő feldolgozását.

dr. Pintér István

A Szegedi Egyetem jogi karán végzett 1983-ban, nemzetközi tanulmányokat folytatott a brüsszeli és a bradfordi egyetemeken, a bécsi Diplomáciai Akadémián, valamint a Budapesti Corvinus Egyetem gazdasági diplomácia szakán. 1990-ig a honvédségnél teljesített hivatásos katonai szolgálatot. 1991-től pro bono ügyvédként olyan civil szervezeteket segített, mint a Transparency International, a Belső Ellenőrök Egyesülete, vagy a Budapest Klub. 2003 óta vezeti a Geopolitikai Tanácsot, amely független szellemi műhelyként a biztonság kutatására szakosodott. Iparjogvédelmi, valamint bank-szakjogászként kutatási területe a nemzetközi pénzügyi rendszer biztonsága és a digitális gazdaságra való átállás. 2006-ban a fehérorosz választásokra delegált EBESZ misszió magyar csoportjának vezetője. 2009-ben az International Institute

for Strategic Studies London tagja, rendszeres résztvevője a Commonwealth Office Wilton parkbeli, valamint a bratislava-i GLOBSEC biztonságpolitikai szemináriumainak. 2008-9 között az Országgyűlés mellett nemzetbiztonsági szakértő. 2009-ben Dohában, 2011-ben Marrakechben az ENSZ Korrupció-ellenes Egyezmény felülvizsgálati konferenciáinak civil megfigyelője. 2010-ben a Független Médiaközpont civil újságírói oklevelét szerzi meg, majd két évig alapító-főszerkesztője a secinfo.hu hírportálnak.

Előadást tartott a legnagyobb magyar egyetemeken kívül Kisinyovban, a NATO németországi képzési központjában, valamint Párizsban. Rendszeresen publikál a biztonság témakörében. Geopolitikai szakértőként folyamatosan jelen van a magyar médiában.

Lektorok

Dr. Botz László Ph.D.

Nyugállományú honvéd tábornok. Egyetemi oktató. Kutatási területei: biztonságpolitika-nemzetbiztonság. Oktatott tárgyak: konfliktus és válságkezelés, kritikus infrastruktúrák védelme, nemzetközi szervezetek válságkezelő tevékenysége, diplomácia. 2003 óta tagja a Geopolitikai Tanács Kuratóriumának.

Dr. Eszes István Ph.D.

Dr. Eszes István közgazdász a Budapesti Gazdasági Egyetem (BGE) tanára. Gimnáziumi tanulmányait követően a Marx Károly Közgazdaságtudományi Egyetemen tanult. Egyetemi doktori címet 1980-ban érte el, 2000-ben pedig a „Közgazdaságtudományok doktora (Ph.D.)" tudományos fokozatot szerzett, 1990 óta tanít a közgazdasági felsőoktatásban. Az általa oktatott tárgyak a marketing, az online marketing, az e-kereskedelem és e-business és vállalati szimuláció. Kutatási területe az online marketing és az e-kereskedelem, e témakörökben az elmúlt évek során nyolc könyve, valamint közel száz publikációja jelent meg.

Erdős André

Erdős André nagykövet multilaterális kérdésekkel megbízott külügyi helyettes államtitkár, majd Magyarország ENSZ-képviselője volt, többek között a világszervezet Biztonsági Tanácsában. Később az ország párizsi nagykövetévé nevezték ki. Jelenleg a Magyar ENSZ Társaság és a Magyar Atlanti Tanács alelnöke, egyetemeken oktat. 2003 óta a Geopolitikai Tanács Kuratóriumának tagja.

Biographies

Mr. Miklós Barsy Lt. Colonel (ret.)

Officially served in the army for 25 years during which he was appointed as financial manager, as supervision and internal control manager, as economic planner, and participated in the development of the Economic Information System as developer. As a civilian, after retiring from the military, he became a controlling manager at an economic organization that operated hotels and cultural institutes. Currently he is working at a subsidiary company of the OTP Bank group, where he specializes in economic planning, reporting, evaluating and analysing companies' market value, organizing operational risk management and corporate management systems, and developing technologies related to the digital economy. He is taking part in the development of the digital bank project and the corporate database and information system. His qualifications: Budapest University of Technology and Economics Certified Economist, Budapest University of Economic Sciences (Corvinus) Defense Economics Expert, DRMI Naval Postgraduate School Risk Management course qualification. Professional qualifications: Certified Auditor and registered member of the Hungarian Chamber of Auditors. In 2004 he joined the Council of Geopolitics Foundation where he has been leading the Foundation's Applied Risk Management Unit.

Mr. Gábor Berki Police Captain (ret.)

Mr. Gábor Berki is a retired police captain who worked for approximately 25 years in different signaller-IT positions at the Ministry of Interior, at the National Police Headquarters Budapest, and at Pest County Police Head-

quarters. He graduated from the Dennis Gabor College as an Expert in IT-Engineering, then he passed the police officer retraining of the Hungarian Police College. He got his Master Degree as C3 system manager after finishing studies on the relevant major at the Miklós Zrínyi National Defence University. Currently he is a PhD student in the Doctoral School of Military Engineering of the National University of Public Service. His field of research is computer network warfare. He lives in Budapest, married and has a daughter.

Mr. László Dornfeld

The author was born in Miskolc and continued his studies on the University Of Miskolc Faculty Of Law. He engaged scientific life in his gradual years and successfully participated with his studies in four local and two national Scientific Students' Associations winning two first places on the national level. He finished his studies with a cum laude degree and continued to PhD studies in the Deák Ferenc Doctoral School. The focus of his research is the countering of cybercrime, especially through investigation. In his papers and lectures he doesn't only focus on Criminal Law and Criminal Procedure but also on specific questions of International Law and Constitutional Law.

Mr. Arthur Keleti

Mr. Arthur Keleti has been working for T-Systems Hungary since 1999, currently in the position of IT Security Strategist. As the founder and main organiser of the conference Day of IT Security (ITBN CONF-EXPO) he has a comprehensive view of the entire Hungarian and European IT Security Market and actively endeavours to help its development. Considering his market activity after a period spent with the Hungarian Foreign Trade Bank (MKB) he joined the Finnish Telecom owned EasyCall and then Eurohivo paging companies then continued his career at ICON (as head of Secure Point, a business line manager and Director of Communications and Business Development) to finally end up working for KFKI later T-Systems. He is also

the founder and president of the Voluntary Cyber Defence Collaboration an independent civil organisation of battle hardened cyber security professionals with the goal to help protect the national cyber space and to support the flow and sharing of critical information.

Previously he developed and designed computer games, composed music for games and wrote articles in journals.

"I sincerely believe in creative innovation and the utilisation of the opportunities given in communication between people. I am convinced that the efforts made at security help us become deliberate, organised and level-headed. Security gives strength, stability and reliability which constitute the basis of every predictable economic and human system."

Mrs. Józsefné Kilin

The author is Systems- and Public Administration Manager. After working as statistician for two decades at the Central Statistical Office, she spent most of her career at the Hungarian Parliament as Director General and played a significant role in the planning and development of the Parliamentary Information System. She managed the development and standardization of the Parliament's information flows, including the legislative statistical system. Prior to her retirement, for ten years she managed the IT processing of the annual budget bills and MPs connecting motions in the Parliament's information system.

Mr. István Pintér LL.M.

Dr. István Pintér, graduated from the Faculty of Law of the University of Szeged in 1983, and then pursued international studies at the universities of Brussels and Bradford, at the Diplomatic. Academy of Vienna, as well as in the economic diplomacy programme of the Corvinus University of Budapest. He served as a professional officer in the Hungarian Defence Forces until 1990. From 1991, as a pro bono lawyer, he assisted non-govern ment

organisations such as Transparency International, the Institute of Internal Auditors, and the Budapest Club. Since 2003, he has been heading the Council on Geopolitics, which is an independent think tank in the field of security. As a lawyer specialized in the fields of the protection of industrial property and banking law, his main areas of research included the security of the international financial system and the transition to the digital economy. In 2006, he was the leader of the Hungarian group of the OSCE mission delegated to observe the elections in Belarus. In 2009, he was a member of the London-based International Institute for Strategic Studies, and a regular participant of the Commonwealth Office's seminars on security policy at Wilton Park, and of GLOBSEC in Bratislava. Between 2008 and 2009, he was a national security expert at the Hungarian Parliament. He was a civilian observer at the review conferences of the United Nations Convention against Corruption in 2009 in Doha, and in 2011 in Marrakech. In 2010 he received a diploma in citizen journalism from the Centre for Independent Journalism, after which he was the editor-in-chief of the news portal secinfo.hu for two years. In addition to the major Hungarian universities, he gave papers at Chișinău, at the German training center of NATO, as well as in Paris. He publishes regularly on the topic of security. As an expert of geopolitics, he is continuously present in the Hungarian media.

Lectors

Mr. László Botz Ph.D.

Retired army general. University lecturer. Research areas: security policy-national security. Subjects taught: Conflict and Crisis Management, Critical Infrastructure Protection, Crisis Management Activities of the international Organizations, Diplomacy. He is member of the Curatoria of the Council on Geopolitics since 2003.

Mr. István Eszes Ph.D.

Dr. István Eszes, economist, professor of the Budapest University of Economics (BGE). Following the secondary school he pursued studies at Károly Marx University of Economic Sciences. He earned his university degree in 1980 and then PhD in Economics in 2000, and has been a lecturer of economic sciences in the higher education since 1990 in the following disciplines: marketing, online marketing, e-commerce, e-business and corporate simulation. Direct areas of his research work includes online marketing and e-commerce. Author of eight books and nearly one hundred scientific publications in the above subjects.

Mr. André Erdős Ambassador (ret.)

Ambassador André Erdős served as Deputy State Secretary of the Foreign Ministry in charge of multilateral questions. Later he was appointed Ambassador of Hungary to the United Nations where, among other functions, he sat on the Security Council as representative of his country. Afterwards, he

became the Hungarian Ambassador to Paris. At present, he is Vice-president of the Hungarian UN Association and of the Hungarian Atlantic Council. He is also teaching at various Hungarian universities. He is member of the Curatoria of the Council on Geopolitics since 2003.

Bevezető helyett

Frédérick Douzet*

Geopolitika a kibertér megértéséhez**

Fordította: Monti Norbert

Nyelvi lektor: Vincze Katalin

* Az Université de Paris VIII Geopolitikai Francia Intézetének professzora, a Castex kiberstratégiai elnöke (IHEDN partneri társulás, az Airbus Group támogatásával)

** A cikk a Hérodote, 2014. év 152-153. számában jelent meg.

Bevezető

A Hérodote havilap már 1997-ben színt vallott az „Internet politizálja a világot" című cikkével, amelyben bejelentette: „az Internet a konfliktusok késleltetése helyett, inkább megsokszorozza és komplikálja azokat" (Douzet, 1997). Az optimista véleményekkel szemben, amelyek a földrajzi határok megszűnését jósolták, havilapunk már akkor rámutatott azon geopolitikai kihívásokra, amelyeket a megállíthatatlan információ és kommunikációs rendszerek elterjedése okoz világszerte.

> *Az internet már önmagában is több geopolitikai konfliktus forrása. A különböző érdekeltségű nemzetek mindenféle dominálási stratégiát vetnek be, hogy ellenőrizhessék a hálózatok tartalmát, működését és gazdasági növekedését. A nemzetbiztonság számára stratégiailag fontos (…) és a hatalmi harcok során rendkívül erős eszköz a csoportok, kisebbségek, politikai, vallási és gazdasági erők kezében, helyi vagy akár világszinten.*

Edward Snowden nyilvánosságra hozott titkos dokumentumai az Egyesült Államok Nemzetbiztonsági Ügynökségének (NBÜ) teljes körű megfigyeléséről, minden kétséget kizáróan mutatják, hogy a földrajzi tényezők továbbra is lényegesek, és a geopolitika még mindig segít a modern világ konfliktusainak megértésében. A stratégiai és nemzetközi tanulmányok (CSIS)[1] kutatója, James A. Lewis is így érvel. Bemutatja, hogy a titkos dokumentumokról szóló információk hatása országonként változó, de globálisan, a számítógépes forradalom ellenére, pillanatnyilag az USA stratégiai érdekei és céljai továbbra is változatlanok maradnak. Az a térképészeti kutatás, melyet Louis Pertnaud[2] végzett, feltárja a politikai határok jelentőségét, még akkor is, ha a technológia átszeli azokat. Az 1990-es évek elején a tér és idő határait nem ismerő kommunikáció robbanásszerű növekedése a demokratikus eszmék és értékek terjesztését és ezzel együtt a demokratizálódás, illetve béketerem-

1 Stratégiai és Nemzetközi Tanulmányok Kutatóközpontja, amelynek a székhelye Washington DC-ben található, három egymást követő évben A Global Go To Think Tank Index az első agytrösztként tarja számon a „Nemzet védelem és biztonság" kérdésében, a University of Pennsylvany éves beszámolója az Egyesült Államok agytrösztjeiről.

2 Az Université de Paris VIII Geopolitikai Intézetének Master hallgatója.

tés reményét ígérte. A hálózatok összekapcsolódásából megszületett kibertér a „globális falu" eszmei képét vetítette fel, amelyet már Marshall McLuhan harminc évvel ezelőtt megálmodott (McLuhan, 1964). A kommunikációs hálózatok bővítése mindig is egy jobb világ utópiáját vetítette elénk (Musso, 2003; Mattelart, 2009); de az internet nemcsak ígéretet, de kihívást hozott magával.

Az internet exponenciális növekedése forradalmasította életmódunkat, felforgatta a gazdaságot, megsokszorozta a kommunikációs eszközeink számát és újabb látóhatárokat tárt elénk, amelyeket csak most kezdünk igazán felfedezni. Ám ugyanakkor területi feszültségeket keltett és megnövelte a konfliktusok számát, hiszen mindenki azért küzd, hogy ellenőrizhesse és szabályozhassa az internetet. Az új fenyegetésekből új feszültségek kristályozódtak ki. Ezek a kiberbűnözéshez vagy az informatikai hálózatok felhasználásához kötődnek, és a már meglévő politikai konfliktusok, katonai összeütközések, gazdasági nézeteltérések, hírszerzés, diplomáciai és kulturális befolyás keretein belül játszódnak le. A Big Data (hatalmas mennyiségű adat) és az Open Data (nyilvános adatok tárháza) megjelenésével egyre több vita alakul ki a magánélet tiszteletben tartásának, a szólásszabadság és egyéb személyi szabadságjogok kérdésében. A Snowden-ügy mindezeket egyszerre érinti, mivel a virtuális térben e tényezők összefonódnak.

Sokáig az internet kérdése a kulturális és technológiai szakértők kis csoportjának a kezében volt. Azonban, a dilemmák berobbantak a közszférába, mivel az internet gyors fejlődésével (közel 3 milliárd felhasználó világszerte) a mindennapi életünk szerves részévé vált, így sok technikai döntés vált politikai és stratégiai döntéssé is. A kibertérben mozgó sok szereplő (egyének, csoportok, start-up vállalkozások) gyors reagálásukkal és elképesztő kreativitásukkal kivették részüket – és a profitot – a hálózat növekedéséből, ha akarjuk, ha nem.

A kormányok, a katonai haderők, a vállalkozások és a polgárok egyre inkább meg akarják érteni a felmerülő kérdéseket, hogy megvédjék érdekeiket. Koherens stratégiát kívánnak kiépíteni, hogy új lehetőségeket ragadhassanak meg a kockázati tényezők kezelésével egy időben. Ez különösen igaz az államok esetében, amelyek mindent átható hatalma szembesül a virtuális tér többi szereplőjével, a bűnözőkkel, a hackerekkel, aktivistákkal, a nagy

magánvállalatokkal, a másként gondolkodókkal, a nem állami szférához tartozó szereplőkkel vagy éppen más államokkal. Ezen erőhatalmi összeütközések nem a klasszikus geopolitikai térben zajlanak, de mégis szükségünk van a geopolitikára az elemzésükhöz.

A geopolitika meghódítja a kiberteret

Felvetődik a kérdés, miképp tudjuk megérteni a kibertérben zajló konfliktusokat a geopolitika segítségével. A geopolitika tanulmányozza és különböző szinteken elemzi a hatalmi versengést és befolyást egy-egy területen. Foglalkozik a területen jelenlévő konfliktus dinamikájával, az ellentmondások bemutatásával, a szereplők stratégiájával, amely a terület ellenőrzéséhez, megszerzéséhez és érdekeik megvédéséhez szükséges az adott földrajzi térségben. Vagyis a földrajzi terület van figyelmének központjában, amely a kibertér esetében nyilvánvalóan problémát okoz. A kibertér egy új területi forma lenne? És, ha ez igaz, melyek lennének a földrajzi határai? Melyek a felségterület határai?

Mit értünk kibertér alatt? Nem létezik egységes és tárgyilagos meghatározás, de több definíciót is találhatunk, amelyek többé-kevésbé pontosak, és tükrözik a szereplők aggodalmait, illetve érdekeit. Az oroszok, ugyanúgy, mint a kínaiak, kevésbé használják a kibertér fogalmát – amely egy külön terület gondolatát ébresztené fel – így inkább internetről beszélnek. Ily módon az információbiztonság és a viták megoldása az állam kompetenciájává válik. A könnyebb megértés érdekében, létezik egy minimális meghatározás: A kibertér egyszer's mind az Internet[3] és az a tér, amit létrehoz: egy immateriális tér, amelyben földrajzi területtől független változások történnek, minden nemzet polgárai között, pillanatok alatt, a távolságot teljesen megszüntetve.

Az internet technikai definíciója általánosan elismert (lásd a szószedetet a kiadvány végén): a világ informatikai hálózata több, mint 40000, ugyanazt

3 Pontosabban a digitalizált adatok automatizált kezelése a számítógépes hálózatok világhálózatán, a Nemzeti Hálózat- és Információbiztonsági Ügynöksége eszerint, 2011. Az információs és kommunikációs rendszerek nemcsak az internetre korlátozódnak, de az internet hozta létre mindazt, amit ma kibertérnek tartunk.

a nyelvezetet használó, autonóm hálózatok kapcsolata. Viszont az általa létrehozott tér meghatározása nehezebb, mert ellentmondásos nyilatkozatokból, a tudományos-fantasztikus irodalomból, az aktivizmusból, a politika és a marketing területéről származó képekből táplálkozik. A *Felhő* csak még bonyolítja a szemantikai ködbe burkolózó kiberteret.

Réteges szerkezet

Ahhoz, hogy jobban megértsük a kiberteret meg kell említenünk annak réteges szerkezetét. A virtuális teret, oly „rétestésztának" tekinthetjük, melynek különböző rétegei között kölcsönhatás van. A szereplők 3, 4, 5 vagy akár 7 rétegre is szétbonthatják ezt. Ennek a struktúrának minden szintjén a szereplők közötti hatalmi versengést találjuk, gyakran technikai kérdésekkel kapcsolatban, amelyek mégis rendkívül geopolitikaiak, ahogy ezt látni is fogjuk. Az egyszerűség kedvéért négy réteget fogunk bemutatni. Az első a fizikai réteg. Az internet infrastruktúráját főleg tengeralatti és szárazföldi kábelek összessége alkotják, melyek az internet gerincét (backbone), illetve a távközlési rendszerek és számítógépek jelentik: egy sor földrajzi és politikai korlát alá vetett, földrajzi területre telepített hardverről van szó, amelyet megépíthetnek, átalakíthatnak vagy tönkretehetnek, rákapcsolhatnak vagy lekapcsolhatnak a hálózatról. Jérémy Robine és Kavé Salamtian cikke megmutatja ennek az infrastruktúrának a fontosságát és stratégiai jellemzőit. Az infrastruktúra, mivel geolokalizálható, könnyebb felmérni térképészetileg, mint kibergeográfiailag. Kevin Limonier térképekre alapozva elemzi az orosz infrastruktúra stratégiai jellegzetességeit és azon ábrázolásokat, amelyek azokat alátámasztják. A fizikai infrastruktúrát a nyitottság és az információáramlás nevében hozták létre integrált biztonság nélkül. Az internet alapítóatyáinak egyike, Louis Pouzin szerint az Internet biztonságossá tételéhez az alapoktól kellene elkezdeni az újraépítését[4].

A második réteget alkotja a logisztikai infrastruktúra. Ide tartoznak mindazon szolgáltatások, amelyek lehetővé teszik az adatátvitelt a hálózat egyik

4 N. Madelaine, «Louis Pouzin: "L'Internet doit être refait de fond en comble"». *Les Échos,* n°21442 du 24 mai 2013, p. 23

pontjáról a másikba, vagyis az információáramlást, hálózati adatcsomagokra bontva, a feladótól a címzettig. A logisztikai felépítés alapvetően a harmonizáción, egy közös nyelvezeten alapszik, amely lehetővé teszi, hogy minden számítógép kommunikálhasson egymás közözött: ez az Internet Protocoll (TCP/IP). Ezek a szolgáltatások az „útválasztók", azaz a hálózati forgalomirányításhoz szükségesek, hogy az adatcsomagok áramolhassanak a hálózatok között. Ezen kívül van az Azonosító (a hálózati azonosító vagy felhasználói név) és a Hálózati cím (amely átalakítja a címeket jelölő számsorozatokat olvasható szavakká a felhasználó számára). Más tényezőket is lehet geolokalizálni néhány technikai beállítással (domain nevek, IP címek…). Bertrand de La Chapelle interjú során beszél a hálózati címek körül folyó vitákról. Az Egyesült Államok továbbra is erős szimbolikus hatalmat gyakorol a hálózati címek felett a Kereskedelmi Minisztériumon keresztül. Dominique Lacroix pedig bemutatja a domain nevek megszerzésének gazdasági és politikai kihívását.

A harmadik réteg az alkalmazásokból áll, ezek felhasználóbarát informatikai programok, amelyek lehetővé teszik, hogy bárki használhassa az internetet anélkül, hogy ismerné a számítógépes programozást (Web, email, közösségi oldalak, kereső motorok). A Snowden-ügy világosan megmutatta néhány nagyvállalat (Google, Facebook, Amazon…) alkalmazásainak világszintű sikerét. Ezek azok a nagyvállalatok, amelyekre a felhasználók szívesen rábízzák személyes adataikat, és amelyeket a marketing, illetve az ország információszolgáltatói ügyesen kiaknáznak. Mindezt Stéphane Frénot és Stéphane Grumbach a gazdaság új fekete aranyának tartják. Az adatok nem tűnnek el így a felhőkben (Cloud), de a magán- és közszereplők kezelés alatt álló szerverekben tárolják őket.

Végül a negyedik réteg a társadalmi információ és interakció rétege, amit néha kognitív vagy szemantikai rétegnek is neveznek. Itt játszódik felhasználók eszmecseréje valós időben szerte a világon, és ezt lehet a legnehezebben geopolitikai szempontból megérteni és ábrázolni. Ez azonban a legkevésbé sem irreleváns, amikor meg kell határoznunk mely országok a legbarátiabbak a Facebook közösségi oldallal kapcsolatban, milyen nyelven lehet elérni a Föld bizonyos régióinak az információit, honnan indulnak ki a közösségi oldalakon folyó lázadások vagy félrevezetési kampányok egy kormánnyal vagy intézménnyel szemben.

A kibertér lenne egyszerre mindez: emberek, adatok és számítógépek hálózata – és egyre inkább elterjedő mobil eszközök hálózata (telefonok, tabletek és hamarosan hűtőszekrények, karkötők, sportcipők…); információs tér, területhez nem kötött információcsere, amelyet nehéz megérteni. Fizikai területre épített materiális infrastruktúrából áll, ide értve a világűrben megtalálható műholdakat is. A felhasználó és céljai szerint tehát a kibertér jelenthet egy fizikai infrastruktúrát vagy teljesen más fogalmat.

A geopolitika egy létfontosságú eszközt nyújt a kibertér megértéséhez: az ábrázolásokat. Ezen ábrák konstrukciók, gondolkodásmódok, a geopolitikában szereplő eszmék együttesének többé-kevésbé logikus és koherens halmaza. Az objektív tényekre alapozza a megfigyeléseit, megőrizvén mélyen szubjektív jellegét. Az ábrák nem semlegesek: befolyásolhatják a szereplők stratégiáit, hogy meggyőzzék, felbujtsák, lelkesítsék, mobilizálják a további szereplőket (akik lehetnek a választópolgárok, az aktivisták, a befektetők, a haderők vagy az internet felhasználók…).

Gyarmatosítás a kibertérben

A kibertér nem egy földrajzi értelembe vett terület, azaz „térség, amelyen egy emberi csoport él, és amelyet kollektív tulajdonának tekint" (Lacoste, 2003), vagy az államok szempontjából ítélve „határokkal körbezárt térség, amelyen az állam kifejti a jogkörét" (Lacoste, 2003). Olyan térnek tekinthetjük, amelyben az emberek érintkeznek, de még földrajzi területnek is feltűntethető, mint ahogy Alix Desforges a virtuális teret ábrázolta a cikkében.

A kibertér fogalma paradox módon két teljesen ellentétes okból született meg. Először a sci-fi író, William Gibson (1984) írt az elektronikusan generált, „végtelen kuszaság" háromdimenziós teréről, amelybe a szereplők számítógéphez csatlakozva lépnek be. Mentálisan megjeleníti az egész emberiség informatikai rendszereinek szívében elraktározott információit és adatait, amelyet az internet felhasználók generációja fog birtokolni.

Ez a megjelenítés lázba hozta az internet úttörőinek képzeletét. 1990-ben meg is alkották az Electronic Frontier Foundation-t (EFF), jóval azelőtt, hogy az internet a nagy közönség színe elé került volna. Az alapítvány neve a „ha-

tárvidékre" és vadnyugatra hivatkozik, amely Frederick Jackson Turner történész elmélete szerint az amerikai demokrácia bölcsője. John Perry Barlow, alapító tag, 1996-ban még a virtuális tér függetlenségi nyilatkozatát is megfogalmazza, amelyben kijelenti, hogy a kibertérnek saját szuverenitása van, illetve, hogy az „intellektualitás civilizációjában" a világ kormányainak törvényei nem alkalmazhatóak. Alix Desforges szerint az 1960-as évek kulturális forradalma inspirálta a hálózat felépítését a nyitottság, az önirányítás, a szabad információcsere és szólásszabadság jegyében. Erősen decentralizált, központ nélküli, hogy az információ szabadon tudjon áramlani, bármilyen akadály ellenére is. Olyan világ ez, ahol minden, ami az emberi elmétől származik „újratermelhető és terjeszthető anélkül, hogy pénzbe kerülne". A szabadság szele folyamatosan lelkesíti a hacktivistákat, hogy harcoljanak minden olyan próbálkozással szemben, ami a szabad információáramlást gátolná az interneten.

Egy ideig elhanyagolták a koncepciót, de a virtuális tér újból előkerül a 2000-es évektől kiindulva. Az államok vitáikban úgy állítják be, mint olyan terület, amelyet meg kell hódítani, ellenőrizni, felügyelet alatt tartani és birtokolni. Terület, amelynek tiszteletben kell tartani a határait, a szuverenitását és törvényeit. Legfőképpen azonban a nemzetbiztonság elleni fenyegetésként és a nemzeti érdekek célpontjaként látták.

A 2007-ben Észtország ellen indított támadások sokként érték a kormányokat, köztük Franciaországot is. A kormányok felismerték, hogy mennyire le vannak maradva az ilyen fenyegetések kivédésében A tallini szovjet hősi emlékmű eltávolítása nagy port kavart fel. A kormányoldalak, a nemzetbiztonsági szervek, de a bankok és más közszolgáltatásokat is ért a masszív szolgáltatásmegtagadással járó támadás (DDoS) zajlott le. Több tízezer zombi számítógép hálózata, vagyis botnetek árasztották el egyszerre az ország hálózatait, amíg teljesen le nem bénították őket (fekete képernyő). Ezek a botnetek vírussal megfertőzött gépek, amelyeket sokszor a felhasználók tudta nélkül irányítanak. A támadással napokon át megfosztották a lakosokat az online közszolgáltatásoktól. Az orosz kormány tagadott minden felelősséget, még ha a technikai és politikai nyomok Oroszország felé mutattak is. Az azt követő évben a Grúziát ért kibertámadás ugyancsak megmutatta, hogy egy ilyen jellegű csapás milyen módon is tudja segíteni a konvencionális erőket

egy fegyveres konfliktus során. Azóta több ország, köztük Franciaország is, megerősítette kapacitását és próbálta ellenőrizni, illetve növelni hatalmát a kibertérben.

Stéphan Dossénál, a francia védelmi minisztérium köztisztviselőjénél tisztábban nem is fogalmazhatnánk: „Úgy tűnhetett, hogy az államoknak fel kellett húzniuk a zászlót a kibertérben, amit elfoglalnak, és ahol szuverenitásukat gyakorolják, hogy a szűzföldeket gyarmatosítsák és felkészüljenek egy esetleges támadásra" (Dossé, 2010). A 2013-as biztonsági fehér könyv tisztán kijelenti, hogy a kibertér stratégiai prioritás és a kiberfegyverek az arzenál részét képezik.

Kibertér: Az államok ellentámadása

Kevés állam látta előre, hogy milyen stratégiai tétje lesz az információs és kommunikációs rendszerek gyors növekedésének és interkonnekciójának. Stratégiai szinten csak Oroszország, Kína, illetve az Egyesült Államok reagáltak hamar. Oroszország és Kína történelmükből fakadóan is ismerik az információ fontosságát, míg az Egyesült Államok a technológiai fejlődés élvonalán jár. Az innováció kezdetileg az okosan reagáló egyének és kis vállalkozó csoportok kezében volt. Ők tudták a legjobban kihasználni az új, és alig szabályozott médiumok adta lehetőségeket. Nekik köszönhetjük azokat a kiváló eredményeket, amelyek radikálisan megváltoztatták életvitelünket (szórakozás, kollektív finanszírozás, aktivizmus, marketing…), és így eddig elképzelhetetlen lehetőségeket tártak fel. Ám ugyanígy hackerek, bűnözők és bérencek is gyorsan, hatékonyan ki tudták használni ezeket az eszközöket. Az utóbbiak tevékenysége idézte elő a politikai hatalom és intézmények jelenlegi reakcióját. Bruce Schneier információbiztonsági szakértő kiválóan rátapint arra, hogy a kibertér konfliktusai a disztributív hatalom (aktivisták, disszidensek, hackerek és bűnözők), illetve a hatalom hagyományos birtokosai (kormányok, nagyvállalatok, intézmények) között alakultak ki[5]. Megmutatja, hogy kezdetben a rendszer hozzáférhetősége és decentralizációja a kis szereplőknek kedvezett – ideértve a rosszindulatú szereplőket is. Látszólag

5 „The battle for power on the Internet: Bruce Schneier TEDxCambridge 2013" a TEDxTalks által publikált videó 2013.09.25. –letöltve 2013.02.16 (www.youtube.com)

legyőzhetetlenné tette őket az a hatékonyság és koordinációs kapacitás, amit a rendszer nyújtott. Azonban a hagyományos szereplők a stratégiai téthez mérhető nagy eltökéltséggel állnak bosszút.

A biztonság nevében

Szuverenitásuk megvédésének érdekében az államok teljes erőbedobással térnek vissza a kibertérbe. A kibertámadások megállításának nehézségei kihathatnak a nemzetbiztonsági és a területvédelmi kapacitásaikra. Leginkább a létfontosságú infrastruktúra védelmét hangsúlyozzák, hiszen azoknak bármilyen jellegű megzavarása vagy szabotálása a civil lakosságot is veszélyeztetheti. Ez a fenyegetés szítja a legbaljósabb diskurzusokat is. Azon vitáznak a szakértők, hogy egy kibertámadás milliók halálát és államok bukását is okozhatja, még ha ez egy kis valószínűségű és be nem bizonyított, de ki nem zárható lehetőség. Olivier Kempf rámutat arra, hogy a terrorizmus és a kibertér közötti kapcsolat nem is olyan egyértelmű, mint ahogy azt feltételeznénk a domináns véleményekből. Rodrigo Nieto Gomez elemezte a kiberterrorista amerikai ábrázolásának konstrukcióját és szerepét a biztonságpolitikában. Ez az ábrázolás általában kriminalizálja a hackereket és ösztönzi a titoktartást ott, ahol az innovációnak pedig hatalmas ereje lenne. Ezzel elrejtik, hogy valójában mit is jelenthetne a terrorizmus a kibertérben.

A terroristatetteken kívül kritikus fontosságú az információ kézben tartása. Az információ gyűjtése, elemzése, manipulálása stratégiai előnyt jelent az ellenséggel szemben és megingathatja bizalmát saját információjának megbízhatóságában. A kibertámadások megzavarhatják az ellenség kommunikációját, és hatással lehetnek műveleteire, hiszen a koordináció egyre jobban alapszik a hálózatokon. A klasszikus elrettentő és biztonsági stratégiák nehézségekbe ütköznek, mert bonyolult kideríteni a támadások mögött állók kilétét és a támadások miértjét. Ugyanígy megnehezíti a klasszikus stratégiák bevetését az, hogy a technológia olcsó és könnyen elérhető, ezzel felerősítve a kis szereplőket a nagyhatalmakkal szemben. Azok az országok, amelyek leginkább függnek a hálózatoktól ugyanígy a legsebezhetőbbek a támadásokkal szemben. Ám az is valószínűbb, hogy fejlesztik hálózataik

védelmét, offenzív kapacitásukat, illetve kihasználják a hálózatok adta lehetőségeket, hogy növeljék erejüket és hatékonyságukat.

Az ideológiai harc a közösségi oldalakon is folytatódik. A demokráciában a kormányok nem hagyhatják figyelmen kívül az ellenzéket és a közvéleményt. Viszont, még a nagyhatalmak sincsenek felkészülve azokra az online „csomagokra", amelyet a dzihadisták tesznek elérhetővé, hogy gyorsan radikalizáljanak egyéneket, és egyénre szabott terrorista praktikákat ajánljanak.

Másrészt a belbiztonság és közrend megtartását kihívás elé állítja az a szervezett vagy szervezetlen bűnözés, amely a hálón található. Ez lehet illegális behatolás, adatlopás és megsemmisítés, illetve bármilyen bűnözői tevékenység a hálókon (bankrablás, csalás, személyazonossággal való visszaélés stb.). Az azonosítást nehezíti a bizonyítékok volatilitása. Gyors közbenjárás hiányában a bűnjelek eltűnhetnek a képernyőkről. A távtevékenység pedig tovább bonyolítja a nyomozást, a gyanúsított letartóztatását és bíróság elé állítását. A bűnözés könnyedén áthidalhatja a határokat a hálózatokon keresztül, ami nem igaz a rendfenntartókra. Ha a bűnöző és az áldozat egy országban találhatók, a hatóságok gyorsan tudnak cselekedni. Viszont amikor a bűnöző, az áldozat, és/vagy a hálózat különböző országokban találhatók, nemzetközi együttműködésre van szükség mind a rendfenntartók, a rendőrség és a bíróságok részéről, amelyek sokszor túl lassúak ahhoz, hogy hatékonyan lépjenek közbe. Igazságszolgáltatási határok szelik fel a kiberteret, és a rendőrség csak hivatalos engedéllyel léphet be, még ha csak a bűnözőt kívánja elfogni.

A kiberbiztonság dilemmái arra késztetik a kormányokat, hogy aktívan figyeljék a kibertér történéseit, ezzel kockáztatva, hogy az egyéni szabadságjogokat megsértik, ahogy azt a Snowden-ügy is felfedte. Az önkényuralmi rendszerek számára a kibertér megfigyelése és ellenőrzése létfontosságú a rendszer megőrzésének érdekében, mert a legnagyobb fenyegetés számukra belülről jön. A nagymennyiségű információmozgás gyengítheti az önkényuralmi rendszereket, ám ez az információ ugyanígy nagy szerepet játszik a disszidensek és más fekete bárányok felismerésében. Fréderick Douzet Kínáról szóló cikkében bemutatja, hogy eddig a rezsim kreatívan tudta venni az új kihívásokat.

A szuverenitás kihívásai

Bertrand de La Chapelle, az Internet et Juridiction (Internet és Igazságszolgáltatás) projekt alapítója egy interjúban említette meg, hogy a szuverenitás gyakorlása mennyivel bonyolultabbá vált az államok számára, mivel a joghatásköri korlátok kibogozhatatlanok a kibertérben. A kibertérben a tevékenységek túlmennek a határokon, és az állam már nem tudja érvényesíteni a törvényeit és jogszabályait. Ez akár saját területén, saját polgáraival is megtörténhet, ha éppen egy külföldi vállalkozás nyújtja a szolgáltatást. A jogkör a kibertérben gyakran a hatalmi versengések terméke, semmint konszenzuális. A visszatérő konfliktusok egyike a szólásszabadságot érinti. Franciaországban hozott szigorítások például elképzelhetetlenek az Egyesült Államok jogi keretein belül. 2012-ben antiszemita kommenteket posztoltak franciául egy, a Twitter-en indított, élményítő viccversenyen a (zsargonban hashtagként mondott) #UnBonJuif („Egy jó zsidó"). Ez hosszú huzavonához vezetett a francia igazságszolgáltatás és az amerikai cég között. Csak tíz hónapos per után fogadta el a Twitter, hogy kiadja azokat az adatokat, amelyek lehetővé tették a posztolók beazonosítását. Az internet nagyvállalatai – a híres GAFA (Google, Amazon, Facebook, Apple) oly mértékű gazdasági befolyást szereztek, amellyel hatalmi játszmába szállhatnak. Nem könnyen vetik alá magukat egy olyan állam igazságszolgáltatásának, amely az általuk tárolt tartalom eltávolítását vagy a felhasználóik adatainak kiszolgáltatását írja elő. Ez az önkényuralmi rendszerek esetében a felhasználók védelmének szempontjából előnyös lehet, de ezzel egy nyereséges piac elvesztését kockáztatja a vállalat.

Végül az államok gazdasági és pénzügyi szuverenitása kemény kihívások elé néz. A hálózatok jelentősen meggyorsították az árucikkek és a pénzügy forgalmát, amely megkönnyíti az adócsalást és a nemzetközi pénzügyi válságok elterjedését. Dominique Lacroix cikke többek között bemutatja, hogy az új domain nevekre jelentkező nagyvállalatok adóparadicsoma hol koncentrálódik. A Yahoo! tevékenységének átszervezése Európában Írországban történt (ahol a társasági adó 12,5%-os[6]), ami a vállalat különböző adóköteles

6 Összehasonlításképpen a kivetett társasági adó azon vállalatok esetében, amelyeknek a tőkéje kevesebb, mint 75%-ban magánszemélyek kezében van, 33,1% az összes nyereséget illetően. (impots.gouv.fr)

európai telephelyeinek áthelyezéséhez vezet. A hálózatok növelik az ipari kémkedés, a szellemi és ipari tulajdon vagy az üzleti titok ellopásának kockázatát és nagyságát. Danilo D'Elia elemzi ezeket a kockázatokat és megmutatja, hogy a geopolitikai konfliktusok milyen potenciált rejtenek. Túlmegy a nemzetek gazdasági és pénzügyi erején, olyan mértékben, hogy a magán szektor érdekei összekapcsolódnak a nemzeti érdekekkel és a vállalatok kiberbiztonsága nemzeti érdekké is válhat. Magától értetődik, hogy a kiberbiztonság piaca ugyanannyira érzékeny, mint amennyire virágzó, ami arra ösztönzi a kormányokat, hogy részt vegyenek benne.

Új fenyegetések?

Sok fenyegetés nem jelent újdonságot, de sokkal gyorsabban, erősebben, eddig nem tapasztalt mértékben terjednek a kibertérben. Legyen szó kínai hackerekről, akik nagymennyiségű információt lopnak el cégektől (a Mandiant beszámoló szerint), a 1,7 millió fájlról, amit Snowden adott le, a hihetetlen nagyságrendű adatról, amit az NBÜ gyűjtött össze vagy az Aramco 300000 számítógépéről, amiket egy csapásra szabotáltak 2012-ben; a következmények gyorsabbak, erősebbek és nagyobbak, mint amit eddig tapasztaltunk.

Néhány kihívás viszont a kibertér sajátja: beazonosítani és bebizonyítani a támadás forrását, előrelátni, megakadályozni, vagy megállítani a támadást; a szuverenitás és igazságszolgáltatás szövevényessége; a technológia gyors evolúciója és a hálózatok permanens rekonfigurációja, amelyeknek gyors és folyamatos adaptációra van szükségük; a kísérleti kiberfegyverek kifejlesztése; ezen fegyverek tesztelésének nehézségei; hatásainak kétségessége, hiszen sok függ az ellenfél kapacitásától; és végül a tény, hogy a legjobb támadások azok, amiket nem veszünk észre… Sokak szerint a kibertér új területe (vagy környezete) a hadászatnak, a szárazföld, tenger, víz és űr mellett. Ám a többivel ellentétben ez nem egy természetes környezet – minden, ami a kibertérben történik mesterséges – és így átíveli a többi közeget.

A stratégiának, amit az államok fejlesztettek ki, hogy megvédjék szuverenitásukat és maximalizálják hatalmukat a kibertérben, geopolitikai következményei vannak. Komoly kérdéseket vetnek fel, új fenyegetéseket kreálnak.

Miért tanulmányozzuk a kibertér geopolitikáját?

A kiberkonfliktusok technikai szálainak van mivel elbátortalanítani a polgárokat, illetve az emberi- és társadalomtudományok kutatóit. Nem véletlen-e vajon, hogy e kérdések hosszú ideig a szakértők kis csoportjának a kezében maradtak? Miért foglalkozunk velük mindezek ellenére? Mert ebben a világban szeretnénk élni. Mert az információs és kommunikációs rendszerek állandó jelleggel jelen vannak a mindennapi életünkben, és az ezzel kapcsolatban meghozott döntések érinteni fogják az életünk minden aspektusát. Mert számos hatalom anélkül fejlődött ki, hogy az ellenzékkel megvitatták volna a fékek és ellensúlyok rendszerét.

Egy fordulóponton vagyunk és sokan közülünk, beleértve választott képviselőinket, felfedezik azokat az eszközöket, programokat és politikát, melyeket a nagyvállalatok, a kormányok vagy a bűnözők fejlesztettek ki azért, hogy megvédjék az érdekeiket és maximalizálják a teljesítményüket, profitjukat a kibertérben. A régi stratégiai paradigmák és nemzetközi játékszabályok nem érvényesek, az újak még megírásra várnak. A technológiai fejlődés gyorsasága meghaladja egy új jogi keret kidolgozásnak vagy a törvények adaptációjának gyorsaságát. A partnerek közötti titoktartás kultúrája, a bizalomhiány lelassítják az erőfeszítéseket. Válaszút előtt állunk. Mindez kihatással lesz a jövőnkre. Három terület különösen megérdemli a figyelmünket.

Béke és kollektív biztonság

Az első probléma a béke és a kollektív biztonság kérdése. Ennek a számnak több cikke is mutatja, hogy a fenyegetettség mennyire is dominálja a jelenlegi vitákat. Különösen az Egyesült Államok irányvonala az, amelyet a vita és eszközök eszkaládólása jellemez, amelynek egyik motorja a Kína elleni versengés. A kínai kormány törvényes úton vagy illegálisan, minden információt összegyűjt, legyen az informatikai, ipari, gazdasági, politikai vagy hadászati. Ennek a stratégiának célja, hogy információs erőfölényt szerezzen az Egyesült Államokkal szemben, amely riasztó aggodalmat kelt a tengerentúlon.

Az előző két év folyamán a média rengeteg titkot tárt fel, szakértők kijelentéseket tettek, kongresszustagok és még maga a Fehér Ház is feltárták a kiberfenyegetések kockázatait, amelyek a nemzet biztonságát és jólétét veszélyeztetik. Egyre többen vádolják nyíltan Kínát. A nemzeti hírszerzési szolgálat igazgatója, Jim Clapper egy szenátusi bizottság előtt bejelentette, hogy a kiberfenyegetés azon a ponton van, hogy veszélyesebbé válhat a nemzetbiztonság számára, mint a terrorizmus.

Az általános szövetségi megszorítások ellenére a kibervédelem költségvetése 800 millió dollárral nőtt 2013-ban. A Kiberhadviselési Parancsnokságnak[7] pedig megszabták, hogy effektíve 900 főről 4900 főre kell, hogy nőjön az elkövetkező években. A Snowden-ügy rámutatott, hogy milyen agresszív információgyűjtési politikát folytatott az Egyesült Államok, még ha ez a többi nemzettel való együttműködés és az eddigi bizalom kárára is megy. James Lewis a politikát relatívnak látja, hiszen a kínaiak és oroszok számára ez nem volt meglepetés, és emiatt nem is fogják kétségbe vonni a nemzetközi tárgyalásokat. Továbbra sem erős a bizalom és több köztisztviselő is hangoztatja, hogy „a kibertérben nincsenek barátok".

Sokak szerint az Egyesült Államok fogja kezdeményezni az első kiberháborús hadműveletet, egy kísérleti támadást, amely a kényszerítő diplomácia és a fegyveres támadás közötti harmadik utat képviseli. David Sanger feltárta a New York Times-nak, hogy a Stuxnet nevű, az izraeli titkosszolgálattal együtt kidolgozott vírus hogyan támadta meg a Natanz centrifugáit, hogy ezzel is lelassítsák Irán nukleáris programját.

Az elmúlt két év információi és a nemrég tett bejelentések arra utalnak, hogy a kiberfegyverkezési verseny elkezdődött. Több ország is prioritásává tette a kiberbiztonságuk és kiberkapacitásuk növelését és fejlesztését. Franciaország és az Egyesült Királyság kijelentették 2013-ban, hogy offenzív kapacitásaikat növelni fogják. 2011-ben az Egyesült Államok, illetve 2013-ban Franciaország azt nyilatkozta, hogy egy nagy volumenű kibertámadás akár háborús tettnek is minősülhet, és fenntartják a jogot, hogy visszavágjanak. Az oroszok bírálják a kibertér militarizálását, miközben ők maguk is fejlesztik saját kapacitásukat.

7 A kiberműveletek és a NSA katonai egysége

Martin Libicki, a RAND vállalat kutatója és a kibertérbeli elrettentés úttörője cikkében arról írt, hogy a konfliktusok milyen szinten eszkalálódhatnak, ha a kibertámadásokra konvencionális módon válaszolunk. Véleménye szerint a károk kisebbek maradnak, ha a kibertérben zajlanak le, ami emiatt nyílván kevésbé elrettentő is. Oriane Barat-Ginies, nemzetközi jogi doktor ellenben a Tallinni Kézikönyvet író szakértők érveit hozza fel. Ez a kézikönyv különböző jogi javaslatok gyűjteménye, ami azt fejti ki, hogy a nemzetközi jog hogyan használható fel a kibertérben. E gyűjtemény szerint a jogszerű védekezés és konvencionális fegyverek használata kibertámadás esetén megengedett, hiszen az utóbbi fegyveres agressziónak minősül.

Az eszkalálódás kockázatát komolyan kell vennünk. Ahogy ezt a két cikk is mutatja, nincs semmilyen garancia arra, hogy egy, a kibertérben elkezdett konfliktus a kibertérben fog maradni. Nem ismerjük eléggé a kiberfegyverek járulékos veszteségét sem. Az amerikai köztisztviselők pedig bejelentették, hogy akár pontos csapásokat is indíthatnak a kibertérben, ami elég aggasztó.

Ebben a kontextusban a hidegháborúval való összevetések megsokszorozódnak. A *Foreign Policy*ban David Rothkopf még a *hűvös* háború ötletét is felveti, ami egy kicsit langyosabb és szerteágazóbb, mint a hidegháború: „A *hűvös* háború célja az, hogy folyamatosan tudjunk csapásokat mérni anélkül, hogy élesben folyna háború. Mindezzel kevésbé kívánatossá, sőt szükségtelenné teszi a forró háborút" [Rothkopf, 2013].

Vissza kell-e állítani a hidegháborús (vagy *hűvös* háborús) szövetségeket? Szabad-e továbbra is a nemzetközi kapcsolatok pesszimista jövőképében gondolkodnunk és nulla-összegű játéknak tekintenünk azt? Vagy ez egy lehetőség arra, hogy a kollektív biztonság keretein belül gondolkozzunk, ezzel belevonva a folyamatba olyan országokat, mint Kína és Oroszország? Eme két ország hajlandó együttműködni a nemzetközi szabályozások létrehozásában, még ha nagy nézőpontbeli különbségek is vannak, ahogy azt James Lewis is megemlítette. Martin Libicki cikke rámutatott, hogy stratégiai megfontolásokra lesz szükség ahhoz, hogy az eszkalálódást megelőzzük. A vita még távol áll a megoldástól.

A másik kérdés az, hogy a kollektív biztonság érdekében mégis milyen keretrendszert építünk ki. A közös európai biztonság- és védelmi politika létrehozása már nehéz volt, és a kibervédelemi politika meghatározása még

nehezebb. A kapacitások megosztása a szuverenitás elhagyásának tűnhet, mert a technológia az az érzékeny pont, amely egy állam erősségeit és gyengeségeit tárhatja fel. Jean-Loup Samaan és Vincent Joubert bemutatták, hogy az Európai Unió és a NATO ezeket a kérdéseket stratégiai prioritásaikba ágyazták és kezdeményező lépéseket tettek. De a szerepek és kompetenciák felosztása továbbra is tisztázatlan maradt, és jelenleg úgy tűnik, a két intézmény között alig van koordináció, és a szuverenitás béklyóin nehéz felülkerekedni. Ráadásul a szövetségesek között nagy kapacitásbeli különbségek vannak. Leginkább a fejlett technológiával rendelkező országok tulajdonítanak nagy fontosságot a nemzeti szuverenitásnak és ápolják kétoldalú kapcsolataikat ezen a területen, főleg az Egyesült Államokkal.

A transzatlanti vitát tovább bonyolítják a gazdasági kérdések. A Snowden-ügy fényt vetett arra, hogy az európai országok adataik kezelésében menynyire függnek a nagy amerikai vállalatoktól. Ezek az adatok így nyílván az Egyesült Államok kormányának is a fennhatósága alá kerülnek. Ugyanezt a függést vehetjük észre az eszközök esetében, amelynek fő alternatívája a szintén problematikus kínai eszközök. Sokan az európaiak naivitására tapintottak rá, akik azóta megkérdőjelezik szuverenitásuk megőrzésének lehetőségét a nyitott piacokon. Lehet-e az európai kiberbiztonságot fejleszteni függetlenül a kibervédelemtől? Mit tehet Európa a rendeleteken, technikai szabványokon és iparpolitikán keresztül a kiberbiztonság javítása érdekében? Milyen alternatíva létezik a kínai és amerikai felszerelésekre és eszközökre? A belföldi piacok túl korlátozottnak tűnnek ahhoz, hogy valóban versenyképesek maradjanak. Akkor hogyan tudjuk az államok közötti bizalmat növelni, közös politikai és ipari megoldásokat találni?

Ezek sürgető kérdések, mert a biztonsági fenyegetésen kívül, a digitális adatok halmaza nő és még nőni fog. Hogyan védjük meg őket? És kitől?

A demokrácia és az egyéni szabadságjogok

Egyre több személyes adat lesz elérhető az interneten, többé-kevésbé nyíltan. Az OPEN DATA-val (nyílt adatok) közadatok, az adminisztráció adatai elérhetők lesznek, új információs eszközöket és olyan átláthatóságot nyújtva,

amely a demokrácia működését javíthatná. Remélhetjük, hogy különösen Franciaország, ahol a publikus adatok kommunikációja még messze sem tökéletes, előnyben részesíti majd a nyitottság ezen mozgalmát. Azonban, a személyes adatok kriminális vagy véletlen jellegű közzététele felveti a nagyvállalatok és a kormányok belépésének a kérdését.

Ha van legalább egy dolog, amelyben mindenki egyetért Edward Snowden esetén az az, hogy elindított egy vitát, amelyre különben nem lett volna alkalom. Az informátorok, akik előzőleg megpróbálták felhívni a figyelmet az NBÜ tevékenységére, nem kaptak nagy visszhangot. Szükség volt egy világszintű eseményre azért, hogy a nagyközönség rádöbbenjen és politikai kérdéssé tegye ezt az ügyet. A 2001. szeptember 11-i terrortámadások már nem elegendőek a vita elleplezésére. A kérdés az lett, hogy hogyan lehet kibékíteni a demokráciát és a megfigyelést.

A demokratikus ellenőrzés folyamata ebben a témában a polgárok nagytöbbsége között ismeretlen – sőt még a képviselők esetében is – és láthatólag az Egyesült Államokban, a nagyon behatárolt procedúrák ellenére is (legalábbis papíron) diszfunkcionálisak. Ádáz jogi viták folynak arról, hogy a kormány túllépte a saját jogkörét és eltaposса az állampolgárok civil jogait. Még ha úgy tűnik, a beletörődés magával sodorta a francia reakciókat, a német közvélemény felbolydult. A Stasi emléke nem is olyan távoli… A titkokat gyakran követeli a hírszerzés azért, hogy megőrizzék a nyomozások hatékonyságát, azonban jelenlegi társadalmunkban egyre nehezebb megőrizni ezeket az információkat, még a kormány számára is. Snowdennek valószínűleg még sok versenytársa lesz.

A biztosítékok, a fékek és ellensúlyok (ki, mikor, hol és hogyan?), a megfigyelések kiértékelései (amit közpénzből fizetünk) nemcsak arra jók, hogy egyéni szabadságjogainkat és a demokrácia eszméit megőrizzük, hanem a megfigyelés törvényességét is megszabjuk.

A tét nagy horderejű. Az egészségügyi kartonunk, a politikai véleményünk, az iskolai eredményeink, a szexuális orientációnk, vásárlásaink, utazásaink, barátaink, barátaink barátai, a barátaink barátainak a barátai… Az összes információ és még több más nyomozás, egyeztetés tárgyát képezhetik, és egy ijesztően pontos profil kialakítása válik lehetővé. Sok információ ma már

elérhető és gyakran önszántukból adják ki a közösségi oldalak és blogok felhasználói.

A biztosítékok kérdése felvetődik a nagyvállalatok esetében is, amelyek nincsenek alávetve a demokratikus ellenőrzésnek, csak a törvényeknek és a kormányukkal való erőltetett együttműködésnek. Érdemes még megemlíteni, hogy az adatok kiaknázásából származó előnyök, amelyek elemzik az ízléseinket, memorizálják a választásainkat és testreszabott szolgáltatásokat javasolnak számunkra, sokszor a szabadságjogaink megsértésének kompromisszumával jár.

Ezek a viták hatalmas gazdasági problémákat tárnak fel. Stéphane Grumbach és Stéphane Frénot, az INRIA kutatóinak cikke megmutatja, hogy az adatok összegyűjtésének, keresztezésének, elemzésének és kiaknázásának képessége társadalmaink gazdasági motorjává vált. A nyílt-adatok piacán tagadhatatlan stratégiai előnyt jelent az amerikai vállalatoknak az online szolgáltatásokban elért dominanciájuk, amelyhez hozzákapcsolódik az adatfeldolgozás szakértelme, a technológiai know-how. Másrészt a szuverenitás kérdései és a Snowden-ügy tovább komplikálhatja a kereskedelmi megállapodásokról folyó tárgyalásokat. Ezeket mégsem fogjuk lényegesen megkérdőjelezni. A döntés az európaiak kezében van, akik – ellentétben néhány feltörekvő piaccal –, nem lettek internetes bajnokok.

Ezen kívül még felvetődik, hogy az európai tagállamok képesek-e politikai és gazdasági befolyást kovácsolni az internet óriásaival szemben. A személyes adatok védelmének reformja lehetővé tenné a mozaikszerű európai nemzeti törvénykezés harmonizálását, elősegítené a vállalatok mobilitását Európában, illetve megerősítené az állampolgárok jogainak védelmét. A törvény a személyes adatokat gyűjtő cégeket kötelezné, hogy azokat csak a felhasználók beleegyezésével gyűjtsék; megengedné a lehetőséget, hogy az adatokat törölni lehessen; illetve létrehozna egy ügynökséget, amely a pereket kezelné. A Snowden-ügy dacára a törvényjavaslat 2015-ben el lett napolva, amiért az amerikai nagyvállalatok különösen masszív lobbiját és a tagállamok komoly nézeteltéréseit okolhatjuk. A lehetőség széles tárháza áll előttünk…

Az internet jövője

Végezetül a nemzeti stratégiák is hozzájárulnak az internet kialakításához, amelyek szintén fontos kihívások. Dilma Rousseff, Brazília államfője a maszszív ellenőrzésről szóló információk feltárását követően (mobiltelefonját ideértve) kifejezte azon kívánságát, hogy leváljon a túlságosan amerikaissá vált (USA centrikus) internetről és egy, 2014 áprilisában tartandó csúcstalálkozó megrendezését javasolta az internet szabályozásáról Brazíliában. Bertrand de La Chapelle interjújában megemlíti ezt is mint kihívást. Ebert Mannes és Tim Maurer bemutatják, hogy a feltörekvő országok, ahol a netfelhasználók száma rohamosan növekszik, rosszul élik meg az amerikai fölényt, amely az internet architektúrájában, irányításában, a felszerelésekben, a szolgáltatásokban, a tartalomban és az adatok kezelésében lévő dominanciát takarja. Ezért saját befolyásukat növelő stratégiát fejlesztenek ki. A BRICS körülbelül húsz afrikai országgal van partneri kapcsolatban, és egy 32000 km hosszú tengeralatti kábel projektet indítottak el, amely összekötné Oroszországot, Kínát, Indiát, Dél-Afrikát, Brazíliát (BRICS) és az Egyesült Államokat. Ugyanakkor a BRICS-országok nem képeznek egy homogén csoportot és nem ugyanazokkal a demokratikus hagyományokkal rendelkeznek, mint ahogy Hannes Ebert és Tim Maurer cikke is mutatja.

Számos demokratikus állam aggódik az „internet balkanizációja" miatt. A hálózat fizikai és politikai szétaprózódása, kezdeti sikerének, szabad és nyílt szellemének elvesztését jelentené. Kína, Oroszország, Irán, Szaúd-Arábia, Észak-Korea stratégiákat alakítottak ki a hálózatuk ellenőrzésére, a fizikai infrastruktúrától a tartalom forgalmáig. Kevin Limonier cikke nagyon jól bemutatja az Oroszország által készített ábrákat és stratégiákat, amelyekkel megvédi a szuverén internet koncepcióját. A Telekommunikáció Nemzetközi Szövetségének berkeiben ezen országok az állami ellenőrzésű internet fejlesztését javasolják. Bertrand de La Chapelle szerint a nemzetközi tárgyalások rendszeresen két kritikus ponton akadnak el: a nyugati államok előrébb teszik az emberi szabadságjogok tiszteletét (szólásszabadság, információhoz jutás, a magánélet tiszteletben tartása), illetve a nem állami szereplők bevonását egy többszereplős kormányzási modellbe, míg Kína, Oroszország és más államok számára e kérdések kizárólag az államok szuverenitását illetik.

Az összekapcsolt gazdasági és politikai érdekeknek elég erősnek kell maradniuk, hogy az eddigi közös alapstruktúra ne legyen kérdéses.

Az NBÜ programjáról szóló titkos információk, az olyan feltörekvő demokratikus országok felemelkedése, mint Brazília és India, és az Icann erőfeszítései, hogy figyelembe vegyék a regionális követeléseket, már mozgatják a szálakat. Tét az internet jövője. Hogyan lehet helyet csinálni minden nemzet számára és kialakítani egy elegendően biztonságos környezetet, mindezzel megtartva a hálózatok szabad és nyitott mivoltát?

Zárószó

A kibertér egy időben vált a szereplők közötti hatalmi versengés kérdésévé, az összeütközés színterévé és a geopolitikai konfliktusok kegyetlen fegyverévé. A kibertérért és a kibertérben folyó harcok nem különíthetők el a klasszikus geopolitikai hatalmi versengéstől. Ezek ellenben egy új módja és dimenziója a geopolitikának, amely minden szinten és több skálán van jelen.

A kibertér geopolitikai kihívásai diszkréten keveredtek a politikai, gazdasági, szociális és kulturális meggondolásokkal. A többlépcsős és transzdiszciplináris jellege megnyitja az informatika, sőt még a matematika előtt is, és ezzel lehetővé teszi a geopolitika kérdéseinek elemzését egész komplexitásukban.

A viták technikai dimenziója kétségtelenül különös erőfeszítést igényel az olvasó számára. De megéri a fáradtságot. Mivel nemcsak a kibertér hatalmi és biztonsági kérdéseiről van szó, hanem azon értékekről is, amelyeket mint demokratikus nemzet megvédünk. Olyan értékek, amelyek szeretnénk, ha irányítanák az általunk épített világot.

Felhasznált irodalom

CATTARUZZA A. et DOUZET F. (2013), « Le cyberespace au cœur de tensions géopolitiques internationales», DSI, hors-série n°32.

DESFORGES A. (2013), « Les frontières du cyberspace», in DOUZET F. et GlBLIN B. (dir.), Des frontières indépassables?, Armand Colin. Paris.

DOSSÉ S. (2010), «Vers une stratégie de milieu pour préparer les conflits dans le cyberes¬pace? », DSI, n°59. mai.

DOUZET F. (1997), « Internet géopolitise le monde », Hérodote, n° 86/87. p. 222-233.

–, (2007), «Les frontières chinoises de l'Internet», Hérodote, n° 125, p. 127-142.

L'Internet Corporation for Assigned Nantes and Numbers (Icann) est l'organisation qui coordonne le système d'addresses Internet et de noms de domaine (<www.icann.org>).

–, (2013), «Chine. États-Unis: la course aux cyberarmes a commencé». Sécurité globale, n°23.

–, (2013), «Chine: cyberstratégie, l'art de la guerre revisité». Diploweb, 12 septembre (<www.diploweb.com>)

GIBSON W. (1984), Neuromancer, Ace, New Jersey.

KE\1 PF O. (2012), Introduction à la cyberestratégie, Economica, Paris.

LACOSTE Y. (dir.) (1993), Dictionnaire de géopolitique, Flammarion, Paris.

LACOSTE Y. (2003), De la géopolitique aux paysages, dictionnaire de la géographie, Armand Colin, Paris.

MATTELART A. (2009), Histoire de l'utopie planétaire. De la cité prophétique à la société globale, La Découverte, Paris.

MCLUHAN M. (1964), Understanding Media. The Extensions of a Man, McGraw-Hill. New York.

MUSSO P. (2003), Critique des réseaux, PUF, Paris.

ROTHKOPF D. (2013), «The cool war», Foreign Policy, 20 février.

SANGER D. (2013), « In cyberspace, new cold war», New York Times, 24 février.

VlRlLlO P. (1997), « Un monde surexposé », Le Monde diplomatique, août.

DR. DORNFELD LÁSZLÓ*

(dlaci120@gmail.com)

A kibertér főbb nemzetközi és nemzeti szabályozásai

Lektorálta: ERDŐS ANDRÉ

* A szerző a Miskolci Egyetem Állam és Jogtudományi Karának I. évfolyamos doktorandusza, témavezetője Dr. habil. Róth Erika egyetemi docens

Absztrakt

A kibetérben található fenyegetések elleni fellépés mind állami, mind nemzetközi szinten egyre erősödik. Az egyes szereplők egyre szervezettebb formában igyekeznek fellépni a bűnözők ellen, gyakran egymást segítve. Az eredményes együttműködést nehezíti azonban az, hogy az érintett felek eltérő szabályozási rendszerek megvalósulásában érdekeltek, amely kibertérrel kapcsolatos politikájuk fontos részét képezi. A két fő modell az Egyesült Államok és az Európai Unió által támogatott több érdekelt fél bevonásával történő, és a Kína és Oroszország által pártolt nemzeti szuverenitáson alapuló multilaterális szabályozás. A tanulmány célja, hogy feltárja az ezek között húzódó különbségek okait és a szabályozások fontosabb fejlődési irányait.

Kulcsszavak: kibertér: kiberbűnözés, szabályozás

Abstract

The willingness of countering threats that are present in cyberspace is growing both on national and on international levels. The actors are trying to step up more organically against the involved criminals, often cooperating with each other. However there is an obstacle in the way of successful international cooperation – the actors are interested in implementing different types of legal regimes which is an integral part of their individual policies. The two main models are the multi-stakeholder approach supported by the US and the EU and the regime based on national sovereignty promoted by China and Russia. The main goal of this study is to unfold what are the causes of this difference and to give a review over the most important tendencies of the evolution of the legal regimes.

Keywords: cyberspace, cybercrime, regulation

Bevezetés

Mikor az internet még csak a hadsereg számára elérhető technológiaként létezett, nem volt szükség szabályozás kidolgozására a területen. A jogellenes használatuktól való félelem még akkor is igen jelentéktelen volt, amikor a hálózatok többségét nagy cégek működtették. Azonban ahogy a civil szektor és a lakosság számára is széles körben hozzáférhetővé vált a technológia, a helyzet gyökeresen megváltozott. Az e-kereskedelemben új szabályozás vált szükségessé, az államok működését pedig az e-közigazgatás kiépítése tette gördülékenyebbé. A felhasználók számának növekedésével a kiberbűnözés jelentette fenyegetés is jelentősen megnőtt. Hamarosan a hadseregekben is felismerték, hogy az internet segítségével emberveszteség nélkül okozhatnak súlyos károkat az ellenségnek, és ennek elérésére hamarosan az egyszerű polgárok is képessé váltak, mint mutatja azt például az Észtország internetes infrastruktúrája elleni oroszpárti hackertámadás 2007 áprilisában. (Jensen, 2015, p. 276.)

A kibertér információbiztonságát érő összes jelentősebb eddigi fenyegetés nemzetközi vonatkozásokkal rendelkezett. Az államok egyre inkább felismerték, hogy egyedül nem képesek gátat szabni ennek az új jelenségnek. Éppen ezért – bírjanak bármilyen felfogással is a kiberteret illetően – a nemzetközi együttműködés szükségessége vitathatatlanná vált. (Zhang, 2013, p. 123.) Ebből a körülményből következik, hogy a kibertérrel kapcsolatos szabályozási modellek nemzetközi érvényesítésére az államok egyre nagyobb hangsúlyt helyeznek. A jelentősebb szereplők nemzeti szinten az Egyesült Államok, Kína és Oroszország, míg szupranacionális és nemzetközi szinten az Európai Unió és az ENSZ.

A jelenlegi szabályozásban fontos szerep jut még az iparban érdekelt nagy multinacionális cégeknek (pl. Google, Apple, Microsoft), amelyek saját szabályaik szerint járnak el számos kérdésben, így például egyes – akár politikai – tartalmak eltávolításáról saját belátásuk szerint döntenek. Sokan kritizálták a Facebookot, amikor idén májusban egy volt alkalmazottjuk a sajtónak arról nyilatkozott, hogy a népszerű hírek kiválasztásánál a szerkesztőcsapat tudatosan mellőzte a konzervatív honlapokat. (Lakner, 2016) Ez jól mutatja, hogy a nagy cégek milyen jelentős befolyással lehetnek a szolgáltatásaikat használók véleményének formálására. Mivel az alapvető jogok – így a szólásszabadság

is – csak az állam és az egyén kapcsolatában értelmezhetők, az államihoz hasonló jogosultságokat gyakorló cégek korlátozás nélkül dönthetnek tartalmak sorsáról.

Az egyes szabályozási modellek számos kisebb-nagyobb jelentőségű kérdésben eltérnek egymástól, mint például a szolgáltatók szerepe és bevonása, a jogsértő tartalom kiszűrésének a módszerei, az interneten folyó kommunikáció ellenőrzése stb. Ezek mindegyikét lehetetlen lenne ennek a tanulmánynak a keretei között tárgyalni, ezért a főbb irányvonalakra és kérdésekre fogok a következőkben koncentrálni. Célom, hogy bemutassam a világon található jelentősebb szabályozási megoldásokat, és ezek fejlődési tendenciáit.

1. Egyesült Nemzetek Szervezete

Az ENSZ kiberteret érintő szabályozásának kidolgozásával a Közgyűlés több határozatban is foglalkozott. Az 1998-ban Oroszország javaslatára elfogadott 53/70. sz. közgyűlési határozat a kiberteret érő új fenyegetésekkel kapcsolatban fogalmazott meg ajánlást a tagállamok számára. 2006-ban a 60/45. sz. határozat a főtitkár számára egy nemzetközi, kormányzati szakértőből álló csapat összehívását írta elő, amelynek feladata volt jelentést készíteni az információbiztonságot fenyegető létező és potenciális veszélyekről. A jelentés 2010-re készült el. Fontos szerepet tölt be a szabályozásban a Nemzetközi Távközlési Egyesület (ITU), amelynek 191 tagállama és 700-nál is több ágazati tagja van (köztük például az Európai Bizottság), működési területét pedig gyors ütemben terjeszti ki az internetre is. (Sofaer – Clark – Diffie, 2010, pp. 187–188.) 1988-ban Melbourne-ben a Távíró- és Telefonszolgáltatók Világkonferenciáján (WATTC-88) fogadták el a nemzetközi távközlési szabályozást (International Telecommunication Regulations, ITR), amely azóta sem változott. A szabályozás célja a határokon átnyúló telekommunikációs forgalmat biztosító rendszerek együttműködő képességének (interoperabilitás) és összekapcsolódásának megkönnyítése. Többek között olyan kérdéseket érint, mint a díjazás és számvitel, felelősség vagy adóztatás. Ugyanakkor olyan időszakban született, amikor az internetszolgáltatók jelentős része állami tulajdonban volt, és mára

időszerűvé vált felváltása és szabályainak az új kihívásokhoz való igazítása. (Internet Society, 2011)

2003-ban és 2005-ben Genfben és Tuniszban a szervezet megtartotta az Információs Társadalom Világcsúcsát (World Summit on the Information Society, WSIS), amelyen a tagállamok amellett foglaltak állást, hogy a szervezet legyen a fellépés vezetője az új információs és kommunikációs technológiák biztonsága, és az ezek iránti bizalom kiépítésében. Számos egyeztetést követően ezen cél elérése érdekében 2007. május 17-én létrehozták a Globális Kiberbiztonsági Menetrendet (*Global Cybersecurity Agenda*, GCA), amelynek célja, hogy keretet biztosítson a kiberteret fenyegető növekvő fenyegetés elleni nemzetközi fellépés koordinálásához. A GCA fontosnak tartja, hogy minden érdekelt fél egyesített erőfeszítése révén valósuljanak meg célkitűzései. (Sofaer – Clark – Diffie, 2010, p. 186–187.) Az Egyesült Államok Kormányzati Ellenőrzési Hivatalának 2010. júliusi jelentése rámutat, hogy egyetlen központi szereppel bíró szerv híján a kiberbiztonságban résztvevő nemzetközi szervezetek nagy száma akadályozhatja a nemzetközi koordinációt. A jelentés rámutat, hogy a hálózatbiztonsági vészhelyzeteket elhárító csoportokkal (*Computer Emergency Response Team*, CERT) való állami együttműködés számos nehézséggel bír, és a szervezetek egy része – mint például az ENSZ által létrehozott Globális Reagálóközpont (Global Response Center) – nem képes arra, hogy minden résztvevő előnyére szolgáló, legitimitással bíró globális biztonsági szolgáltatást nyújtson. (Sofaer – Clark – Diffie, 2010, p. 186.)

2011 szeptemberében Kína, Oroszország, Kazahsztán, Kirgizisztán, Tádzsikisztán és Üzbegisztán javaslatot terjesztettek az ENSZ Közgyűlés elé a kiberbiztonság megteremtése érdekében, amelyben hangsúlyos szerepet kapott a nemzeti szuverenitás részét képező kiberszuverenitás, vagyis a kormányok azon joga, hogy határaikon belül korlátok nélkül ellenőrizhessék az adatforgalmat. (Jong-chen, 2015) Ezen országok képviselői közös levélben kérték az ENSZ főtitkárát, hogy a sanghaji együttműködés részeként elfogadott nemzetközi magatartási kódexet a Közgyűlés 66. ülésszakán hivatalos dokumentumként terjessze a megjelentek között. (Zhang 2013, p. 126.) Változtatásokat követően Oroszország és Kína 2015 januárjában ismét benyújtotta a magatartási kódexet a főtitkárnak, ami jól mutatja, hogy nem tettek le annak nemzetközi elfogadtatásának szándékáról. (Grisby, 2015)

2012-ben a Dubajban tartott nemzetközi távközlési világkonferencián (WCIT) Oroszország, Kína, Brazília és India olyan javaslattal álltak elő, ami jóval nagyobb szerepet szánt volna az internet szabályozásában az ITU-nak. A kibertér szabályozásában a nemzeti szuverenitás elvét valló országok részéről ez azért különösen lényeges, hiszen így végső soron az államok jutnak szélesebb beleszólási lehetőséghez. (Eichensehr, 2015, p. 331.) Az Egyesült Államok élesen ellenezte a javaslatot, azon az alapon, hogy abban csak vertikális módú irányítás valósulna meg, és a többi érdekelt fél nem kerülne bevonásra. Mások azt emelték ki, hogy ezzel a világpolitikai érdekeknek rendelnék alá egy nagyon gyorsan fejlődő technikai terület szabályozását, amely megbénítaná a döntéseket. Megint mások a beterjesztő országokban működő, szabad információáramlást korlátozó internetszabályozás alapján fogalmaztak meg kritikát. (Sasso 2012; Rosenzweig 2012, p. 414.)

Oroszország javaslata az internetet egyértelműen az ITU szabályozása alá rendeli, és egyúttal a domainnevek kiosztását felügyelő ICANN nem kormányzati szervezet pozícióját is gyengíti. A javaslat ugyanis egyenlő jogokat biztosított volna ezen a területen a tagállamoknak. A világkonferencia eredménye felemás volt: egyrészt az Egyesült Államok és szövetségesei sikerrel akadályozták meg az ITU vagy az ENSZ domainnevek elosztásába történő bevonását, és a szerződésbe belefoglaltattak egy nyilatkozatot, amely szerint annak hatálya nem terjed ki a tartalomszabályozás kérdéseire. Másrészt azonban elfogadásra került az orosz javaslat módosított változata, és ezt a határozatot az egyezményhez csatolták. Eszerint „minden kormányzatnak egyenlő szerepet és felelősséget kell biztosítani a nemzetközi internetszabályozásban", ami igen távol áll a nyugati küldöttségek által szorgalmazott minden érdekelt bevonásával működő modelltől. Összesen nyolcvankilenc ország – köztük Oroszország, Kína, Dél-Afrika, számos afrikai és arab ország – írta alá az új egyezményt, míg az Egyesült Államok, az EU tagállamok, Kanada, Ausztrália, Új-Zéland és India nem. (Eichensehr, 2015, pp. 333–335.)

Az amerikai küldöttség vezetője, Terry Kramer nagykövet öt indokot nevezett meg az elutasítás okaként. Az első, hogy a javaslat a közreműködő ügynökség (*operating agencies*) helyett az elismert közreműködő ügynökség (*recognized operating agencies*) kifejezést használta. Az első megnevezés a hagyományos telekommunikációs közszolgáltatásokat nyújtókat jelöli, amely-

be nem tartoznak bele az internetszolgáltatók, a magán- és kormányzati hálózatok. Az amerikai vélekedés szerint amennyiben ezekre is kiterjed az egyezmény, úgy az internet állandó figyelés alá vehető. A második ok a spamek tilalma, amely az amerikai álláspont alapján a kifejezés egyik formája, ezért a véleményszabadság védelme alá tartozik. A harmadik ok a hálózatbiztonsági kérdések felvetése, amely a nagykövet szerint nem az ITR szabályozási körébe tartozó kérdés. Kifejtette továbbá, hogy egyetlen kormányzat vagy nemzetközi szervezet sem irányíthatja az internetet és dönthet annak fejlődési irányáról, így az ENSZ sem. Utolsóként azt említette, hogy bár az előzetes megbeszélések során Hamadoun Touré biztosította arról, hogy internettel kapcsolatos kérdések nem lesznek a megbeszélésen, ezek mégis előkerültek. Kramer szerint ugyan az amerikai küldöttség jóhiszeműen próbált hozzáállni ezekhez, a többi küldöttség által tett, oda nem illő javaslatok alaposan megváltoztatták a megbeszélés jellegét. (Popescu, 2012)

2014-ben a dél-koreai Puszanban tartott Meghatalmazotti Konferencián szintén több internettel kapcsolatos javaslat került benyújtásra. Például Oroszország javasolta, hogy az ITU kezdje meg az IP-címek kiosztását, amelyet jelenleg nem kormányközi szervezetek végeznek, az arab államok pedig a kormányok internetre vonatkozó döntési lehetőségét növelték volna. India javaslata a belföldi internetforgalmat az államhatárokon belül tartotta volna, így az azon túli címek eléréséhez külön csatlakozásra lett volna szükség. (Dickinson 2014) Az Egyesült Államok és partnerei azonban sikeresen megakadályozták ezek mindegyikének elfogadását, így a status quo fennmaradt.

Ebben az évben Zhao Houlin, egy kínai állampolgár lett az ITU új főtitkára, aki korábban hét évig a szervezet főtitkárhelyetteseként tevékenykedett. Az ő irányítása alatt jelentősen megváltozott a megbeszélések hangneme a szervezet 2015-ös világkonferenciáján, amely már korántsem olyan konfrontatív, mint 2012-ben volt. Ezzel sikeresen kivívta az amerikaiak dicséretét is. (Austin, 2016, p. 174)

2. Egyesült Államok

2.1. Az amerikai szabályozás

Az Egyesült Államok kétféle módon közelít a kiberbiztonság kérdéséhez: egyrészt nemzeti érdekei védelmében saját belső védelmét megerősítette új törvények elfogadásával és betartatásával, másrészt nem amerikai állampolgárok és más államok esetén jelentős lépéseket tesz az információk gyűjtésére. Ez utóbbi akkor derült ki, mikor Edward Snowden 2013-ban nyilvánosságra hozta az NSA működésével és feladatával kapcsolatos adatokat. (Zhang 2013, p. 121.) A biztonságpolitikai szakértők azt javasolják, hogy a nemzeti jogszabályok segítsék elő a támadásokról szóló információk megosztását, az állami szervek működjenek együtt a magánszektorral, valamit államilag támogatott kutatások segítségével építsenek ki gyors és effektív védelmet a kibertámadások ellen. Ugyanakkor ezek a módszerek hatástalanok olyan esetekben, amikor a támadók olyan külföldi országból származtak, amelyben az USA nem tudja a jogszabályait érvényre juttatni. (Sofaer – Clark – Diffie, 2010, p. 184.)

Az USA elsők között ismerte fel a kibertér fenyegetései elleni állami fellépés szükségességét. A későbbi számítógépes csalással és visszaéléssel foglalkozó törvény (*Computer Fraud and Abuse Act*, a továbbiakban CFAA) előkészítése már 1976-tól elkezdődött, és a Kongresszus 1984-ben fogadta el, ekkor még egy másik törvény részeként. Az elkövetkező két évtizedben nyolc alkalommal módosították a jogszabályt, amelyek fokozatosan kiterjesztették hatályát. Míg kezdetben csak a „szövetségi érdekeltségű" számítógépek elleni támadást büntették, a 2008-as módosítás eljutott oda, hogy a világ összes számítógépét a szabályozás alá vonja. (Dornfeld 2015, pp. 69–71.) Ezt számos egyéb szabályozás is követte, mint például az információszabadságról (*Freedom of Information Act*), a számítógépes biztonságról (*Computer Security Act*), a gyermekek online magánéletének védelméről (*Children's Online Privacy Protection Act*), a biztonságos közhálózatokról (*Secure Public Networks Act*), a titkosított kommunikációról (*Encrypted Communications Privacy Act*), a telefonos vásárlók védelméről (*Telephone Consumer Protection Act*) stb. szóló törvények. Ennek a jelentős méretű joganyagnak köszönhetően az Egyesült Államok szabályozása az egyik legrészletesebben kimunkált a világon.

A törvényeken kívül számos elnöki rendelet is született, egyes fontos kérdések szabályozásával kapcsolatban. 2011-et követően sok vita folyt az amerikai törvényhozásban a kritikus infrastruktúra védelmét illetően, amelyek azonban nem vezettek eredményre. Végül 2013. február 12-én Obama elnök, egy amerikai erőmű leállását eredményező kibertámadást követően kiadta a kritikus infrastruktúra kibervédelmének javításáról szóló 13636. számú elnöki rendeletet, amelyben a Nemzeti Szabványügyi és Technológiai Intézetet (*National Institute for Standards and Technology*, NIST) bízta meg a kritikus infrastruktúra többségét birtokló magánszektorral való együttműködés részleteinek kialakításával. (Wiley Rein, 2013; White House, 2013) 2015. április 1-jén született meg a 13694. számú elnöki rendelet, amely olyan természetes és jogi személyekkel szemben teszi lehetővé pénzügyi szankciók alkalmazását, akik súlyos nemzetbiztonsági kockázatot jelentő kibertevékenységekben vesznek részt, kereskedelmi titkokat szivárogtatnak ki vagy ezekben bármilyen segítséget nyújtanak. Feltétel, hogy ezen elkövetők teljesen vagy jelentősen az Egyesült Államok területén kívül működjenek. Bár a rendelet nem mondja ki, elsődlegesen a Kínából és Oroszországból érkező – amerikai feltételezések szerint államilag támogatott – támadásokra adott válaszlépésként értelmezhető, főleg, mivel ezeknek az államoknak nincs kiadatási egyezményük az USA-val.

Az internetsemlegesség – melynek általános kérdéseit az EU-val foglalkozó fejezetben részletezem – fontos szabályozási kérdésként merült fel, és Barack Obama választási programja részévé is tette az elképzelést. 2002-ben a Szövetségi Távközlési Bizottság (*Federal Communications Commission,* FCC) úgy döntött, hogy az internetszolgáltatók nem telekommunikációs szolgáltatást nyújtanak, így nem is vonatkoznak rájuk a telekommunikációs törvényben a közös szállítókkal kapcsolatban megfogalmazott kötelező szabályok. A 2005-ben kiadott internetes szabályozási nyilatkozatban négy internetszabadsági alapelv került meghatározásra. Ez a felhasználók jogait tartalmazza, így: a törvénybe nem ütköző tartalmakhoz való szabad hozzáférés, a választásuk szerinti alkalmazások futtatása, az eszközeik közötti összeköttetés, valamint a szolgáltatók közötti verseny. (Walthall, 2010, pp. 21–22.) Az ezt követő években az FCC kiállt az internetsemlegesség mellett. Miután 2007-ben kiderült, hogy a Comcast internetszolgáltató megakadályozza vagy jelentősen

lassítja a BitTorrent feltöltéseket, a szervezet 2009 októberében törvényalkotási javaslattal állt elő az ilyen gyakorlat megakadályozása érdekében. Ennek folytatásaként 2010 decemberében kiadták az internet szabadságának megőrzéséről szóló utasítást, amely kompromisszumos megoldásként továbbra is engedélyezte a forgalomirányítási technikák használatát, ha azok nem valósítanak meg megkülönböztetést, illetve blokkolást vagy feltorlódást. (Null, 2011, pp. 461–462.) A Verizon azonban megtámadta a döntést, és a Szövetségi Fellebbviteli Bíróság 2014. január 14-én megszületett ítéletében (740 F.3d 623 (D.C. Cir. 2014)) úgy határozott, hogy az FCC-nek nincs hatásköre a szabályozás meghozatalára, mivel az internetszolgáltatók nem tekinthetők közös szállítóknak. A szervezet nem támadta meg a bíróság döntését, ehelyett 2015. február 26-án olyan döntést hozott, amely mégis az 1934-es kommunikációs törvény és az 1996-os telekommunikációs törvény alá tartozónak mondta ki az internetszolgáltatókat. Az FCC ezt követően április 13-án adta ki új, a szabad internet megőrzéséről és elősegítéséről szóló utasítását. A szabályozást a szolgáltatók érdekvédelmi szervezetei megtámadták, de 2016. június 14-én a Szövetségi Fellebbviteli Bíróság ezt elutasította. Az érdekeltek azonban nem nyugodtak bele a döntésbe, így az internetsemlegességgel kapcsolatos vita várhatóan a Legfelsőbb Bíróságon és a Kongresszusban fog folytatódni. (Npr, 2016)

A bűnüldözés érdekei és az amerikai Alkotmányban (különösen annak első, negyedik és ötödik kiegészítésében) lefektetett alapvető jogok összeütközése megjelenik a kiberbűnözéssel kapcsolatos ügyekben is. Az ötödik kiegészítés tartalmazza az önvádra kötelezés tilalmát, ami azt jelenti, hogy a terhelt nem kötelezhető a saját bűnösségét alátámasztó írásbeli vagy szóbeli vallomás megtételére. A bírói gyakorlat alapján ez nem vonatkozik a tárgyi bizonyítékokra – a szolgáltatásukra már viszont igen – és az önként tett kijelentésekre, így azokra sem, amiket a terhelt az interneten tett közzé, akár nyilvános, akár zárt csoportban. Érdekes kérdésként merül fel, hogy amennyiben valaki titkosítással védi az illegális tartalmat a számítógépén, úgy az kötelezhető-e a jelszó átadására. 2007-ben Sebastian Boucher gyermekpornográfia birtoklásával kapcsolatos ügyében a szövetségi bíróság úgy ítélte meg, hogy az Alkotmány tiltásába ütközne, amennyiben a vádlottat kötelezik a kód megadására. Másabb lenne azonban egy hasonló ügy kimenetele, amennyiben a kódot a terhelt egy naplófájlba menti le. Ez ugyanis nem tekinthető vallo-

másnak, így nem esik az ötödik kiegészítés védelme alá. (Brenner, 2011, pp. 115–118.) A tartalomszabályozás terén a szövetségi kormány nem hozhat kormányszintű szabályozást, mivel az az Alkotmány első kiegészítésébe ütközne, így elsősorban az intézményi szinten megvalósuló szűrést támogatják. Ebben az esetben a felhasználóitól magasabb, de az államitól alacsonyabb szinten (pl. a munkáltató, az iskola vagy a könyvtár) döntik el, hogy mely tartalmak nem elérhetők. (Parti, 2010, p. 99.) Ez alól kivételt az obszcén tartalmak, és különösen a gyermekpornográfia jelentenek, amelyek nem élvezik az első kiegészítésben foglalt védelmet. A gyermekek online védelméről szóló 1998-as törvény (*Child Online Protection Act*) azt kívánta megakadályozni, hogy a kiskorúak számukra károsnak ítélt tartalmakhoz férjenek hozzá az interneten. A törvényt vizsgáló bíróságok megállapították, hogy a törvény korlátozásai számos ponton nem voltak megfelelőek, így például túlzottan tág fogalmakat használt, és az egyes tartalmak károsságát nem azok kontextusával együtt értelmezték. 2008-ban a 3. Fellebbviteli Bíróság ezért alkotmányellenesnek nyilvánította. (Lamut, 2008)

A szabályozás egységes érvényesülését szolgálja, hogy bár főszabályként a szövetségi kormánynak csak korlátozott bűnügyi hatásköre van, kizárólagos hatáskörrel bír a tagállamközi és államközi kereskedelemben, és így gyakorlatilag a számítógépeket és hálózatokat érintő ügyekben is. (Borisevich et al. 2012, p. 278.) Ugyan az Egyesült Államok 50 tagállamának és a fővárosnak a kiberfenyegetésekkel kapcsolatos szabályozása nagymértékben konzisztens a szövetségivel, előbbiek alkalmazása számos nehézséget okozna és áttekinthetetlen, szövevényes rendszert alkotna. (Brenner, 2011, p. 85.) A szövetségi szabályozás fontosságából következik, hogy a bírói gyakorlatnak – különösen a szövetségi Legfelsőbb Bíróság ítéleteinek – fontos szerepe van a jogszabályok értelmezésében és fejlesztésében. (Dornfeld 2015, pp. 71–73.)

Intézményi szinten elnöki bizottságot hoztak létre a kritikus infrastruktúra védelmére, amelynek feladata a kiberbiztonság irányítása és koordinálására, valamint 2008-ban létrejött az Átfogó Nemzeti Kiberbiztonsági Kezdeményezés (*Comprehensive National Cyber-security Initiative*). (Zhang 2013, p. 123.) Az USA Belbiztonsági Minisztériumán belül működik a Nemzeti Kiberbiztonsági Részleg (*National Cyber Security Division*), amely a fenyegetésekre való reagálással és a kockázatkezeléssel foglalkozik. A kibertámadások elhá-

rításáért a hadseregen belül működő Kiberparancsnokság felel. (Levin – Ilkina, 2013, p. 19.)

2.2. Kiberdiplomácia: új tényező az amerikai külpolitikában

Az Egyesült Államok külpolitikájában egyre hangsúlyosabb szerepet kap az új kiberfenyegetésekkel szembeni nemzetközi együttműködés kialakítása, valamint az internetszabályozás alapelveinek a megfogalmazása. Az ország a több érdekelt bevonásával működő (*multi-stakeholder*) rendszer elképzelését támogatja, vagyis az ipar szereplői, a civil társadalom, a tudományos élet képviselői és az egyének bevonásával megvalósuló szabályozást, amelyet alapvető fontosságúnak ítél. A megoldás támogatásában nemcsak a szabadságjogok szélesebb érvényesülése játszik közre, hanem az a tény is, hogy a számítástechnikai cégek és a működésben szerepet játszó nem kormányzati szervek – mint például az ICANN – amerikai kötődéssel bírnak. (Eichensehr, 2015, pp. 346-347.)

Az Egyesült Államok Kormányzati Ellenőrzési Hivatalának 2010. júliusi jelentése szerint akkor még nem volt egységes stratégia a nemzetközi fellépés céljait illetően, és az egységes irányítás is hiányzott, így ekkor inkább csak ad hoc kapcsolatfelvételekről lehetett beszélni. (Sofaer – Clark – Diffie, 2010, pp. 184–185.) Ez a szemlélet jól megmutatkozott az ITU nemzetközi távközlési szabályozásának (ITR) megújítása kapcsán, amelyet az Európai Unió már szükségtelennek ítélt, az Egyesült Államok azonban 2008-ban kiemelt fontosságúnak nyilvánított. A tárgyalások során képes volt érdekeit jelentős mértékben érvényesíteni, és csak az általa jónak ítélt javaslatokat megtartani, a végén azonban mégis teljes amerikai diplomáciai kudarcként került kommunikálására a folyamat, és a 2012-es egyezménytervezet megbukott. (http://www.internetgovernance.org, 2012)

2010-ben Hillary Clinton külügyminiszter beszélt a kibertér és az emberi jogok kapcsolatáról, és F. D. Roosevelt elnök hét évtizeddel korábbi kijelentését alapul véve a „kapcsolódás szabadságát" az ötödik szabadságként fogalmazta meg.[1] Élesen elítélte azokat az országokat, amelyek cenzúrázzák az

1 Az 1941. január 6-án megfogalmazott gondolat szerint négy alapszabadság illeti meg a világ minden lakosát. Ezek: szólásszabadság, vallásszabadság, a nélkülözéstől való szabadság és a félelemtől való szabadság. Az emlegetett ötödik szabadság digitális alapjogként való kezelése az ENSZ hasonló irányú törekvésével vethető össze. A 2003-as WSIS zárójelentése úgy fogalmaz, hogy mindenkinek lehetőséget kell biztosítani az információs társadalomban való részvételre. (WSIS, 2003)

internet tartalmát, és beszélt hazája aktív fellépéséről az ilyen gyakorlat ellen. (Crook, 2010) 2011-ben az Obama-adminisztráció ismételten megerősítette az internetszabadság fontosságát az amerikai külpolitikában. (Fidler 2012) Ez előre jelezte az Egyesült Államok aktív fellépését az elkövetkező időszakban. Ebből a szempontból kiemelkedő jelentőségű volt a 2011-es év, amikor elfogadták az ország kibertérre vonatkozó nemzetközi stratégiája, valamint több bilaterális egyezmény megkötésére is sor került, amelyekkel a későbbiekben részletesen is foglalkozom.

A kiberstratégia megerősítette azt, hogy az Egyesült Államok az alapjogok érvényesülését tartja bármilyen internetszabályozás alapjának. A szólásszabadságon kívül ez magában foglalja a magánélet védelmének biztosítását és az információ szabad áramlását. A dokumentum második fejezete kifejezetten a diplomáciai célokra koncentrál, amelyek között szerepel a kibertérrel kapcsolatos alapelvek terén konszenzus kialakítása a nemzetközi közösséggel. Ennek módja elsősorban bi- és multilaterális egyezmények kötése, valamint a magánszektor képviselőivel való szoros kapcsolattartás. A dokumentum kitér a kiberfenyegetések elleni fellépésre is, és fenntartja az Egyesült Államok számára a jogot, hogy egy állam részéről érkező kibertámadásra akár gazdasági szankciókkal vagy fegyveresen is válaszoljon. (White House, 2011)

A 2011-ben megkötött kétoldalú megállapodások sorában az elsők között volt a február 4-én bejelentett közös kanadai-amerikai akcióterv, amelyben fontos szerepet kap a kiberbiztonsághoz kapcsolódó együttműködés létrehozása és a digitális kritikus infrastuktúra védelme. Ezekhez kapcsolódóan Kanada vállalta, hogy ratifikálja az Európa Tanács Számítástechnikai bűnözésről szóló egyezményét (a továbbiakban Budapesti Egyezmény) is, amellyel bővebben az Európáról szóló részben foglalkozom. (http://actionplan.gc.ca/2011) Ugyanezen évben kiegészítésre került az 1951-ben megkötött ANZUS-paktum is,[2] amely ezután már a kibertérben indított, a részes felek „területi integritását, politikai függetlenségét vagy biztonságát" fenyegető támadás esetén is előírja az Egyesült Államoknak és Ausztráliának a közös fellépést. (Sullivan

2 ANZUS: Ausztrália, Új-Zéland és Egyesült Államok Biztonsági Egyezménye, 1951. szeptember 1-jén írták alá az érintett államok. 1986-ban, egyéves vitát követően az Egyesült Államok felfüggesztette kötelezettségvállalásait Új-Zélanddal szemben, és azóta csak éves bilaterális találkozókra (AUSMIN) kerül sor Ausztráliával.

2014; Levin – Ilkina, 2013, p. 5.) 2011. május 25-én együttműködésről szóló megállapodás született az Egyesült Királyság kormányával is, amelynek részleteivel a brit szabályozásról szóló fejezetben foglalkozom. (www.gov.uk, 2011) Ugyanezen év július 19-én Indiával közös szándéknyilatkozatot írt alá Lute amerikai helyettes államtitkár, amely a kiberbiztonsággal összefüggő kritikus információk cseréjét irányozta elő. (http://www.dhs.gov, 2011) Ennek folytatásaként 2015. augusztus 11-12-én megbeszélésre került sor az amerikai és indiai kormánydelegációk között, ahol a korábbiakon túl felmerültek a kiberbűnözéssel szembeni fokozott fellépés, az internetszabályozás és a kibertérben történő állami viselkedési normák kérdései is. (White House Statement, 2015) Az Egyesült Államok, Kanada, az Egyesült Királyság, Ausztrália és Új-Zéland közötti multilaterális hírszerzési együttműködést Öt Szem (*Five Eyes*) néven is emlegetik. Az Edward Snowden által kiszivárogtatott információk szerint ez egy „szupranacionális hírszerző ügynökség, amely nem felelős a részes országok saját jogszabályainak", működési elve pedig az, hogy egymás állampolgárait figyelik meg, ezzel kerülve meg az ezt korlátozó törvényeket. Ezen kívül más szövetséges országok, illetve az ENSZ tisztségviselőinek lehallgatásáról is derültek ki információk. (Ellis, 2014, p. 178.)

Az Egyesült Államok nemcsak a baráti országokkal igyekszik a kibertér szabályozásának jövőjét alakító egyezményeket kötni, hanem azon államokkal is, melyekkel alapvető nézetkülönbség van a szabályozás alapját illetően. 2013 júniusában Oroszországgal született megállapodás, amelyben a felek kötelezettséget vállaltak, hogy a nemzetbiztonságot érintő incidensekről valós idejű kommunikációt folytatnak közvetlenül egymással. (Eichensehr, 2015, p. 364.)

Kínával kapcsolatban sokkal kevésbé egyértelmű az amerikai viszony. Hillary Clinton 2010-es kijelentése elsősorban a kínai módszer kritikája volt, melyet éles diplomáciai válasz követett Peking részéről. (Crook 2010) Xi Jinping elnök 2013-as hivatalba lépésekor küldött gratulációjában Obama elnök egyúttal felvette a kiberbiztonság kérdését, amely a másik fontos töréspont a két állam között. Xi későbbi amerikai látogatása alkalmával is utalt az amerikai elnök azon internetes betörésekre, amelyek szerinte Kínából indultak – amit a kínai vezetés tagadott –, és az amerikai kormányzaton kívül számos nyugati vállalat számára is súlyos károkat okoztak, elsősorban ipari kém-

kedéssel. A kérdésben azonban nem közeledett a két fél álláspontja. (Lee, 2014, p. 951) 2015. szeptember 24-25-én Xi elnök ismételt amerikai látogatása során a két ország számos ügyben, így a kiberbiztonság kérdésében is egyezményt kötött. Ebben a felek megegyeztek arról, hogy fellépnek a területükről elkövetett kiberbűncselekmények ellen, és ezek eredményéről szükség esetén tájékoztatják egymást. Ezen kívül létrehozásra kerül a kiberbűnözés elleni fellépés és a kapcsolódó kérdésekkel foglalkozó magas szintű kapcsolattartási mechanizmus. Egyúttal a felek ígéretet tettek arra, hogy nem hajtanak végre vagy támogatnak tudatosan olyan cselekményeket, amelyek üzleti titkok és szellemi tulajdon lopására irányulnak. (White House Fact Sheet, 2015)

Az Egyesült Államok a Mandiant biztonsági cég 2013-as jelentése óta nyíltan a kiberbetörések egyik fő forrásának nevezi Kínát. A dokumentum szerint a kínai Népi Felszabadító Hadsereg 61398. számú egysége áll a nagyszámú támadás mögött. Az amerikaiak gyakran egyoldalú igénye Kínával szemben a kibertámadások mérséklésére valószínűleg nem segíti a feszültségek enyhülését, hiszen maga az amerikai kormányzat is érintett volt bizonyos kiberháborús eszközök alkalmazásában. Snowden 2013-as szivárogtatását követően kiderült, hogy az Egyesült Államok 2011-ben 231 támadást hajtott végre Oroszország, Kína, Irán és Észak-Korea ellen. (Eichensehr, 2015, p. 319.) A leghírhedtebb ilyen akció azonban korábbra tehető: 2007-ben kezdődött meg az az izraeli-amerikai közös hadművelet, amelynek keretében kártevő szoftverrel fertőzték meg az iráni atomkutatásban urándúsításra használt centrifugákat. (Moore, 2013, p. 226.) A Stuxnet névre hallgató vírus húszszor összetettebb kódolással készült, mint más kártevők, és szinte teljesen hibamentes. Úgy írták meg, hogy a rendszerbe jutást követően képes legyen teljesen önállóan működni. További különlegessége, hogy úgy képes megváltoztatni az érintett rendszerek működését, hogy közben mindent rendben lévőnek mutat a kezelőszemélyzet felé. Terjedéséhez úgynevezett nulladik napi sebezhetőségeket használt ki, és a gyárakban, erőművekben, valamint a kritikus infrastruktúráknál (pl. forgalomirányító rendszerekben) használt Siemens programozható logikai vezérlőket fertőzte meg. Tényleges célpontjai csak bizonyos, megadott azonosítószámmal ellátott típusok voltak, amelyeket elsősorban Iránban gyártottak. 2010 júniusában jelenlétét számos ilyen helyen fedezték fel. A kártevő az év novemberéig az iráni centrifugák ötödét rongálta meg, ezzel több hónapos leállásra kényszerítve

az iráni atomprogramot. (Sipos, 2016, p. 29.) A 2016. július 8-án megjelent *Zero Days*[3] című dokumentumfilm amellett érvel, hogy a korábban tagadott amerikai–izraeli kormányérintettség egyértelmű a bizonyítékok fényében. Emellett szól például a kártevő kifinomultsága, továbbá az, hogy a célba vett rendszerek megfertőzése, azok internettől való elzártsága miatt csakis személyi közreműködéssel történhetett. A támadók az iráni urándúsító üzem beszállítóit fertőzték meg először, és rajtuk keresztül juttatták be a Stuxnetet. További jel a támadás állami tervezettségére, hogy a kártevő támadása idején számos vezető iráni atomtudós merénylet áldozata lett. A dokumentumfilmben megszólaltatott amerikai és izraeli személyek alapján a Stuxnet létrehozásának kezdeményezője George W. Bush elnök volt, aki el akarta kerülni a nyílt fegyveres konfliktust Iránnal, ugyanakkor az iráni nukleáris kapacitás kiépülését is meg akarta akadályozni. Belső források szerint a kártevő fejlesztésében részt vett az NSA, a CIA, az amerikai hadsereg Kiberparancsnoksága, a Moszad és a kiberháborúra specializálódott izraeli 8200-as egység. A kódban elhelyeztek egy záró dátumot is, amely csak néhány nappal esik Barack Obama elnöki beiktatása elé, és többek szerint ez is a Bush-adminisztráció érintettségét mutatja a kártevő elkészítésében. Ugyanakkor a támadásokra már Obama elnök kellett, hogy engedélyt adjon, mivel – mint az a Snowden által kiszivárogtatott anyagok között lévő elnöki rendeletből kiderül – támadó kibertevékenységet csak az elnök utasítása alapján lehet folytatni. A leállás dátuma és a támadások közötti időintervallumban a kártevő kódja fejlesztésre került. Ezt azonban már a gyors eredményeket akaró izraeliek saját maguk végezték el, és a változtatások azt eredményezték, hogy a kártevő elterjedt az egész világon, és létezése nyilvánosságra került.

Kínával kapcsolatban ugyanakkor más hangok is vannak, amelyek az együttműködés helyett a szankciós politikát javasolják. 2006-ban a Kongresszus egyik képviselője javaslatot tett a globális online szabadságról szóló törvény (*Global Online Freedom Act*, GOFA) elfogadására, aminek oka az amerikai információs magáncégek és a kínai kormány közötti együttműködés vitás megítélése volt. Újabb javaslatok kidolgozására került sor 2007-ben, 2009-ben és 2011 áprilisában, illetve decemberében. Ezek közül a 2007-es

3 Az alkotás címe (nulladik napok) az olyan számítástechnikai sebezhetőségekre utal, amelyeket a támadón kívül senki más nem fedezett még fel, ezért javítani sem tudták azokat.

javaslat jutott legtovább a jogalkotási eljárásban, mivel az a Kongresszus elé került, miután Christopher Smith republikánus képviselő benyújtotta azt. A javaslatot rajta kívül 3 republikánus és 4 demokrata képviselő támogatta. A szavazásra bocsáthatóságról az Energiaügyi és Kereskedelemi, valamint a Jogi Bizottság döntött, amelyek elutasították annak Kongresszus elé terjesztését. (GovTrack, 2016; Congress, 2016) Ennek a változatnak három fő sarokpontja volt: éves jelentések készítése az egyes országokban tapasztalható internetkorlátozásokról, a leginkább korlátozó országok megjelölése és végül a rendszer fenntartásához szükségesnek ítélt technikai javak ezen helyekre történő exportjának korlátozása. (Fidler, 2012) Véleményem szerint egy ilyen lépés megtétele egyértelműen a hidegháborús COCOM-lista[4] felélesztését jelentené, és jelentősen rombolná az államok közötti bizalmat, ellehetetlenítve a közös nevezőre jutást.

3. Európa

3.1. A közösségi szabályozás kezdetei

Európában az 1990-es években kezdett el kialakulni a kibertér szabályozása, egyszerre nemzeti és nemzetközi szinten. Az utóbbi formálásában a legaktívabbak az Európa Tanács és az Európai Unió voltak. Az internethozzáféréssel rendelkező háztartások aránya világviszonylatban is kiemelkedően magas az EU tagállamokban, az Eurostat (2015) adatai szerint 2014-ben átlagosan 78%-os volt. A jelentős számú felhasználó mellett a másik fontos tényező, ami a szabályozás alakulását befolyásolta, az e-kereskedelem jelentőségének felismerése volt. Az Unió JOIN/2013/01 sz. európai kiberstratégiájának preambuluma évi 500 milliárd euróra becsülte azt a gazdasági növekedést, amit az egységes digitális piac kialakítása jelentene. A stratégiában megfogalmazásra kerül az a felismerés is, hogy ennek alapja a felhasználói bizalom megteremtése.

A bizalom megteremtésének egyik fontos eszköze a kiberbűnözés elleni fellépés erősítése. Ennek terén az európai jogharmonizáció 1989-ben kez-

4 COCOM-lista: a hidegháború nyugati blokkjába tartozó országainak a keleti blokk államaival szemben bevezetett gazdasági embargója, amely megtiltotta csúcstechnológiai termékek ide történő exportját.

dődött el, amikor az Európa Tanács kibocsátotta a számítógépekkel kapcsolatos bűncselekményekről szóló R (89) 9. számú Miniszteri Bizottsági ajánlást, amelyben a kriminalizálandó cselekményeket határozták meg a jogalkotó számára egy minimum, illetve egy fakultatív listába foglalva. Ennek előkészítése már 1985 óta folyt egy szakértőkből álló bizottságban, amelynek zárójelentésében foglalt tanulságait az ajánlás részévé tették. Hat évvel később került megalkotásra az információs technológiával összefüggő büntető eljárásjogi problémákról szóló R (95) 13. ajánlás, amelyben alapvető eljárásjogi kérdések kerültek tisztázásra. (Walden, 2004)

2001. november 23-án került elfogadásra az Európa Tanács Számítástechnikai bűnözésről szóló egyezménye (a korábban már említett Budapesti Egyezmény), amely jelentős előrelépés volt, hiszen míg az ajánlások végrehajtása teljesen opcionális, ennek ratifikációjával a részes államok kötelezettséget vállalnak annak érvényre juttatására. A szerződést 2001-ben 35 ország írta alá, köztük olyan Európa Tanácson kívül államok, mint az Egyesült Államok, Kanada, Japán és Dél-Afrika, ám az egyezmény ratifikációja több országban is várat még magára. (Buono, 2012, p. 336.) 2012-re harminchat ország ratifikálta a szerződést, köztük az Egyesült Államok, rajtuk kívül pedig további tizenöten aláírták, de még nem ratifikálták, mint pl. Kanada, Dél-Afrika és Svédország. (Borisevich et al. 2012, p. 272.) A Budapesti Egyezmény lefektette a kibertér szabályozásának azon minimumát, amelyet a nyugati világ egyöntetűen elfogad. Jól mutatja ezt az is, hogy a Brit Nemzetközösség 54 igazságügyi minisztere támogatta az Egyezmény mintájára megalkotott a számítógépes és számítógépes környezetben elkövetett bűncselekményekről szóló LMM (02) 17. modelltörvényt. (Walden, 2004, p. 324.) Más szervezetekben is az Egyezmény alapján képzelik el a kiberbűncselekményekkel kapcsolatos szabályozás megalkotását, így például a Karib-tengeri Közösségben (Project Cybercrime, 2014) és a Délkelet-ázsiai Nemzetek Szövetségében (ASEAN, 2008).

Az Európa Tanács ezt követően is részt vett a kibertér szabályozásának alakításában, továbbá számos, az igazságszolgáltatásban dolgozók részére szóló továbbképzést szervez. (Council of Europe, 2016) 2012-ben – az Európai Unióval közös CyberCrime@IPA projekt kereti között –, az angol Nigel Jones felügyeletével kezdődtek el a munkálatok az elektronikus bizonyításról szóló

útmutató elkészítésén. Ennek célja azon országok bírói, ügyészi és rendőrei munkájának segítése, melyek még csak most dolgozzák ki a kiberbűnözés elleni fellépésről szóló stratégiájukat. A dokumentum még ebben az évben elkészült és június 7-én az Octopus konferencián, amelyen 80 ország, nemzetközi szervezetek, a magánszektor és a tudományos élet szakértői voltak jelen. (Electronic Evidence, 2016)

3.2. Az Európai Unió kiberbiztonság megteremtésére irányuló lépései

A kiberbűnözéssel kapcsolatos európai jogharmonizációra az Európai Unió keretei között is sor került. Az Unió szupranacionális szabályozásában hangsúlyos szerep jutott a kiberbűnözés elleni közös fellépés megteremtésének. Az 1992-ben elfogadott Maastrichti Szerződés alapján létrejött hárompilléres rendszerben a kiberbiztonság a második pillért jelentő közös kül- és biztonságpolitika, a kiberbűncselekményekkel kapcsolatos szabályozás pedig a harmadik pillér, a bel- és igazságügyi együttműködés része lett. Ez a két terület sok vonatkozásban hasonlított egymásra, ami abból fakadt, hogy mindkettő az államközi együttműködés szintjén valósult meg. Az ezekkel kapcsolatos döntések meghozatalához – néhány végrehajtó jellegű szabályt kivéve – a tagállamok Európai Tanácsban lévő állam- és/vagy kormányfőinek egyhangú döntésére volt szükség, valamint az Európai Bizottság meg kellett ossza kezdeményezési jogát a tagállamokkal, és a Parlamentnek mindössze korlátozott konzultatív jogkör jutott. Továbbá az EU nem fogadhatott el közvetlen hatályú szabályozást, és az EU Bírósága nem vizsgálhatta a megszületett másodlagos jogforrások érvényességét, valamint szerződésekkel való összeegyeztethetőségét. (Chalmers 2014, p. 53.)

Az 1999-ben hatályba lépett Amszterdami Szerződés fontos, harmadik pillért érintő újítása volt a kerethatározatok bevezetése, amely lényegét tekintve közvetlen hatály nélküli irányelv volt. (Peers 2011, pp. 272–273.) Ilyen formában került sor a kibertérre vonatkozó legtöbb jogforrás elfogadására. Fontos lépés volt a 2005//222/IB kerethatározat elfogadása, amely a Budapesti Egyezmény megoldásait vette át. A 2007-ben Észtország ellen oroszpárti hackerek által elkövetett kiterjedt kibertámadás tapasztalatai nyomán került sor a 2008/114/EK irányelv elfogadására, amely a kritikus infrastuktúra ki-

jelölésével és védelmével foglalkozik. A Lisszaboni Szerződés 2009-es hatályba lépéséig ezen rendelkezések végrehajtásának eszközrendszere csak igen nehezen volt biztosítható. A hárompilléres rendszer számos problémával és hiányossággal küzdött, többek között a tagállamoknak széles jogköröket biztosító szabályozásból eredő uniós intézményrendszer elégtelen mozgásteréből és a másodlagos jogforrások tagállamok általi helytelen átültetéséből következően. A Lisszaboni Szerződés elfogadása jelentős változásokat hozott, így a Tanácsban a döntéshozatalhoz már nincs szükség egyhangúságra, csak minősített többségre; bővültek a Parlament jogalkotási lehetőségei, és a Bíróság is minden jogkörét gyakorolhatja. (Buono, 2012, p. 336.; Chalmers, 2014, p. 583.)

A Szerződés után kezdődött meg az addigi másodlagos uniós jogforrások újragondolása, és a kiberbűnözéssel kapcsolatos EU szabályozás új alapokra helyeződött mind jogi, mind politikai szinten. A 2005-ös kerethatározat eddigre már elavulttá vált, mivel elfogadásakor a jogalkotó még nem ismerte fel a nagyméretű kibertámadásokban rejlő veszélyeket, valamint a botnetek megjelenése is új kihívást jelentett, melyet a jogforrás nem volt képes kezelni. (Buono, 2012, pp. 338.) Az ennek felváltására elfogadott 2013/40/EU irányelv már kriminalizálta a botnetek előállítását, árusítását, használatra történő beszerzését, behozatalát és forgalomba hozatalát is, valamint a bűnüldöző szervek szorosabb együttműködésére tett javaslatot az információs rendszerek ellen elkövetett bűncselekmények esetén. Fontos újítása az irányelvnek, hogy 10-11. cikke lehetővé teszi a jogi személyek felelősségének a megállapítását, és velük szemben különleges szankciók alkalmazását irányozza elő, mint az elkövetésre használt létesítmények bezárása vagy a bíróság által elrendelt felszámolás.

A tartalomszabályozás kérdései egységes uniós szabályozás hiányában elsősorban tagállami hatáskörbe tartoznak. Közülük számosan, így például Németország, az Egyesült Királyság és Magyarország is jogrendje részévé tette az internetblokkolást. (Parti, 2010) Kivételt képez a gyermekpornográfia, amely kapcsán a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló 2011/93/EU irányelv 25. cikke előírja a tagállamoknak, hogy az ilyen tartalommal bíró vagy azt terjesztő honlapokat azonnal távolítsák el, ami történhet a hozzáférés meggátolásával is.

Szintén nincs egységes, szupranacionális szintű szabályozás azzal kapcsolatban, hogy a titkosítással védett, feltehetően jogsértő tartalomhoz tartozó jelszó gyanúsítottól történő megszerzése az önvádra kötelezés tilalmába ütközik-e. A 2016. május 10-11-én Dublinban megtartott *Fighting Cybercrime: Between Legal Challenges and Practical Difficulties* című konferencián tartott előadásában Philippe van Linthout belga vizsgálóbíró is érintette a kérdést. Ő az ittas vezetéshez hasonlította az esetet: az intézkedés alá vont sofőr sem tagadhatja meg, hogy alávesse magát a szondáztatásnak vagy vérvételnek. A belga büntetőtörvénykönyv egy, míg a francia kódex három évig terjedő szabadságvesztéssel rendeli büntetni azt, aki megtagadja a feloldáshoz szükséges jelszó átadását a hatóságoknak. Utóbbi szerint a büntetés mértéke öt évig terjedő szabadságvesztés, ha a titkosított információ segítségével más bűncselekményt lehetett volna megelőzni. Ez sem jelent azonban megoldást: a VeraCrypt már képes úgy titkosítani adatokat, hogy maga a felhasználó sem ismeri az azt feloldó jelszót. Rainer Franosch hesseni első ügyész elmondta, hogy éppen ezért olyan esetekben, amikor félő, hogy a gyanúsított ezzel az eszközzel fog élni, kommandósok segítségével fogják el.

3.3. Az uniós jog egyéb internetre vonatkozó szabályozásai

A kiberbiztonságon túl számos más kérdésben is az európai szabályozás egységesítésére törekszik az Unió. Ezek közül a legfontosabbak az e-kereskedelem, az elektronikus tartalomszolgáltatás és az adatvédelem területén született másodlagos jogforrások. Ennek kiépítésében lényeges cél volt a telekommunikációs piac liberalizációja és összehangolása, amely néhány – a nemzeti viszonyokhoz történő jobb igazítás érdekében meghagyott – kivétellel meg is történt. Számos fogyasztói szolgáltatás ára csökkent ennek köszönhetően, ám ezen intézkedések nem váltották be a hozzájuk fűzött reményeket, és nem nőtt jelentősen a befektetések mértéke. Hogy az egyes nemzeti szabályozások különbségéből adódó nehézségeket megszüntessék, a Tanács és a Parlament COM(2013) 627 számmal javaslatot tett az elektronikus hírközlés egységes európai piacáról szóló rendelet elfogadására. Ez az Európa 2020 stratégia részét képező uniós Digitális Menterend legelső pillére. (Bartóki-Gönczy, 2014, pp. 3–4.)

A 44/2001/EK rendelet elfogadása fontos lépés volt annak érdekében, hogy megszűnjenek az interneten kötött szerződésekkel kapcsolatos bizonytalan-

ságok. A rendelet ugyanis bizonyos feltételek fennállása esetén lehetőséget teremt arra, hogy az így kötött fogyasztói szerződések esetén a fogyasztók lakóhelyükön perelhetőek legyenek, illetve indíthassanak pert. (Erdős, 2014, pp. 84–86.) Hasonlóan lényeges volt a fogyasztók jogairól szóló 2011/83/EU irányelv, amely számos rendelkezéssel igyekszik a digitális piac iránti bizalmat megteremteni. Így például a kereskedő a vásárlás előtt köteles meghatározott információkról (mint pl. a termék lényeges tulajdonságai, az elfogadott fizetési módok stb.) tájékoztatást adni, valamint a vásárláshoz vezető gombnak is egyértelműen tükrözni kell funkcióját. A szerződés másolatát vagy visszaigazolását a fogyasztó számára papíron vagy más adathordozón biztosítani kell. Továbbá az áru minőségét szavatolja az, hogy a fogyasztó 14 napon belül indoklás nélkül elállhat a szerződéstől. Ezek a rendelkezések mind arra szolgálnak, hogy a felhasználókat ne lehessen silány termékek árusításával megtéveszteni, és aláásni az internet iránti közbizalmat, amelynek erősítése az EU egyik igen fontos politikája.

Fontos még megemlíteni az internetsemlegesség kérdését is, hiszen az elvet támogatók szerint az internetet nyitottsága és könnyű elérhetősége tette sikeressé, és szerintük ezeket a feltételeket a megfelelő verseny érdekében jogi eszközökkel kell biztosítani. Ugyanakkor mivel az internet hozzáférésért fizetni kell, az azonos feltételek nem érvényesülnek, és a hálózatok jelenlegi kapacitása is véges. Ez utóbbi miatt jelent meg a szolgáltatók részéről a forgalomirányítási technikák alkalmazása, amely ugyanakkor lehetőséget teremtett arra, hogy bizonyos szolgáltatásokat ne vagy ne egyenlő minőségnek nyújtsanak a felhasználók részére. (Mester, 2012, pp. 149–150.) Az ezzel kapcsolatos vita az EU-ban 2009-ben kezdődött el, amikor a korábbi szabályozási keretet felülvizsgálták. (Bartóki-Gönczy, 2014, p. 12.) 2011-ben a Parlament és a Tanács COM (2011) a 222. sz. közös közleményében kiállt a semleges és nyitott internet mellett. Az ezt érő fenyegetések közé sorolta az adatforgalom blokkolását és gátolását, valamint az adatkérések feltorlódását és az átláthatóság hiányát. A Bizottság 2015. június 30-án kelt IP/15/5265 sajtóközleményében jelentette be, hogy döntés született a roaming díjak eltörléséről, valamint a nyílt internet támogatásáról. Ennek értelmében a felhasználók szabadon eldönthetik, milyen tartalmakhoz férnek hozzá, és ezt sem blokkolni, sem lassítani nem lehet, továbbá a fizetett prioritizálás is tiltott lesz. Vagyis min-

den adatforgalmat egyformán kell kezelni, ami alól csak pontosan meghatározott – biztonsági jellegű – kivételek lehetnek. Ugyanakkor a javaslatot számos kritika érte, amelyek szerint homályos és pontatlan megfogalmazásai kiskapukat biztosítanak a szabályozás megkerülésére. Az ezzel kapcsolatos módosító javaslatok mindegyikét leszavazták a Parlamentben. (Price, 2015)

Nagy változásokra került sor az uniós adatvédelmi szabályozásban is. A személyes adatok kezeléséről szóló 95/46/EK irányelv rendelkezései alapján személyes adatot csak akkor lehet harmadik országba továbbítani, ha az ottani védelem szintje megfelelő. Az irányelv lehetőséget biztosít a Bizottság számára, hogy az megállapítsa a megfelelő védelmi szint meglétét egy országban, ekkor nem kell alkalmazni a különleges korlátozásokat az ide irányuló adattovábbítások esetén. A Bizottság a védett adatkikötőről szóló 2000/520/EK határozatában elismerte az Egyesült Államok Kereskedelmi Minisztériuma által kiadott biztonságos kikötőkre (*Safe Harbor*) vonatkozó alapelveket mint a védelem megfelelő szintjét. Ez a döntés olyan feltételek mellett is lehetővé tette az amerikai cégek számára a személyes adatok továbbítását, amelyeknél a szabályozás lényeges eltérései miatt egyébként nem lett volna lehetőség. Az Unió által meghatározott három alapelvnek (adatvédelmi politika átláthatósága, biztonságos kikötő alapelveinek a vállalati adatvédelmi politikába építése és hatósági végrehajtás) meg kellett felelni.

Az EU intézményei számára mindig is fontos kérdés volt az adatvédelmi szabályok maradéktalan betartása, és ezek elégtelensége esetén fellépett. Így például a Bíróság 2006 májusában a C-317/04 és C-318/04. egyesített ügyekben formai okok miatt megsemmisítette az USA és az Európai Közösség közti személyes adatok továbbításáról szóló megállapodást, amely a terrorizmus elleni küzdelem részeként született meg. 2014 májusában a C-131/12. ügyben a Bíróság úgy határozott, hogy a keresőmotorok működtetői felelősek a külső honlapokon fellelhető személyes adatok kezeléséért, és az érintettek közvetlenül megkereshetik őket, hogy töröljék a róluk információt tartalmazó linket a találati listáról. (Lehóczki, 2015, p. 94.)

Éppen ezért váltott ki heves reakciókat Edward Snowdennek az amerikai hírszerzés működését felfedő 2013-as kiszivárogtatása. Az Unióban, és különösen Németországban, jelentős megrendülést okoztak azok a hírek, miszerint az NSA korlátlan hozzáféréssel bír a kibertérben található személyes adatok-

hoz. (Lehóczki, 2015, p. 93.) A Bizottság az ügyre reflektálva két közleményt is megfogalmazott a kérdésben 2013 novemberében: a COM(2013) 846 a bizalom helyreállításával, a COM(2013) 847 pedig a rendszer vizsgálatával foglalkozott. Utóbbi során a Bizottság jelentős hiányosságokat talált, amelyek orvoslására 13 pontból álló ajánlást fogalmazott meg. A biztonságos kikötő végét azonban a Bíróság a C-362/14 számú, Schrems-ügyben hozott ítélte jelentette. Schrems osztrák állampolgárként az ír adatvédelmi hatósághoz nyújtott be panaszt, mivel a Facebook európai leányvállalata itt működik, és innen továbbítják az amerikai szerverekre a feltett tartalmat, ezt azonban elutasították. Az ír legfelsőbb bíróság az EU Bírósághoz fordult előzetes döntéshozatali kérelemmel, amely 2015. október 6-án hozott ítéletében érvénytelennek mondta ki a Bizottság 2000/520/EK határozatát, ezzel véget vetve a biztonságos kikötő rendszerének. Az ítélet nem csak az ezt követő adattovábbításra, de a már ott tárolt adatokra is vonatkozik, hiszen a határozatot visszamenőlegesen is érvénytelennek kell tekinteni. (Lehóczki, 2015, pp. 95–98.)

A személyes adatok védelméről szóló COM(2012) 11 rendelet javaslatát négy év vita után, 2016. április 15-én fogadták el a 95/46/EK irányelv felváltására. Az uniós jogalkotó célja ezzel az volt, hogy az adatvédelmet megnehezítő gyors technológiai fejlődésre választ adjon. Az új szabályozás gazdaságilag is fontos, hiszen remények szerint növeli az internetes kereskedelembe vetett bizalmat.

3.4. Az EU kiberteret érintő politikája: több érdekelt bevonása

Az Európai Unió a kibertér szabályozásával kapcsolatban igyekszik minél aktívabb külpolitikát folytatni, és aktívan részt venni a kiberbiztonsággal kapcsolatos nemzetközi diskurzusban. A 2012-es ITU nemzetközi távközlési világkonferencián való részvétel kapcsán a Tanács COM(2012) 430 határozatában úgy fogalmazott, hogy a nemzetközi távközlési szabályozás (ITR) bármely módosítása összhangban kell, hogy legyen az uniós vívmányokkal, és segítenie kell az Unió céljainak elérését. 2014-ben a Tanács következtetései a kiberdiplomáciáról című 9967/4/14. számú dokumentumban sor került a kibetérrel kapcsolatos nemzetközi politika hat uniós pillérének meghatározására. (Dancă 2015, p. 95.) A dokumentumban olyan EU-s értékek jelennek meg, mint az emberi jogok védelme a kibertérben, a hatályos nemzetközi

jog alkalmazása a nemzetközi biztonság területén és a több érdekelt bevonásával működő szabályozási modell támogatása. A Tanács számos célt is megfogalmaz ebben, mint például az EU versenyképességének és jólétének fokozása, a kiberkapacitás-építés és -fejlesztés, valamint a nemzetközi partnerekkel való szorosabb együttműködés.

Intézményi szinten is megfigyelhető ennek a szabályozási modellnek az alkalmazása. Az 526/2013/EU rendelet – felváltva a 460/2004/EK rendeletet – újragondolta az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (European Network and Information Security Agency, ENISA) feladatköreit, és jelentősen kibővítette azokat. Fontos szerep jut a szervezet számára a hálózat- és információbiztonsággal kapcsolatos – mind az uniós szervezetekkel, mind a harmadik országokkal történő – együttműködés kiépítésében. Ennek részeként az ENISA és az Európai Közös Kutatóközpont 2010-ben megtartotta első páneurópai kiberbiztonsági gyakorlatát, a „Kiber Európa 2010"-et, amely a tagállamok közötti szorosabb együttműködést volt hivatott elősegíteni. (Zhang, 2013, p. 124.)

Az Európai Bizottság COM (2012) 140 közleményében beszámolt az Europolon belül egy új szervezet létrehozásáról, amelynek feladata kifejezetten a kiberbűncselekményekkel kapcsolatos bűnüldözési feladatok összehangolása. Ez 2013. január 1-jén kezdte meg működését Hágában Europol Számítástechnikai Bűnözés Elleni Európai Központ (European Cybercrime Centre, EC3) néven. A nyomozásokban való segítségnyújtáson kívül számos más tevékenységet is ellát, így például információt gyűjt, és elemzi a kiberbűnözés alakulását, segít a tagállamoknak a kapacitásépítésben, valamint kapcsolatot teremt a bűnüldöző szervek és a magánszektor, valamint a tudományos élet között. (Buono, 2012, pp. 340–342.) A szervezeten belül működik egy rendőri különítmény is Kiberbűnözés Elleni Közös Munkacsoport (Joint Cybercrime Action Taskforce, J-CAT) néven, amelyben négy unión kívüli ország – Egyesült Államok (FBI, USSS), Kanada, Ausztrália és Kolumbia – is képviselteti magát. Ennek feladata a kulcsfontosságú kiberfenyegetések – így például az online csalás, botnetek és gyermekek szexuális kizsákmányolása – elleni fellépés. (Europol, 2014)

Politikai szinten nagyon lényeges a 2015 áprilisában elfogadott európai biztonsági stratégia (COM (2015) 185.), amely számos kihívás mellett foglal-

kozik a kiberbűnözés elleni fellépéssel is. A dokumentum kiemeli a harmadik országokkal megkötött kölcsönös jogi segítségnyújtási megállapodások fontosságát. Az Uniónak a harmadik államok közül tízzel van stratégiai partneri megállapodása (USA, Kanada, Mexikó, Brazília, Dél-Afrika, India, Kína, Japán, Dél-Korea és Oroszország), amelyek közül az Egyesült Államokkal való együttműködés a kiberbiztonság területén a leginkább elmélyült. (Dancă, 2015, p. 96.) A biztonsági stratégia kiberbűnözéssel foglalkozó fejezete külön nevesíti az EU–USA kiberbiztonsággal és számítástechnikai bűnözéssel foglalkozó munkacsoportot a támogatandó nemzetközi kezdeményezések között. Ennek fontosságát mutatja, hogy az USA-val való együttműködést már a két évvel korábbi kiberbiztonsági stratégia is szorgalmazta, amely az EU legfőbb partnereként tekint az Egyesült Államokra. (Fahey, 2014, p. 47.) Az EU ugyanakkor nem kíván együttműködni sem Kínával, sem Oroszországgal a kiberbiztonság területén, sőt politikailag motivált támadásaik miatt a biztonságot gyengítő tényezőként tekint rájuk. Ennek a hozzáállásnak az egyik oka, hogy az orosz–uniós viszony jelentősen megromlott a kelet-ukrajnai konfliktus kitörése óta. (Dancă, 2015, p. 96.)

3.5. Egyesült Királyság: a különutas politika

Az Egyesült Királyság igen korán nemzeti joga részévé tette a kiberbűnözés elleni fellépést. Az 1990-ben elfogadott számítógépes visszaélésről szóló törvény (*Computer Misuse Act*) három magatartást kriminalizált: engedély nélküli hozzáférés a számítógéphez, engedély nélküli hozzáférés további bűncselekmények elkövetésének szándékával és a számítógépes adatok engedély nélküli módosítása. 2006-ban a rendőrségi és igazságszolgáltatási törvény (*Police and Justice Act*) kisebb mértékben kiegészítette a jogszabály szövegét. 2000-ben fogadták el a vizsgálati hatáskörök szabályozásáról szóló törvényt (*Regulation of Investigatory Powers Act*), melynek rendelkezései szerint az elektronikus kommunikáció határozat nélkül is lehallgatható, amennyiben a résztvevők legalább egyike beleegyezett ebbe. A 2012-ben előterjesztett javaslat a hírközlési adatokról szóló törvényről (*Communications Data Bill*) kötelezte volna a szolgáltatókat arra, hogy 12 hónapra megőrizzék a felhasználók böngészési előzményeit, valamint felhatalmazta az államot arra, hogy monitorozza az internetes kommunikációt, és a mobiltelefonok használóját

azonosító adatokhoz hozzáférhessen. A javaslatot a liberális demokraták élesen ellenezték annak lehetséges alapjogsértő következményei miatt, amely végül nem került elfogadásra. (Levin – Ilkina, 2013, p. 18.) 2015-ben a kormányzó konzervatív párt átdolgozott formában, jóval szigorúbb előírásokkal újra benyújtotta azt. (BBC, 2015) A feladatok ellátásra két specializált szervezetet hoztak létre: a Kiberbiztonsági Irodát (*Office of Cyber Security*) és a Kiberbiztonsági Műveleti Központot (*Cyber Security Operations Centre*). Előbbi a különböző kiberbiztonsági tervek koordinálását, míg utóbbi a jelentősebb kormányzati és nem kormányzati információs rendszerek védelmét látja el. (Zhang, 2013, p. 125.)

Az Egyesült Királyság kiberbiztonsággal kapcsolatos politikáját az teszi különutassá, hogy a kormány a Lisszaboni Szerződést csak jelentős engedmények árán ratifikálta, és ezek között volt az igazságügyi és belügyi együttműködést érintő uniós jogszabályokból való kimaradás lehetősége, amellyel azóta is él. (Egedy, 2013) Másik hasonló engedmény volt annak kimondása, hogy a közös kül- és biztonságpolitikára vonatkozó rendelkezések nem érintik a tagállamok hatásköreit külpolitikájuk kialakításában. Mindezek miatt kijelenthetjük, hogy az Unióból történő kilépésről szóló június 23-i népszavazás eredménye érdemben nem fogja megváltoztatni a kiberbiztonság területén eddig folytatott brit politikát.

2010-ben megszületett a Stratégiai Védelmi és Biztonsági Felülvizsgálat, egy évvel később pedig elfogadták a nemzeti biztonsági stratégiát, amely a terrorizmust, a kibertámadást, a katonai krízist és a természeti katasztrófákat tartja a legjelentősebb biztonsági fenyegetéseknek. (Zhang, 2013, p. 125.) 2011 novemberében pedig nyilvánosságra hozták az ország kiberbiztonsági stratégiáját, amely 2015-ig elérendő célként tűzte ki a kiberbűnözés megállítását; az Egyesült Királyság online érdekeltségeinek határozottabb védelmét; egy nyitott, stabil és színes kibertér létrehozását és az ezek biztosításához szükséges kapacitás kiépítését. A program megvalósítására 650 millió fontot költöttek. Ez jól mutatja, hogy az ország elsősorban a kiberbűnözés letörésében érdekelt – amely felmérések szerint évi 27 milliárd fontos veszteséget okoz a brit gazdaságnak –, és elsősorban erre koncentrál, nem a kibertámadások elleni védekezésre. (Levin – Ilkina, 2013, pp. 16–17.)

Nemzetközi szinten az Egyesült Királyság aktívan részt vesz a kibetér szabályozásáról folyó diskurzusban. 2011-ben David Cameron brit miniszterelnök és Barack Obama amerikai elnök közös közleményt adtak ki a kiberbiztonság terén történő együttműködésről. Eszerint a két ország összehangolja kutatás-fejlesztési tevékenységét, az információtechnológiák fejlődése kapcsán rendszeres együttműködést alakít ki a kapacitásépítésben résztvevő szervek között, a kiberbűnözés elleni fellépéshez szükséges eszközök számát növeli, a magánszektorral és a kereskedelmi partnerekkel szoros együttműködést hoz létre. További fontos pont még, hogy az Egyesült Királyság bejelentette csatlakozását a Budapesti Egyezményhez, és kifejezte szándékát annak ratifikációjára. (www.gov.uk, 2011) Az együttműködések terén érdemes továbbá megemlíteni az Egyesült Királyság-Kína Internet Keresztasztalt, amelynek célja a kommunikáció erősítése és a közös bizalom kiépítése. Szemben tehát az EU-val, az Egyesült Királyság partnerként tekint Kínára. (Zhang, 2013, p. 125.)

3.6. Oroszország

Oroszország gyakran a legnagyobb hackerpopulációval rendelkező országként élt a köztudatban. Olyan támadások fűzhetők oroszok nevéhez, mint az 1995-ös Levin-ügy, amelynek során mintegy hárommillió dollárt loptak el az amerikai Citibank ügyfeleitől. (Warren – Streeter, 2005, pp. 41–42) De hasonlóan nagy visszhangot váltott ki a Target amerikai cégcsoport rendszereibe történő 2013-as betörés, amely szintén az Orosz Föderációból indult ki. (McDougal, 2015, p. 55.) Az orosz hackerek nagy száma azonban nem véletlen: a hidegháború vége felé a hírhedt KGB számos számítógépes specialistát képezett ki, illetve használt fel a COCOM-listán szereplő nyugati szoftverek illegális beszerzése érdekében. A keleti blokk felbomlása után sok, ilyen kapcsolatokkal rendelkező volt államvédelmi ügynök csatlakozott a szervezett bűnözéshez. (Warren – Streeter, 2005, pp. 121–122)

Az orosz jogrendszer a kiberbűncselekmények esetén a szövetségi szerveknek biztosít elsőbbséget és általános illetékességet, míg a helyi adminisztráció csak korlátozott jogkörökkel bír. (Borisevich et al., 2012, p. 278.) Az 1996-os büntetőtörvénykönyv 272. szakasza bünteti a számítógépes információhoz való illetéktelen hozzáférést. A törvények védik a szellemi alkotásokat, és a Btk. komoly büntetéseket tartalmaz ezek megsértésének esetére. Ettől is

súlyosabb büntetés jár abban az esetben, ha valaki kártékony programokat terjeszt az interneten. A probléma gyökerei nem a törvényekben, hanem azok betartatásában keresendők: az orosz rendőrség gyakran hezitál fellépni az ilyen ügyekben, és ha meg is teszik, akkor is gyakran igen alacsony büntetéseket szabnak ki a bíróságok. (McDougal, 2015, pp. 56–58.) Egyes orosz régiókban a látencia mértéke az információkhoz való illetéktelen hozzáférés esetén meghaladhatja a 80%-ot is. (Borisevich et al., 2012, p. 285.)

A felderítésért a Belügyminisztérium „K" osztálya felelős, amelynek adatai alátámasztják a növekvő számú elkövetést. 2012 első felében 5956 kiberbűncselekmény ügyében indult nyomozás, amely 11%-kal több az előző év hasonló időszakához képest. A Group-IB orosz biztonságtechnikai cég szerint a fentebb említett okokon kívül ebben az is közrejátszik, hogy az egyes csoportok együttműködnek egymással a minél nagyobb profit érdekében. Ugyanakkor az orosz hatóságok keményen fellépnek a gyermekpornográfiával szemben: 2011-ben a „szornyak" (сорняк) névre keresztelt akció során szerzett bizonyítékok alapján 131 büntetőeljárás indult meg. A program eredményeként egy 24 országot magában foglaló együttműködés jött létre. A 2000-ben született Orosz Föderáció Információbiztonsági Doktrínája a kibertámadásoktól való védelmet tekinti elsődleges célnak. (Levin – Ilkina, 2010, pp. 30-31.)

Akárcsak más államokban, az orosz hadseregnek is van kiberháborúra szakosodott hadereje, amely azonban a kémkedés helyett inkább katonai célok elérése fókuszál. Nyugati vélemények szerint ők voltak felelősek az Észtország ellen 2007-ben ért kibertámadásokért, a 2008-as orosz–grúz konfliktus során grúz kormányzati weboldalakat elérhetetlenné tevő, és a 2014 óta tartó ukrán válság során az ukrán kormány elleni akciókért. (Muir, 2014, pp. 78–79.) Oroszország azonban ezen esetekben tagadta az érintettségét, és egyszerű internetes aktivisták tevékenységének tudta azt be. Ugyanakkor semmiféle hajlandóságot nem mutatott abban, hogy az észt hatóságokkal együttműködve felkutassa az elkövetőket. (Jensen, 2015, p. 278.) A 2010-ben született új katonai doktrína egyértelműen a hadsereg feladatának tartja a kiberbiztonság biztosítását, valamint jelentős katonai fenyegetésként értékeli az ország információs infrastruktúrája elleni támadásokat. (Levin – Ilkina, 2010, p. 31–32.)

Oroszország a nemzetközi színtéren nyíltan támogatja a nemzeti szuverenitáson alapuló szabályozás szükségességét. Az ITU 2012-es világkonferen-

ciáját megelőzően, 2011 júniusában Vlagyimir Putyin miniszterelnök kijelentette, hogy országának célja az, hogy a szervezeten keresztül nemzetközi irányítás alá vonja az internetet. (Eichensehr, 2015, p. 332.) Bár az ország már hosszú ideje Kína szövetségese az internetszabályozás nemzetközi kérdéseiben a hasonló célok miatt, Muir rámutat, hogy közöttük az együttműködés korántsem problémamentes. A két ország között régóta vannak geopolitikai feszültségek (például Szibéria hovatartozását illetően), és az egyéb politikai kérdések körüli viták a kibertér kapcsán folyó együttműködést is ellehetetleníthetik. A szerző véleménye szerint, mivel a Krím-félsziget annektálását követő nyugati szankciók még jobban kiszolgáltatták az orosz gazdaságot Kínának, az oroszok érdekeltek lehetnek a kínaiak meggyengülésében. (Muir, 2014, pp. 88–90) A 2015-ben kötött orosz-kínai bilaterális kiberegyezmény megkötése azonban azt mutatja, hogy ezek a törésvonalak korántsem olyan jelentősek a két ország között.

4. Ázsia

4.1. Kína modellje: az ellenőrzés elsődlegessége

Kelet-Ázsia legnagyobb és a világ második legnagyobb gazdaságaként Kína kibertérre alkalmazott szabályozásának áttekintése különösen fontos. A kínai modell régóta áll tudományos kutatások fókuszában, a nyugati szerzőket elsősorban az ország által alkalmazott szigorú szabályok és az információáramlást gátló, illetve annak ellenőrzésére szolgáló rendszerek érdeklik elsősorban. (Lee, 2014, p. 953.) Austin három időszakra osztja Kína kibertérrel kapcsolatos politikáját: a 2005-ig tartó lassú kezdetet a kiberháborút középpontba helyező elképzelés követte, és 2014 februárjától tör az ország a Xi Jiping elnök által „kiberhatalom"-nak nevezett státuszra. (Austin, 2016, p. 171.)

Az ország a Nyugatnál jóval később, csak az ezredforduló környékén ismerte fel az internet hatalmas gazdasági jelentőségét, és 1994-ben indultak meg a fejlesztések. (Gao, 2011, p. 353.) Emellett nagy szerepet játszott a döntésben annak rossz emléke is, hogy Kína milyen súlyosan meggyengült a XX. századra az ipari fejlesztések elhanyagolása miatt. Ekkor indult a kínai internethasználók száma robbanásszerű növekedésnek, ami az 1997-es egymilliós számról

2001-re huszonkét millióra nőtt. (Hachigian, 2001) Ez a tendencia a China Internet Network Information Center (2015) éves felmérései alapján tovább folytatódik napjainkig is: 2005-ben 111 millió, 2010-ben 457 millió, 2015 elején 649 millió kínai rendelkezett internethozzáféréssel, mely utóbbi a teljes lakosság 49%-át jelenti. Bár ez a lakosságszámhoz viszonyítva arányaiban kevésnek tűnhet, a látszat csal, hiszen már majdnem annyi kínai használja az internet lehetőségeit, mint ahányan az EU-ban és az Egyesült Államokban együttvéve. Ez a világ legnagyobb digitális piacává teszi az országot, ahogy azt már évekkel korábban megjósolták. (Blythe, 2007, p. 1.)

Az internet kínai térhódításánál az államot vezető Kínai Kommunista Párt (CPC) kezdettől fogva ügyelt arra, hogy politikai vezető szerepét biztosítsa. Az új, erősen decentralizált médiát jóval nehezebb ellenőrizni, mint a tradicionális kommunikációs csatornákat. A kormányzat központi, tartományi és helyi szervei ezek ellenére támogatták az internetelérés folyamatos kiterjesztését. (Hachigan, 2001) Az évek során számos olyan jogszabály született, amely a politikai helyzet fenntartását szolgálja. A 33/1997. sz. közbiztonsági minisztériumi rendelet például felsorolja, milyen típusú információkat tilos létrehozni, másolni, keresni és terjeszteni az interneten, és a kilenc elemből álló felsorolás többsége politikai bűncselekményt takar (pl. a szocialista államrend megdöntésére irányul). (Gao, 2011, p. 355.)

Ezen szabályok betartatására a CPC-nek a világ legkifinomultabb, internet ellenőrzésre szolgáló rendszerét sikerült kiépítenie, ami véget vetett azon nyugati reményeknek, hogy az internet elterjedése Kínában a többpártrendszeri változások fontos elősegítője lesz. (Lee – Liu, 2012, p. 127.) Kínában a tartalom szűrése a gyakran nagy tűzfalnak is nevezett Aranypajzs projekt keretei között történik. Az internetszolgáltatók szerepe ebben a rendszerben elsősorban formális, és csak az infrastuktúra működtetésére terjed ki. 2009-ben ennek kiegészítésére előírták, hogy minden számítógép otthoni szűrő szoftverrel együtt kerüljön értékesítésre, amely a gyermekeket hivatott megvédeni a központilag nem kívánatosnak ítélt szexuális, vallási és politikai tartalmaktól. A rendelkezés nagy tiltakozást váltott ki, így végül elálltak a tervtől. (Parti, 2010, p. 99.)

A kínai kormányzat is hamar felismerte a nemzetközi együttműködés szükségességét a kibertéren fenyegető új kihívások leküzdésében, és ezzel kapcsolatban saját elképzelést dolgozott ki. Ez különösen azért fontos számukra,

mert a nyugati szabályozást egyfajta kiberhegemóniaként értékelik, amely közvetlenül veszélyezteti a CPC hatalmát. (Gady, 2014) Mint Austin rámutat, bár Kína normameghatározó ország szeretne lenni a nemzetközi színtéren, jelenleg elsősorban csak normakövető szerepet játszik. (Austin, 2016, p. 172.) Jól mutatja a kínai elképzelést a szuverén államok szabályozásban betöltött szerepéről az a nyilatkozat, amely szerint csak ezeknek „van meg a felelősségük és joguk ahhoz, hogy megtegyék a szükséges intézkedéseket a honi kibertér és a kapcsolódó infrastruktúra fenyegetésektől, zavaroktól, támadásoktól és szabotázstól való védelme érdekében." (Jensen, 2015, p. 297.)

A Sanghaji Együttműködési Szervezet tagállamai államfőinek 2007-es találkozóján közös akciótervet fogadtak el, amelyben megállapodtak azokról az alapelvekről, amelyeket a számítógépes rendszerekkel szembeni kibertámadások elleni fellépésben kívánnak alkalmazni. A fő különbség a Kína, Oroszország, Kazahsztán, Kirgizisztán, Tádzsikisztán és Üzbegisztán által elfogadott dokumentum és a Budapesti Egyezmény között, hogy ez a részes államok számára teljes rendelkezési jogot biztosít a rendszerek és a bennük tárolt adatok felett, beleértve a politikailag veszélyesnek ítélt tartalmak elleni fellépés lehetőségét. (Sofaer – Clark – Diffie, 2010, p. 186.) 2014-ben Kína – a nemzeti szuverenitáson alapuló szabályozási elképzelése népszerűsítése érdekében – Wuzhenben megrendezte első internetes világkonferenciáját. Ennek hivatalos dokumentumában, a wuzheni kiáltványban megpróbálták meggyőzni a nyugati megjelenteket a kínai elképzelések helyességéről, de az álláspontok nem közeledtek egymáshoz. (Gady, 2014)

2015-ben a Sanghaji Együttműködési Szervezet tagjai módosították a korábbi nemzetközi magatartási szabályokra vonatkozó javaslatukat, amelyben megerősítették, hogy az államok szuverén joga politikai döntéseket hozni az internettel kapcsolatos közpolitikai kérdésekben. Egyúttal előírták, hogy minden részes állam köteles más államok szuverenitását, területi integritását és politikai függetlenségét tiszteletben tartani. Ez egyértelműen jelzi, hogy a nevezett államok által kívánatosnak tartott internetszabályozás a kormány ellenőrzése alatt áll. (Jong-Chen, 2015) Az ország 2015-ben bilaterális egyezményt is kötött Oroszországgal az információbiztonsággal kapcsolatos kérdésekről, amely a szoros együttműködés és információcsere mellett politikai jellegű kérdéseket is tartalmaz, így pl. a nemzetközi szervezetekben a szabá-

lyozással kapcsolatos hasonló elképzelések előmozdítását. (Kulikova, 2015) Alekszandr Szalinkov, az Információbiztonsági Intézet vezetője szerint az egyezmény szövege 70%-ban megegyezik a sanghaji együttműködés részeként elfogadott korábbi dokumentuméval, és az újdonság benne a belső szuverenitás védelmének fontosságát taglaló rész. (Roth, 2015) A nyugati elemzők szerint az elfogadásának oka az eddigi együttműködés megerősítése volt, amelynek végső célja a nemzeti szuverenitáson alapuló internetszabályozás multilaterális elfogadtatása. Austin egyúttal rámutatott, hogy az egyezmény 4. cikke nem tiltja a feleknek az egymással szembeni kiberkémkedést és a kiberháborús készülődést. (Gady, 2015) Mivel a szöveg az információs infrastruktúrát érő „jogellenes" beavatkozásokat zárja ki, ez úgy értelmezhető, hogy a tilalom csak békeidőre szól. (Austin, 2016, p. 178.) Akárcsak az orosz-kínai, az amerikai-kínai egyezmény sem tiltja az államtitkok megszerzésére irányuló internetes kémkedést. Ugyanakkor különbséget jelent, hogy az utóbbi tilalmazza a szellemi tulajdon és a kereskedelmi titkok kikémlelését.

Ugyanakkor Austin egy 2014-es amerikai jelentés alapján azon a véleményen van, hogy az eltérő alapkoncepciók ellenére számos kérdésben több a hasonlóság a kínai és az orosz megközelítésben, mint a különbség. Így például Kína támogatja a belügyekbe történő beavatkozás tilalmának kiterjesztését a kibertérre, valamint az internetszabályozás demokratizálását, amely megszüntetné az USA jelentős befolyását a domainnevek elosztását intéző ICANN-ben. A két ország véleménye megegyezik az állami felelősség szabályainak, a háborúindítás jogának és a hadijognak a kibertérben történő alkalmazásában is. (Austin, 2016, p. 176.)

4.2. Dél-Korea

Világviszonylatban Dél-Korea lakossága rendelkezik a legnagyobb arányú szélessávú internetelléréssel. (Leitner, 2009, p. 84) Szabályozásának sajátos jellegét az adja, hogy a koreai háború 1953-as fegyverszüneti lezárása óta nem tudott békeszerződést kötni északi szomszédjával. Utóbbi nem csak konvencionális és – egyes feltételezések szerint – nukleáris fegyverekkel jelent fenyegetést az országra, de a kibertérben is. Észak-Korea internetes kapacitását mutatja, hogy nem csak dél-koreai állami intézmények és hadsereg rendszerei,

de az északi vezetőről paródiafilmet készítő Sony ellen is sikerrel hajtottak végre támadást, jelentős kárt okozva a cégnek. Déli becslések szerint az ország a harmadik legnagyobb kiberháborús támadóerővel rendelkezik a világon. Ugyanakkor tompítja ezt az, hogy gyengén kiépített internetes infrastruktúrája miatt ennek az apparátusnak más államok hálózataira és botnetjeire van szüksége akciói végrehajtásához, ez pedig jelentősen behatárolja mozgásterüket. (Siers, 2014)

Dél-Korea azért is különleges, mert az internetes névtelenség kapcsán igen sajátos szabályozást vezetett be. A nyugati típusú demokráciák általában támogatják az anonimitást, mint például az Európa Tanács 2003-as, az internetes kommunikáció szabadságáról szóló deklarációjában vagy az Egyesült Államok Legfelsőbb Bírósága több ítéletében. 2007-ben azonban ezzel ellentétes szabályozás mellett foglalt állást Dél-Korea kormánya, ahol világviszonylatban is egyedülálló megoldásként az Információs és Kommunikációs törvény módosításával bevezetésre került az ún. „valódi nevet igazoló rendszer". Ezzel létrejött a nyugati demokratikus országok közül a leginkább korlátozó jellegű rendszer.

Lényege az volt, hogy a leglátogatottabb – kezdetben minden napi háromszázezernél, később minden napi százezernél több egyedi látogatóval rendelkező – weboldalat üzemeltető szolgáltatót köteleztek arra, hogy az őket felkereső felhasználókat egy közintézmény honlapjára irányítsák, ahol személyi igazolványszámuk segítségével azonosítaniuk kellett magukat, mielőtt tartalmat tehettek közzé. Az adatokat megőrizték, hogy egy esetleges későbbi büntetőeljárás során felhasználhassák őket. (Leitner, 2009, pp. 84.) A szabályozás szigorúsága összefüggött politikai tényezőkkel, így elsősorban a 2008-as Egyesült Államok elleni tüntetéssel, amelynek oka az amerikai marhahús importtilalmának feloldása volt. Az ekkori online tiltakozások szolgáltattak okot arra, hogy a törvény hatályát jelentősen kiterjesszék. (Leitner, 2009, pp. 92.) Politikailag motivált cenzúrára már korábban is volt példa az országban: a Nemzetvédelmi Törvény kriminalizálja az államellenes véleménynyilvánítást, például Észak-Korea nyilvános dicséretét vagy támogatását. Ezen rendelkezés alapján 2004-ben 31 északpárti weboldalt blokkoltak az országban, amelynek következtében azonban több ezer vétlen honlap is elérhetetlenné vált. (Leitner, 2009, p. 95.)

2012-ben a dél-koreai Alkotmánybíróság megsemmisítette a jogszabályi rendelkezést. Véleményük szerint a valós adatok felfedése előzetes cenzúrához vezetett, súlyos beavatkozást jelentett a felhasználók magánéletébe – hiszen ez alapján visszakövethető volt, mely weboldalakat látogatják –, és egyúttal szükségessége sem nyert bizonyítást, mivel a rendszer nehezen betartatható és kevéssé hatékony volt. A szabályozás egyéb buktatói már korábban kiderültek, így például az összegyűjtött és tárolt adatok védelmének nehézségei, hogy ahhoz illetéktelenek ne férjenek hozzá, illetve a rendszer fenntartásának magas költsége. (Ramstad, 2012)

5. Összefoglalás

Mint az előzőekben bemutattam, számos elképzelés létezik a kibertér szabályozásával kapcsolatos kérdésekben, egymástól különböző mértékű eltérésekkel. Két modell képe rajzolódik ki előttünk: a Nyugat által támogatott több érdekelt bevonásával működőé, valamint a Kína és Oroszország által forszírozott nemzeti szuverenitás alá rendelőé. Előbbi rendszerben az állam a keretet és a kényszerítőerőt biztosítja az internet biztonságában érdekeltek számára, míg a szabályozásban nagy teret kapnak az ágazat szereplői, valamint pontosan szabályozott a katonai felhasználás is. Utóbbi rendszerben az államhatalom monopóliummal bír az internetszabályozás minden kérdésében – különösen a tartalomszabályozásban –, a szolgáltatók és más szereplők pedig csupán a központi hatalom végrehajtóiként jelennek meg. Ezt a rendszert nevezik multilaterálisnak is, mivel az államok között kötött szerződéseken alapulnak a keretei, a katonai felhasználás pedig nem szabályozott vagy részben nem megengedett. (Eichensehr, 2015, p. 321) Mindkét szabályozásnak megvannak a maga előnyei és hátrányai, így például a több érdekelt bevonásával működő rendszer ugyan nagyobb információszabadságot biztosít, másrészről viszont a lobbitevékenység erősen érvényesül a kialakításában és a kiberbiztonság is sokkal nehezebben megvalósítható.

Ezen különbségek a nemzetközi dokumentumokban és diplomáciában is tetten érhetőek. A nemzeti szuverenitás alapú szabályozás pártján állók olyan megoldást támogatnak, amely a többnyire amerikai érdekeltségű nem kor-

mányzati szervek helyett a nemzetközi szervezeteknek – és így az azokban részes államoknak – biztosít nagyobb befolyást. Egy ilyen megoldás azonban elfogadhatatlan a másik modell követői számára, hiszen nem az együttműködésen alapul, hanem vertikális irányítást valósít meg. A 2001-es Budapesti Egyezmény számukra nemcsak a nyugati értékek támogatása miatt vonzó, de azért is, mert csak a szabályozás közös minimumát adja meg, annak kivitelezését pedig az egyes részes államok körébe utalja. Az Egyesült Államok és az Európai Unió folyamatos támogatásának köszönhetően az Egyezmény még sokáig az együttműködés alapját fogja képezni a nyugati államok között. Vagy, ahogy Ian Walden professzor fogalmazott Dublinban: ez marad Az Egyezmény.

Ezen indokok mellett az egyes államok politikai érdekeinek ismerete is fontos az eltérések megértéséhez. Ezek nemcsak aktuálpolitikai jellegűek, hanem mélyebben gyökereznek: egy pontos keretekkel rendelkező szabályozás nemcsak az érdekérvényesítő képességének korlátozása és a Five Eyes-hoz hasonló kezdeményezések megnehezítése miatt nem szimpatikus az Egyesült Államoknak, de az angolszász jogi tradícióknak megfelelő informális együttműködést is ellehetetlenítené. Ezzel szemben a minden érdekelt bevonásának megvalósítása kikezdené a CPC gondosan körbebástyázott hatalmát Kínában. Rajtuk kívül sok ingadozó állam is akad, például India, amely sokáig a nyugati elképzelést támogatta, de újabban szembefordult ezzel, ami jól tetten érhető az ITU puszani meghatalmazotti konferenciáján benyújtott javaslatukban. (Eichensehr, 2015, p. 335.)

A fentebb részletezett modellek azonban ritkán érvényesülnek tisztán. A nyugati demokratikus és autoriter megoldások sok területen – mint például a tartalomszűrés terén – lassú közeledést mutatnak egymáshoz, hiszen sok helyen az állami büntetőjogi igény érvényesítése céljából szélesebb körben alkalmazni kezdték az állami szűrést. (Parti, 2010, p. 99.) A felosztást árnyalja, hogy míg Kína mellett Nagy-Britannia is a kiberbűnözés elleni fellépést tekinti prioritásnak, addig a többi nyugati állam és Oroszország a kibertámadásokkal szembeni védekezést. (Levin – Ilkina, 2010, p. 35.)

Véleményem szerint ezen jogi és politikai okok miatt nem várható a közeljövőben konszenzus a két modell követői között, ugyanakkor a gyakorlat azt mutatja, hogy lassan zajlik az arra érdemesnek tartott megoldások átvétele

egymástól. Amíg a mostanihoz hasonló együttműködés van a modellek jelentős képviselői között, addig ez a folyamat biztosan folytatódni fog.

Irodalomjegyzék

Könyvek

WARREN, Peter – STREETER, Michael (2005): Az internet sötét oldala. Budapest, HVG. 256 p. ISBN 963-7525-815

Könyvrészletek

AUSTIN, Greg (2016) International Legal Norms in Cyberspace: Evolution of China's National Security Motivations. In: OSULA, Anna-Maria – RÕIGAS, Henry. International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn, NATO CCD COE. p. 171–201. ISBN 978-9949-9544-7-6

BRENNER, Susan W. (2011) Cybercrime Law – A United States Perspective. In: CASEY, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. USA, Academic Press. p. 85–122. ISBN 978-0-12-374268-1

CHALMERS, Damian (2014) Eu Criminal Law. In: CHALMERS, Damian – DAVIES, Gareth – MONTI, Giorgio. European Union Law: Cases and Materials. New York, Cambridge University Press. p. 581–629. ISBN 978-0-521-12151-4

DORNFELD, László (2015) A kiberbűncselemények szabályozásának története az Egyesült Államokban és Európában. In: SZABÓ Miklós. Studia Iurisprudentiae Doctorandorum Miskolciensium. Tomus 16. Miskolc, Gazdász-Elasztik Kft. p. 67–86. ISSN 1588-7901

PEERS, Steve (2011) EU Justice and Home Affairs Law. In CRAIG, Paul – DE BÚRCA, Gráinne. The Evolution of EU Law. New York, Oxford University Press. p. 269–298. ISBN 978-0-19-959296-5

SOFAER, Abraham D. – CLARK, David – DIFFIE, Whitfield (2010) Cyber Security and International Agreements. In: CLARK, David. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and

Developing Options for U.S. Policy. Washington D. C., The National Academies Press. p. 179–206. ISBN 978-0-309-16035-3

Folyóiratcikkek

BARTÓKI-GÖNCZY, Balázs (2014) Towards a Single Market for Telecoms. European Networks Law and Regulation Quarterly, 2. évf. 3. sz., p. 3–16. ISSN 2197-4454

BLYTHE, Stephen E. (2007) China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of e-Commerce. Chicago-Kent Journal of Intellectual Property, 7. évf. 2. sz., p. 1–32. ISSN 1559-9493

BORISEVICH, Galina – CHERNYADYEVA, Natalya – FROLOVICH, Evelina – PASTUKHOV, Pavel – POLYAKOVA, Svetlana – DOBROVLYANINA, Olga – GRIFFITH Keeling, Deborah – LOSAVI, Michael M. (2012): A Comparative Review of Cybercrime Law and Digital Forensics in Russia, the United States and Under the Convention on Cybercrime of the Council of Europe. Northern Kentucky Law Review, 39. évf. 2. sz., p. 267–326. ISSN 0198-8549

BUONO, Laviero (2012) Gearing Up the Fight Again Cybercrime in the European Union: A New Set of Rules and Establishment of the European Cybercrime Centre (EC3). New Journal of European Criminal Law, 4. évf. 3. sz., p. 332–343. ISSN 2032-2844

CROOK, John R. (2010) Secretary of State Addresses Human Rights and the Internet. The American Journal of International Law, 104. évf. 2. sz., p. 291–294. ISSN 0002-9300

DANCĂ, Dana (2015) Cyber Diplomacy – A New Component of Foreign Policy. Journal of Law and Administrative Sciences, 2. évf. 3. sz., p. 91–97. ISSN 2392-8298

EGEDY Gergely (2013) Brit kilépés? Polgári Szemle, 9. évf. 1–3. sz., ISSN 1786-6553

EICHENSEHR, Kristen E. (2015) The Cyber-Law of Nations. Georgetown Law Journal, 103. évf. 2. sz., p. 317–380.

ELLIS, Mark S. (2014) Losing Our Right to Privacy: How Far is Too Far? Birkbeck Law Review, 2. évf. 2. sz., p. 173–190. ISSN 2052-1316

ERDŐS István (2014) Az elektronikus kereskedelem hatása Az Európai Unió fogyasztói szerződésekkel kapcsolatos egyes joghatósági szabályainak alakulására. Iustum Aequum Salutare, 9. évf. 2. sz., p. 81–94. ISSN 1787-3223

FAHEY, E. (2014) The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security. European Journal of Risk Regulation, 5. évf. 1. sz., p. 46–60. ISSN 1867-299X

FISH, Eric (2009) Is Internet Censorship Compatible with Democracy? Legal Restrictions of Online Speech in South Korea. Asia-Pacific Journal on Human Rights and the Law, 10. évf. 2. sz., p. 43–96. ISSN 1388-1906

GAO, Henry (2011) Google's China Problem: A Case Study on Trade, Technology and Human Rights under the GATS. Asian Journal of WTO & International Health Law and Policy, 6. évf. 1. sz., p. 351–387. ISSN 1819-5164

HACHIGIAN, Nina (2001) China's Cyber-Strategy. Foreign Affairs, 80. évf. 2. sz., p. p. 118–133. ISSN 0015-7120

JENSEN, Eric Talbot (2015) Cyber Sovereignty: The Way Ahead. The Texas International Law Journal, 50. évf. 2. sz., p. 275–304. ISSN 0163-7479

LEE, Jyh-An – LIU, Ching-Yi (2012) Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China. Minnesota Journal of Law, Science & Technology, 13. évf. 1. sz. p. 125–151. ISSN 1552-9533

LEE, Jyh-An (2014) The Red Storm in Uncharted Waters: China and International Cyber Security. University of Missouri – Kansas City Law Review, 82. évf. 4. sz. p. 951–966. ISSN 0047-7575

LEHÓCZKI Balázs (2015) Európai Bíróság: Az Egyesült Államok „biztonságos kikötő" adatvédelmi rendszere nem biztosítja az uniós polgárok alapjogainak tiszteletben tartását. Acta Humana, 3. évf. 6. sz., p. 93–98. ISSN 0866-6628

LEITNER, John (2009) Identifying the Problem: Korea's Initial Experience with Mandatory Real Name Verification on Internet Portals. Journal of Korean Law, 9. évf. 4. sz., p. 83–85. ISSN 2213-4476

MCDOUGAL, Trevor (2015) Establishing Russia's Responsibility for Cyber-Crime Based on Its Hacker Culture. International Law & Management Review, 11. évf. 2. sz., p. 55-80. ISSN 1555-5070

MESTER Máté (2012) Hálózatsemlegesség az Európai Unióban: veszélyben az internet? Infokommunikáció és Jog, 9. évf. 51. sz., p. 149–154. ISSN 1786-0776

MOORE, Stephen (2013) Cyber Attacks and the Beginnings of an International Cyber Treaty. North Carolina Journal of International Law and Commercial Regulation, 39. évf. 1. sz., p. 224–257. ISSN 0743-1759

MUIR, Lawrence L. (2014) Combatting Cyber-Attacks Through National Interest Diplomacy: A Trilateral Treaty with Teeth. Washington and Lee Law Review Online, 71. évf. 1. sz., p. 73–106. ISSN 0043-0463

NULL, Eric (2011) The Difficulty with Regulating Network Neutrality. Cardozo Arts & Entertainment Law Journal, 29. évf. 2. sz., p. 459–493. ISSN 0736-7694

PARTI Katalin (2010) „10 dolog, amit utálok benned", avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán. Infokommunikáció és Jog, 7. évf. 38. sz., p. 97–103. ISSN 1786-0776

ROSENZWEIG, Paul (2012) The International Governance Framework for Cybersecurity. Canada-United States Law Journal, 37. évf. 2. sz., p. 405–414. ISSN 0163-6391

SIERS, Rhea (2014) North Korea: The Cyber Wild Card. Journal of Law & Cyber Warfare, 3. évf. 4. sz., p. 1–12.

SIPOS Zoltán (2016) A kibertér biztonságával kapcsolatos alapvető kérdések áttekintése. Honvédségi Szemle, 144. évf. 1. sz., p. 27–36. ISSN 1216-7436

WALDEN, Ian (2004) Harmonising Computer Crime Laws in Europe. European Journal of Crime, Criminal Law & Criminal Justice, 12. évf. 2. sz. p. 321–336. ISSN 0928-9569

WALTHALL, Howard (2010) The New Neutrality Debate: An IP Perspective. Landslide, 3. évf. 1. sz., p. 21–25. ISSN 1942-7239

ZHANG, Xinbao (2013) Establishing Common International Rules to Strengthen the Co-Operation of Cyber Information Security. China Legal Science, 12. évf. 1. sz., p. 121–139. ISSN 2095-4867

Elektronikus tartalmak

ACTIONPLAN (2011) Beyond the Border;

Letöltve: http://actionplan.gc.ca/en/content/beyond-border (Utolsó letöltés: 12/01/2015)

ASEAN (2008) EU-ASEAN Workshop on Cybercrime Legislation in the ASEAN Member States;

http://www.asean.org/uploads/archive/apris2_old/file_pdf/Press%20Releases/EU-ASEAN%20Workshop%20on%20Cybercrime%20Legislation%20in%20the%20ASEAN%20Member%20States.pdf (Utolsó letöltés: 14/06/2016)

BBC (2015) Theresa May says ‚contentious' parts of web surveillance plan dropped;
Letöltve: http://www.bbc.com/news/uk-34691956 (Utolsó letöltés: 19/02/2015)

CHINA INTERNET NETWORK INFORMATION CENTER (2015) Statistical Report on Internet Development in China;
Letöltve: http://www1.cnnic.cn/IDR/ReportDownloads/201507/P020150720486421654597.pdf (Utolsó letöltés: 04/01/2016)

CONGRESS (2016) H.R.275 – Global Online Freedom Act of 2007;
Letöltve: https://www.congress.gov/bill/110th-congress/house-bill/275/actions (Utolsó letöltés: 14/05/2016)

COUNCIL OF EUROPE (2016) Trainings on cybercrime and electronic evidence;
Letöltve: http://www.coe.int/en/web/cybercrime/trainings (Utolsó letöltés: 14/06/2016)

DICKINSON, Samantha (2014) How will internet governance change after the ITU conference?
Letöltve: http://www.theguardian.com/technology/2014/nov/07/how-will-internet-governance-change-after-the-itu-conference (Utolsó letöltés: 04/03/2016)

ELECTRONIC EVIDENCE (2016) Electronic Evidence Guide;
Letöltve: http://ic4mf.org/wp-content/uploads/2013/11/2ndDay-p08-2013-11-07-COE-Electronic-Evidence-Guide-IC4MF.pdf (Utolsó letöltés: 12/06/2016)

EUROPOL (2014) Joint Cybercrime Action Taskforce (J-CAT)
Letöltve: https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat (Utolsó letöltés: 15/01/2016)

EUROSTAT (2015) Information society statistics – households and individuals;
Letöltve: http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals (Utolsó letöltés: 10/01/2016)

FIDLER, David P. (2012) The Internet, Human Rights, and U.S. Foreign Policy: The Global Online Freedom Act of 2012;

Letöltve: https://www.asil.org/insights/volume/16/issue/18/internet-human-rights-and-us-foreign-policy-global-online-freedom-act (Utolsó letöltés: 29/02/2016)

GADY, Franz-Stefan (2014) The Wuzhen Summit and Chinese Internet Sovereignty;

Letöltve: http://www.chinausfocus.com/peace-security/the-wuzhen-summit-and-chinese-internet-sovereignty/ (Utolsó letöltés: 10/06/2016)

GADY, Franz-Stefan (2015) Have China and Russia Agreed Not to Attack Each Other in Cyberspace?;

Letöltve: http://thediplomat.com/2015/05/have-china-and-russia-agreed-not-to-attack-each-other-in-cyberspace/ (Utolsó letöltés: 10/06/2016)

GOV.UK (2011) US – UK cyber communique; Letöltve: https://www.gov.uk/government/publications/us-uk-cyber-communique (Utolsó letöltés: 04/03/2016)

GOVTRACK (2016) H.R. 275 (110th): Global Online Freedom Act of 2007;

Letöltve: https://www.govtrack.us/congress/bills/110/hr275 (Utolsó letötés: 14/05/2016)

GRISBY, Alex (2015) Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?

Letöltve: http://blogs.cfr.org/cyber/2015/01/28/will-china-and-russias-updated-code-of-conduct-get-more-traction-in-a-post-snowden-era/ (Utolsó letöltés: 10/06/2016)

HOMELAND SECURITY (2011) United States and India Sign Cybersecurity Agreement;

Letöltve: https://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement (Utolsó letöltés: 12/01/2016)

INTERNET GOVERNANCE (2012) ITU Phobia: Why WCIT was derailed;

Letöltve: http://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/ (Utolsó letöltés: 28/02/2016)

INTERNET SOCIETY (2011) Background: International Telecommunication Regulations

Letöltve: http://www.internetsociety.org/background-international-telecommunication-regulations (Utolsó letöltés: 21/02/2016)

JONG-CHEN, Jing de (2015) Spotlight on Cyber V: Data Sovereignty, Cybersecurity and Challenges for Globalization;
Letöltve: http://journal.georgetown.edu/data-sovereignty-cybersecurity-and-challenges-for-globalization/ (Utolsó letöltés: 15/01/2016)
KULIKOVA, Alexandra (2015) China-Russia Cyber-security Pact: Should the US be Concerned?;
Letöltve: http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned (Utolsó letöltés: 04/03/2016)
LAKNER Dávid (2016) Amit az üzenőfal elbír – Cenzorszerepben a Facebook?;
Letöltve: http://mno.hu/media/amit-az-uzenofal-elbir-cenzorszerepben-a-facebook-1345499 (Utolsó letöltés: 12/06/2016)
LAMUT, Anna (2008) Third Circuit Holds Child Online Protection Act Unconstitutional;
Letöltve: http://jolt.law.harvard.edu/digest/internet/aclu-v-mukasey (Utolsó letöltés: 12/06/2016)
LEVIN, Avner – ILKINA, Daria (2013) International Comparison of Cyber Crime; Letöltve: http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf (Utolsó letöltés: 10/01/2016)
NPR (2016) U.S. Appeals Court Upholds Net Neutrality Rules In Full;
Letöltve: http://www.npr.org/sections/thetwo-way/2016/06/14/471286113/u-s-appeals-court-holds-up-net-neutrality-rules-in-full (Utolsó letöltés: 15/06/2016)
POPESCU, Adam (2012) 5 Reasons Why The U.S. Rejected The ITU Treaty
Letöltve: http://readwrite.com/2012/12/14/5-reasons-why-the-us-rejected-the-itu-treaty (Utolsó letöltés: 02/03/2016)
PRICE, Rob (2015) The European Parliament just dealt a major blow to net neutrality.
Letöltve: http://www.businessinsider.com/european-parliament-net-neutrality-vote-2015-10 (Utolsó letöltés: 05/03/2016)
PROJECT CYBERCRIME (2014) Cybercrime Model Laws;
Letöltve: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf (Utolsó letöltés: 14/06/2016)

SASSO, Brendan (2012) House to examine plan for United Nations to regulate the Internet;
Letöltve: http://thehill.com/policy/technology/229653-house-to-examine-plan-to-let-un-regulate-internet (Utolsó letöltés: 02/03/2016)
SULLIVAN, Clare (2014) Cybersecurity and the ANZUS Treaty: The Issue of U.S.-Australian Retaliation;
Letöltve: http://journal.georgetown.edu/cybersecurity-and-the-anzus-treaty-the-issue-of-u-s-australian-retaliation/ (Utolsó letöltés: 10/01/2016)
RAMSTAD, Evan (2012) South Korea Court Knocks Down Online Real-Name Rule;
Letöltve: http://www.wsj.com/articles/SB10000872396390444082904577606794167615620 (Utolsó letöltés: 30/01/2016)
ROTH, Andrew (2015) Russia and China Sign Cooperation Pacts;
Letöltve: http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=1 (Utolsó letöltés: 10/06/2016)
WHITE HOUSE (2011) International Strategy for Cyberspace;
Letöltve: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Utolsó letöltés: 10/01/2016)
WHITE HOUSE (2013) Cybersecurity — Executive Order 13636;
Letöltve: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636 (Utolsó letöltés: 12/06/2016)
WHITE HOUSE STATEMENT (2015) Joint Statement: 2015 United States--India Cyber Dialogue;
Letöltve: https://www.whitehouse.gov/the-press-office/2015/08/14/joint-statement-2015-united-states-india-cyber-dialogue (Utolsó letöltés: 10/01/2016)
WHITE HOUSE FACT SHEET (2015) FACT SHEET: President Xi Jinping's State Visit to the United States;
Letöltve: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (Utolsó letöltés: 10/06/2016)
Wiley Rein (2013) Combating Cyber-Terrorism: President Issues Executive Order on Improving Critical Infrastructure Cybersecurity;
Letöltve: http://www.wileyrein.com/newsroom-articles-2621.html (Utolsó letöltés: 10/06/2016)

WSIS (2003) Final Report of the Geneva Phase of the Summit WSIS-03/GENEVA/DOC/0009 (rev. 1);
Letöltve: http://www.itu.int/net/wsis/documents/listing.asp?lang=en&c_event=s|1&c_type=o| (Utolsó letöltés: 28/04/2016)

Keleti Arthur
(keleti.arthur@itbn.hu)

A kibertér biztonságának egyes aspektusai

Általános tanulmány a kiberbiztonság jelenlegi helyzetéről, a SOC-ok és a Threat Intelligence szerepéről a kibertér nemzeti és üzleti védelmében

Absztrakt

A tanulmány azzal a céllal készült, hogy bemutassa a kibervédelem jelenlegi helyzetét, azt, hogy a világban az államok és magánszervezetnek mit tehetnek vagy tesznek annak érdekében, hogy a status quon javítsanak vagy jobban irányításuk alatt tarthassák illetve, hogy milyen eszközöket használnak és milyen lehetőségek és mozgástér áll rendelkezésre a további fejlesztésekre. A tanulmánynak nem célja a témában jártas biztonsági szakembereknek részletes műszaki tanácsokkal szolgálni, igyekszik inkább áttekintő útmutatást adni a geopolitikai összefüggések és hosszú távú stratégia iránt érdeklődő szakembereknek és laikusoknak.

A világban az egyik legfontosabb tényező jelenleg a kiberbiztonság. Ennek hiánya évente több mint 400 milliárd dollár kárt okoz és világviszonylatban sok milliárd dollárt költenek a kár enyhítésére. Még mindig sok probléma van a biztonsági rendszerekkel, melyeket a szakemberek próbálnak beazonosítani és befoltozni. A kiberbiztonsági szakemberek csapatokba és központokba történő szervezése és a SOC létrehozása nemzeti és vállalati szinten fontos feladattá vált. Az ilyen központ minden szervezetnél létfontosságú, nagy mennyiségű technológia és emberierőforrás beruházásra van szükség hozzá és érdemes kiegészíteni Threat Intelligence-szel is. Az új technológiák oldalán figyelemre méltóak a Behavior Based Cyber Security megoldások is.

Kulcsszavak: kibervédelem, kiberbiztonság, biztonsági rendszerek

Abstract

The objective of this chapter of the study was the introduction of the present status of cyber security. What nation states and private companies of the World are doing to develop or take status quo better under their control, what tools are used in the process and what possibilities and room they have for further development. Giving deep technical advice to battle hardened cyber security professionals is not aim of this study, it however provides a general overlook for pros and non-pros interested in contexts of geopolitics.

One of the most important factors of the World today is cyber security. The lack of it causes an annual 400 billion us dollars damage and many billions of dollars are spent on mitigating that damage worldwide. Problems of security systems are present and an ongoing work of security professionals to identify and patch them is a daily task. Grouping cyber security pros, organize them into centers and the making of SOCs is a top level priority of nations and companies. Such a center is vital to organizations, it requires big technological and human resource investment and it is highly advisable to extend it with Threat Intelligence. On the side of new technologies Behavior Based Cyber Security solutions are worth to keep an eye on.

Keywords: cyber security, security systems

1. Bevezető

Jelenlegi tanulmányfejezet azzal a céllal készült, hogy bemutassa a kibervédelem jelenlegi helyzetét, azt, hogy a világban az államok és magánszervezetnek mit tehetnek vagy tesznek annak érdekében, hogy a status quon javítsanak vagy jobban irányításuk alatt tarthassák illetve, hogy milyen eszközöket használnak és milyen lehetőségük és mozgásterük áll rendelkezésre a további fejlesztésekre.

A tanulmánynak nem célja a kibervédelemben mélyen jártas biztonsági szakembereknek részletes műszaki tanácsokkal szolgálni, igyekszik inkább áttekintő útmutatást adni a geopolitikai összefüggések és hosszútávú stratégia iránt érdeklődő szakembereknek és laikusoknak.

A kérdéskör feldolgozásakor az anyag az alábbi struktúrát és tematikát követi:

1. Elsőnek a jelenlegi probléma bemutatásával, a kibertámadások számával, a támadók kilétének és motivációjának sokféleségével, a bonyolult állami és céges folyamatokkal, a nagy adatmennyiséggel és a lassú reakcióidőkkel foglalkozunk.
2. A második szakaszban a fenti probléma megoldására tett erőfeszítések logikájába tekintünk bele a kiberbiztonsági képességek érettségi modelljén (https://www.sbs.ox.ac.uk, 2014), a kiberbiztonsági kapacitások építésén, a Security Operations Center (SOC) felállításán, a Threat Intelligence megoldások igénybevételén és a viselkedés alapú megoldások lehetőségeinek (https://techcrunch.com, 2015) bemutatásán keresztül.
   a) Kiberbiztonsági kapacitások modelljét határozzák meg és
   b) Építenek kapacitást (Az egyes országoknak milyen kiberkapacitásuk van jelenleg, mennyit költenek és főleg mire?)
   c) SOC-ok építése (Mi az, miért van? stb.)
   d) Threat Intelligence igénybe vétele és gyártása (Mi az, miért van? Fő szereplők Cisco, FireEye, TrendMicro, Checkpoint, RSA stb.)
   e) Rövid kitekintés a viselkedés alapú megfigyelési technikákra (Behaviour Based Cyber Security)
3. Az utolsó részben pedig összefoglaljuk a tanulságokat, megállapításokat teszünk és levonjuk a megfelelő konklúziókat.

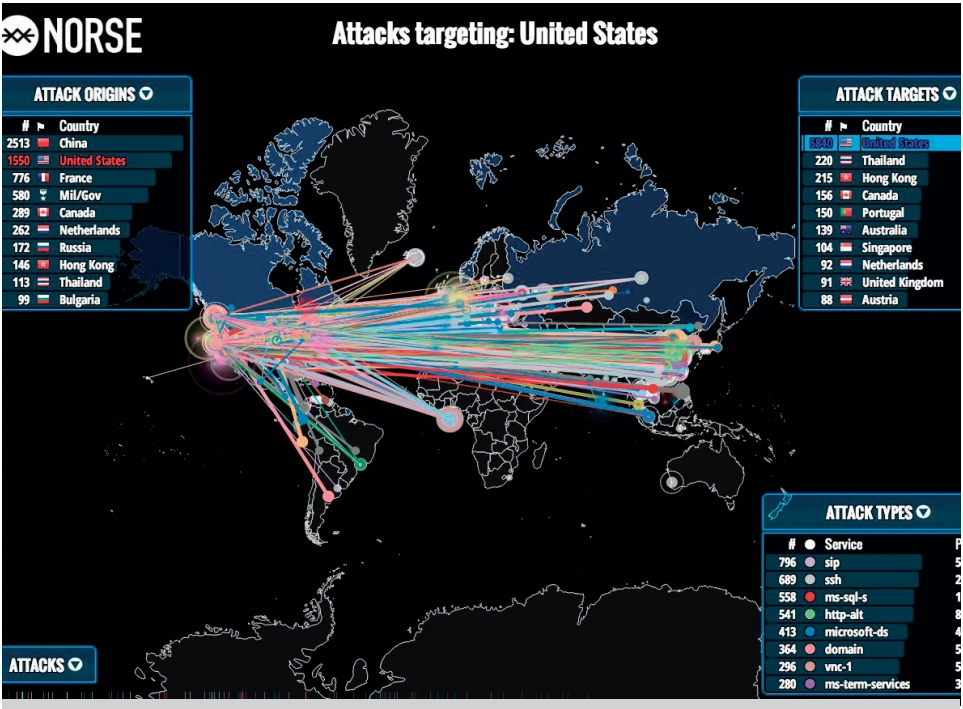
2. Jelenlegi állapot

A nemzetközi és azon belül a magyar kibervédelem nincs sokkal jobb helyzetben, mint a 16. századi európai végvárrendszer: kevés az ember, kevés a pénz és sok a támadó. Ráadásul a védelmi rendszer gyakran elavult, sok helyen lehetnek rések, gyakran azt sem feltétlenül vesszük észre, ami a saját kertünkben zajlik. A globális trendek azt mutatják, hogy a jó szakember ritka mint a fehér holló, az USA-ban például csak 2015-ben több mint 200.000 kiberbiztonsági szakértő állása maradt betöltetlen (www.csoonline.com, 2015), de Magyarországon is hiány van jó informatikai és kiberbiztonsági szakemberekből (www2.deloitte.com, 2016). A cégek gyakran csak azért tartanak fenn kibervédelmi részleget, hogy a belső irányelveknek megfeleljenek és a kliensek által elvárt "biztonságot" megteremtsék, de nem mindig fakad ez belső indíttatásból vagy kellő biztonságtudatból.

A dark weben (amely az internetről egy TOR böngészővel bárki számára elfogadható anonimitást biztosítva elérhető) bárki vehet magának egy-egy hackert vagy bármilyen adatot, csak pénz kérdése a dolog, például 65 millió Tumblr jelszó csak 0.4255 BTC (Bitcoin) ($150) (Deepdotweb, 2016) vagy egy 379 millió bejegyzést tartalmazó adatbázis, amiből 33 millió Twitter jelszó, csupán 10 BTC ($5800) (Mashable, 2016). Az országok dollármilliárdokat (az USA 2017-es költségvetésében 6.7 milliárd dollárt irányoztak elő kiberműveltekre) (www.militaryaerospace.com, 2016) költenek az egymás elleni kiberháborúra, az IT cégek azért hogy a riválisuk előtt járhassanak, bármilyen eszközt bevetnek. Jelenleg a kibertér egy virtuális vadnyugat, ahol lehet fegyver vagy védelem nélkül járkálni, de nem érdemes.

A támadók nagyságrendileg vannak előnyben a védőkkel szemben, míg egy hacker pontosan tudja, mit keres, a védelmi szakembereknek tengernyi adatot kell átfésülniük hogy megtalálják a behatolók nyomát és elhárítsák a fenyegetést. Egy SOC (Security Operations Center) kiépítése és fenntartása cégenként felettébb költséges és az embererő igények miatt könnyedén lehet fenntarthatatlan. A költségek optimalizálása és a szakemberhiány kompenzálása indokolja, hogy a szolgáltatásokat kívülről vásárolják meg a cégek, ezért számtalan szolgáltató van, akik különféle SIM-SIEM (Security information management – Security information and Event Management) szolgál-

(Forrás: map.ipviking.com,2016)

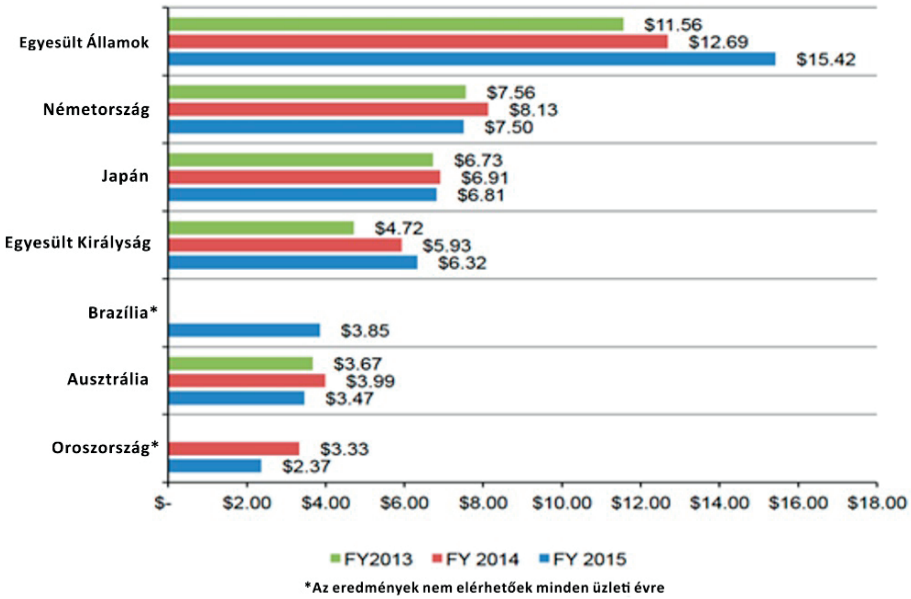


A fenti képen egy threat map látható, amely azt mutatja, hogy mely országokból mely országok felé indulnak az aktuális pillanatban kibertámadások. Ezek azok a támadások, amelyeket az adott szolgáltató rendszere aktuálisan érzékel. Szakmai körökben több kritika érte az ehhez hasonló threat map-eket, mivel nyilvánvalóan nem adnak pontos és akkurátus információt a támadásokról. Ugyanakkor a kiberbiztonsági szakemberek a biztonsággal kapcsolatos legnagyobb problémája a helyzet vizualizációja a releváns döntéshozók számára. Ezt a feladatot tökéletesen ellátja a térkép, mint ahogy konkrétan országokra vagy akár iparági csoportokra leszűrve pedig részletesebb információt is ad, ezért nem ritkán használják SOC-központokban is vagy szakmai bemutatókon.

tatásokat kínálnak (lásd később). De ez nem csak a vállalatokat érintheti. Észtország 2016 nyarán úgy döntött, hogy Angliában helyezi el kormányzati szervereit, mert tart az orosz hackerek támadásaitól (www.ft.com, 2016).

Az „IBM Security Services Cyber Security Intelligence Index," ami 3,700 IBM-kliens részletes analízisét és kiberbiztonsági eseményeit írja le 130 ország-

Ábra 1. A kiberbűnözés összköltsége hét országban
A költségek amerikai dollárban kerültek feltüntetésre (000,000), n = 252 különböző cég



(Forrás: Ponemon Institute: 2015 Cost of Cyber Crime Study: Global, 2015)

A cégeknek egyre több és drágább kihívással kell szembenézni, amint az a fenti ábrából is látható. Hogy jobb áttekintést kapjunk, vizsgáljuk meg a sikeres támadások számát.

2015: 477 támadás 252 szervezetben, avagy 1.9 sikeres támadás cégenként mindent héten

2014: 429 támadás 257 szervezetben, avagy 1.7 sikeres támadás cégenként mindent héten

2013: 343 támadás 234 szervezetben, avagy 1.4 sikeres támadás cégenként mindent héten

2012: 262 támadás 199 szervezetben, avagy 1.3 sikeres támadás cégenként mindent héten

(További értékek és táblázatok: Ponemon Institute© Research Report, 2015 Cost of Cyber Crime Study: Global Benchmark Study of Global Companies Ponemon Institute October 2015.) Ezért van szüksége a cégeknek sokkal alaposabb megközelítésre rendszereik megvédéséhez.

ból, 2012-ben 137,4 millió incidenst említ, amikor valami kártékony tevékenység megpróbált információs rendszereket és adatot ellopni, megzavarni, működés képtelenné tenni vagy elpusztítani. Ez 2.6 millió támadás minden héten, és 0,38 millió minden nap. Ezek közül egymillióból 1,07 volt sikeres. Hogy ezek a támadások mennyi kárt okoztak? A Ponemon Institute becslései alapján egy szervezeti adatbiztonsági incidens átlagban fájlonként 188 dollárba kerül, összesen így 5,4 millió dollárt vesztettek a cégek. De a közvetett költségek és a további implikációk költségei még ennél is magasabbak; egy cég reputációja nagyjából 21%-ot zuhan egy-egy sikeres támadás során, amikor a támadók ügyféladatokat is megszereznek. Ez összesen átlagosan 332 millió dollárt jelent állományonként. A támadások száma az elmúlt 4 évben lényegesen nőtt és az ellopott adatok mennyisége is nagyságrendeket ugrott, a támadások sebességéről nem is beszélve (a 2016-os Anonymous hacker csoport támadásában a Fülöp-szigetek választási rendszere ellen 55 millió választó adatát lopták el és tették közzé órák alatt) (www.hackread.com, 2016), tehát ez az összeg a helyzettől függően 2016-ban már ennek többszöröse is lehet.

3. A probléma megoldása

Az országok és vállalatok döntéshozóinak komoly kihívást jelent a kiberbiztonság kérdése. Egy láthatatlan csatatérbe kell dollármilliókat invesztálniuk, amelynek elég kétes a megtérülése. Milyen opciói vannak tehát annak, aki biztonságban szeretné tudni az állampolgári vagy szervezeti adatait? Az információmegosztásban az, hogy minden cég minden titkát, adatát publikusan elérhetővé tegyen – effektíve nyílt lapokkal játssza –, egy ilyen szinten kompetitív szférában öngyilkossággal érne fel. Tehát a „nekem nincs semmi titkom, nem árthatnak nekem" mint általános irányelv nem állja meg a helyét. Ugyanígy a „kétszer nem csap ugyanoda a villám" sem igaz. A kibertámadások jelentős része nem pillanatszerű, nem egy-egy specifikus dolog az, ami kell a támadóknak, hanem időben hosszan elnyújtott folyamat. Ha egyszer bejutottak egy rendszerbe azok, akiknek nem a károkozás a célja, hónapokig, évekig bujkálhatnak a háttérszervereken, és közben felbecsülhetetlen mennyiségű és értékű adatot bányásznak ki. Még 2016-ban is az átlagos rendszerben

maradó „lappangási ideje" a hackereknek anélkül, hogy észre vennék őket, átlagosan 200 nap (blogs.microsoft.com, 2016).

Hogy biztonságban legyenek az adataink, egy-egy védelmi technológia (pl. tűzfal vagy antivirus) vajmi kevés védelmet nyújt. Több megoldás vagy szolgáltató kombinált szolgáltatásainak fenntartása jár bizonyos előnyökkel, például esetlegesen két nem teljesen azonos adatbázisból dolgoznak vagy eltérő ország és információhátterük van (mint pl. az orosz Kaspersky, a japán TrendMicro vagy az amerikai Intel Security), tehát nagyobb spektrumot fednek le, például Kelet-Európából is érdemes orosz és kínai szolgáltatókat igénybe venni, mivel azok a saját régiójuk tipikus fenyegetéseit jobban ismerhetik, mint egy nyugati szolgáltató. Ugyanakkor különböző fejlesztők szoftvereit összehangolni, karbantartani, a kapott eredményeket értelmezni hihetetlenül nehéz. Egy nagyvállalat szó szerint milliónyi eseményt generál percenként, ráadásul sok esetben ütköző funkciókat tartalmaznak, aminél szükséges egyes dolgok kikapcsolása, az ideális beállítástól való eltérés, ergo biztonsági rések szándékolt bent hagyása a rendszerben. Sajnos általános tapasztalat, hogy ezek a kockázatokat jelentő beállítások komolyan gyengítik a rendszerek védelmét.

Hogy ezeket elkerülhessük, ajánlott egy a feljebb már említett Security Operations Center (SOC) kiépítése vagy pedig egy MSSP (Managed Security Service Provider) szolgáltatás igénybevétele.

3.1. Kiberbiztonsági képességek érettségének meghatározása

Az alábbi rendszert az oxfordi Global Cyber Security Capacity Center dolgozta ki azzal a céllal, hogy egy jól meghatározható formában lehessen besorolni a cégeket és országokat az alapján hogy a lehetőségeikhez képest milyen szinten állnak kiberbiztonsági képességek és kapacitások szempontjából. Öt dimenzió alapján mérik a képességeket, minden egyes dimenzión belül számos további faktor található.

A kiberbiztonság öt dimenziója, ami ma meghatározza a képességeket és kapacitásokat:

1. Kiberpolicyk és stratégiák szintje
2. A társadalmon belüli felelős kiberkultúra színvonala
3. A kibertudatosság az egyszerű dolgozótól a vezetőkig

4. Jogi szabályozás hatékonysága
5. A kockázatok korlátozása szabályozással, standardizálással és technológiával

Ezek alapján besorolható az ország egy úgynevezett cyber security capability maturity modellbe, ahol a legalacsonyabb szint azt jelenti, hogy gyakorlatilag nincsenek kiberbiztonsági kapacitások, a legmagasabb pedig, hogy minden elképzelhető eszköz és tudás rendelkezésre áll.

3.1.1 Az egyes szintek:

- Start-up: ezen a szinten nagyjából semmi nem létezik még, vagy még csak embrionális állapotban, esetleg tervek szintjén.
- Formálódó: néhány dolog már elkezdett kialakulni, de gyakran ad-hoc, rosszul definiált és szervezetlen.
- Kialakult: a védelem elemei a helyükön vannak és működik is, de még kiegyensúlyozatlan, esetleges az erőforrások eloszlása.
- Stratégiai: már eldöntött, hogy mi mennyire fontos, mire mekkora erőforrásokat allokálnak.
- Dinamikus: tisztán látható stratégia van arra, hogy az erőforrásokat bizonyos helyzetekben hogyan csoportosítsák át, a döntéshozás gyors, és folyamatos a környezet megfigyelése.

3.1.2.Kategóriák, ami alapján a szervezet besorolható:

1. Dimenzió
   a) Nemzeti kiberbiztonsági stratégia: milyen szinten és milyen mélységben került kidolgozásra, milyen forrásokkal rendelkezik, mennyire rugalmas.
   b) Incidens válasz: hogyan, milyen gyorsan, milyen eszközökkel történik.
   c) Kritikus nemzeti infrastruktúra védelem: mit, milyen erővel és hogyan védenek.
   d) Krízis menedzsment: mik az akciótervek, hogyan mérik fel a krízis nagyságát, hogyan reagálnak.
   e) Kibervédelmi megfontolások.
   f) Digitális redundancia: mennyire optimalizált a rendszer, vannak-e olyan részei amik ugyanazt a feladatot végzik.

2. Dimenzió
   a) Kiberbiztonsági mind-set: milyen az emberek hozzáállása a kiberfenyegetésekhez.
   b) Tudatosság: mennyire vannak az emberek tisztában a fenyegetéssel.
   c) Bizalom az internetben: mennyire bíznak az emberek az online szolgáltatásokban.
   d) Online magánélet: mennyire fontos, és mit tesznek a megőrzése érdekében.

3. Dimenzió
   a) Nemzetileg elérhető kiberoktatás: mit tesz az állam, hogy a polgárai ismerjék a veszélyeket
   b) A kiberoktatás központi fejlesztése: van-e elég szakértő oktató, ha nincs, tervezik-e orvosolni a hiányt, tanterv fejlesztése.
   c) Céges képzések, a cégek bevonása az oktatásba: vannak-e ilyen tervek vagy már folyamatban lévő programok.
   d) Vezetők hozzáértése: mennyire vannak tisztában a cégek döntéshozói a kiberfenyegetésekkel.

4. Dimenzó
   a) Kiberbiztonság jogi keretei: jogi környezet kialakítása, ennek a színvonala.
   b) Törvényes vizsgálatok: vannak-e a rendfenntartó szerveknek emberei arra hogy fellépjenek a kiberbűnözők ellen és betartassák a szabályokat, a bíróságok értenek-e a témához annyira, hogy releváns döntést hozzanak.
   c) Felelősségteljes közzététel: hogyan szabályozott az adatok, sérülékenységek kiadása, kezelése.

5. Dimenzió
   a) Ragaszkodás a standardekhez: a kötelező folyamatok lefektetése, betartása.
   b) A nemzeti infrastruktúra rugalmassága: új technológiák beszerzése és integrálása a már meglévő rendszerekbe lehetséges-e.

c) Kiberbiztonsági piac: milyen forrásból szerzik be a biztonsági technológiákat, milyen időnként frissítik azokat, esetleg adnak-e el másnak technológiákat.

3.2. Kiberbiztonság Struktúrája és működése

A kiberhadviselés mára bevált módja annak, ha egy országot vagy céget akar valaki „büntetlenül" támadni. A kibertámadások többségükben lekövethetetlenek, maximum következtetni lehet a károkozó kódjának mintázatából és stílusából, hogy vajon ki lehetett a támadó és mi lehetett a célja. A komolyabb támadásokban használt eszközök újfajta elnevezése APT (Advanced Persistent Threat), olyan megoldások ezek, amelyek általában sokáig észrevétlenül dolgoznak egy-egy rendszerben, adatokat szivárogtatnak egy távoli megfigyelőhöz, esetleg később komoly károkat okoznak közvetlenül az adott rendszernek.

Az APT-k célja gyakran „csak" adatlopás, ipari kémkedés, szabotázs, néha viszont a hagyományos hadviselés kiegészítőjeként tekintenek rá. Például a továbbra is tartó orosz-ukrán konfliktus során, a történelem során először ismerte el az USA kormánya dokumentáltan, hogy véleménye szerint valakinek sikerült egy másik ország energiaellátását kizárólag kibertámadásokkal összeomlasztani. (www.reuters.com, 2016). A feltételezhetően orosz támadás következtében 2015. december 23-án 225.000 fogyasztó maradt áram nélkül Nyugat-Ukrajnában. A támadók távolról átkapcsolták a biztosítékokat egy malware segítségével, majd az ügyfélszolgálatokat telefonhívásspammel blokkolták, elmélyítve a krízist.

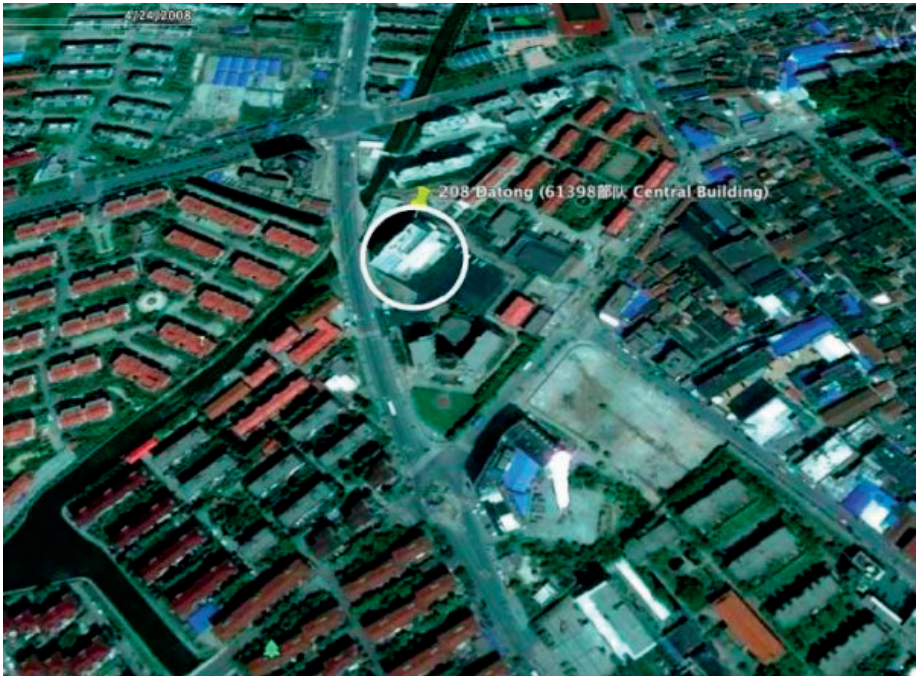
A kiberhadviselésben talán az a legszörnyűbb, hogy csak nagyon körülményesen köthetőek nemzetközi határozatokhoz, általános világelvekhez, ezért sokszor a hackerek és a megbízóik „lelkiismerete" szabhat határt, amely egy hadviselésben nehezen kezelhető elem. „Ma nem létezik olyan nemzetközi álláspont vagy keretrendszer, amely kötelező érvényű lenne bármelyik nemzetállam számára az offenzív kiberbiztonsági műveletek tekintetében." („There is no international standing or framework that is binding over any one nation-state in terms of offensive cyber operations,") – Bradley P. Moss nemzetbiztonsági ügyvéd nyilatkozta a Tech Insidernek májusban. „Bármilyen szabály,

amit magunknak határozunk meg." („It's whatever rules we put in place for ourselves.") (www.techinsider.io, 2016)

Bár az USA és Kína elviekben kötött egy megállapodást (www.nytimes.com, 2015), nevezhetjük kölcsönös kiber megnem támadási szerződésnek, ezt azóta is mindkét fél felrúgja (www.engadget.com, 2015), éppen azért mert rendkívül nehéz – ha nem lehetetlen – 100%-os bizonyossággal megállapítani a támadó személyét/országát. A nagy kiberbiztonsági vállalatok, mint a FireEye-Mandiant, Crowdstrike, Kaspersky Lab, vagy a Symantec gyakran ki tudnak deríteni mélyebb információkat, neveket, csoportokat és hogy valószínűleg ki áll a támadás hátterében, de ez messze nem elég a nemzetközi politikában.

Kik a kiberháború fő játékosai?

Egyértelműen **Kína** áll a kiberhadviselés élén. A kínaiaknak van a világon a legjobban szabályozott internete, fizetett cenzorok szabályozzák a lakos-



(http://edition.cnn.com, 2014)

ságot és a Kínai Néphadsereg kötelékében több tízezer hivatásos hacker szolgál. Nehéz felbecsülni a pontos számukat a fenti képen látható épületben; vélhetően legalább 1000 szerver szolgál ki 2000 hackert, ezt a csoportot úgy ismeri a világ hogy PLA unit 61398, más neveken „UglyGorilla," „KandyGoo", „WinXYHappy". Ez a hatékonyan működő csoport 2014 nyaráig több száz terabyte-nyi adatot lopott el legalább 141 szervezettől (pl. Coca-Cola, RSA Security és az USA kritikus infrastuktúrái) 20 iparágból 2006 óta. (edition.cnn.com, 2014)

Becslések szerint legalább 20 (BBC CIKK LD FELJEBB), de akár 50 ilyen csoport (www.techinsider.io, 2016) is működhet az országban. Pontos azonosításukat nehezíti, hogy vannak a katonaság szervezetén belül működő csoportok, katonai felhatalmazással működő kormányzati szerveknek dolgozó csoportok és vannak nem kormányzati csoportok, akik az épp aktuális érdekeik szerint cselekszenek.

Fontos játékos még **Oroszország** is. A putyini Oroszországban szintén erős az internet irányításának vágya, és az agresszív külpolitikai lépéseket gyakran támogatják meg például a fentebb említett kibertámadásokkal. Az ismételten nagyhatalmi ambíciókat dédelgető Oroszország egyre aktívabban vesz részt a világpolitikában, például aktívan befolyásolja az amerikai elnökválasztást (www.theguardian.com, 2016). Trump pedig beszédben szólította fel az oroszokat, hogy találjanak meg politikai ellenfele, Hillary Clinton által letörölt emaileket (www.nytimes.com, 2016). Az elmondottakat később úgy finomította, hogy csak szarkasztikus szeretett volna lenni, de észlelhető, hogy Trump politikája alapvetően összhangban áll az orosz törekvésekkel.

Az **USA** jelentősen lemaradt a kiberfegyverkezési versenyben. Egy, a Business Insidernek adott riport során John McAfee, az extravaganciája miatt sokat bírált, de tagadhatatlanul professzionális biztonságtechnikai szakértő azt nyilatkozta, hogy „Kínának, Oroszországnak, sőt még Iránnak is megvan a képessége arra, hogy szó szerint visszaküldjön minket a kőkorszakba".

„Egy kiberháború közepén vagyunk, ami nem közelít, nem feldereng a horizonton, hanem már itt van. És úgy tűnik, a kormányzatunkból ezt senki nem érti meg. Ha megértenék, akkor a kínaiak nem lettek volna képesek ellopni 21 millió adatot mindenkiről, aki az amerikai kormánynak dolgozott az elmúlt 50 évben."

McAfee szerint az oroszok és a kínaiak abban járnak Amerika előtt, hogy míg az USA-ban a hackereket ellenségként kezelik, addig Kínában és Oroszországban kormányzati állást ajánlanak nekik. Ezek az emberek kiemelkedően jók a saját területükön, és okosabbak mint az átlag kibervédelmi szakember.

„Olyan sokáig voltunk a világ vezető hatalma, hogy elképzelhetetlennek tartjuk, hogy Amerika csúnyán le legyen maradva a világ mögött egy olyan tudományágban, ami végtelenszer erősebb, mint az összes atombombánk és csatahajónk együttvéve. Elvakítanak a történelmi sikereink."

Természetesen az USA is hatalmas forrásokat csoportosít át kibervédelmi feladatokra, de bizonyos részei a katonai számítástechnikai struktúrának megbocsájthatatlanul elavultak (szokatlan, de érdekes példája ennek, hogy még mindig floppy diszkek vezérelik a nukleáris kilövő rendszert) (www.bbc.com, 2016).

Fontos tényezők még a kiberhadviselésben **Észak- és Dél-Korea**. Észak-Koreának nagyjából 6000 katonája teljesít szolgálatot a kiberfronton és az ország általános számítástechnikai fejletlenségéhez képest kiemelkedően jól teljesítenek (a Sony Pictures 2014-es feltörését, amely állítólag 100 terrabyte mennyiségű adat ellopásával járt is hozzájuk kötik) (www.businessinsider.com, 2014). Továbbá megvan az az előnyük mindenki mással szemben, hogy míg a támadó képességeik a legjobbak közé tartoznak, maga az ország közel sebezhetetlen, mivel az infrastruktúrájuk nincs központosítva és általánosan is nagyon alacsony az internethozzáférés.

Dél-Korea ennek nagyjából az ellentette; az ország technológiailag az egyik legfejlettebb a világon, minden központilag vezérelt, ergo erősen sérülékeny a kibertámadásokkal szemben. Hogy ezt problémát kezeljék a dél-koreaiak azt a módszert választották, hogy az amúgy is kötelező sorkatonaságot az állampolgárok letölthetik katonai kiberszakemberként is, ami egy vonzó életpálya, mert a hazafias érzelmek mellett a techorientált országban a karrierépítést is elősegíti. Az északiaknál kicsit kevesebb, kb. 5500 fős kibervédelmi hadsereg szolgálja az országot, de az ösztöndíjakkal támogatott képzésnek hála a szakembergárda magasabb színvonalat képvisel.

Irán az amerikai-izraeli Stuxnet vírus támadása után 20 millió dollárt költött el a saját kiberhadserege felállítására, ami mostanra a negyedik legnagyobbra nőtte ki magát a világon. Az USA pénzügyi szektorán kívül támad-

ták még a Saudi Aramco olajvállalatot is körülbelül 35.000 számítógép működését megállítva és több hónap folyamatos fennakadást és működési pauzát okozva ezzel a vállalatóriásnak, aki csak méretének köszönhette, hogy gazdaságilag túl tudta élni a kibertámadás okozta megpróbáltatásokat.

„Nagyon gyorsan és nagyon jelentőssé nőtték ki magukat az elmúlt néhány év alatt". („They've grown up very fast and very significant over the past few years,") David Kennedy, a TrustedSec kiberbiztonsági vállalat CEO-ja nyilatkozta ezt a Tech Insidernek. „Ráébredtek, hogy nem lehet légi vagy hasonló erőfölényük, különösen ha az Amerikai Egyesült Államokat nézzük. Tehát nagyon sokat fektetnek be a kibertér részébe." („They realize they can't have any type of superiority around air, or anything like that, especially when it comes to the United States. So they're investing a lot of it into the cyber piece.")

De hol vannak az oroszok? Már bizony ott, ahol az 1965-ös híres magyar vígjáték mondja: a spájzban. Vagyis veszélyesen közel ellenségeik számára. Természetesen a katonaság és a hírszerzés is rendelkezik kibervédelmi kapacitásokkal (ahogy azt az amerikai demokraták szerverei elleni 2016-os támadás is jól példázta), de az orosz kiberbiztonsági kapacitások egyik gerincét a nagy mennyiségű hacker adja és az a módszer, ahogy Oroszország kezeli őket. Vagyis aktívan kommunikál velük és a „munkájukért" cserébe elnézi az egyéni akciókat, ahogy Michael V. Hayden tábornok, az NSA és a CIA egykori igazgatója mondta egy 2016-os kiberhírszerzéssel foglalkozó konferencián.

Izrael jelentős erőt képvisel a kiberpolitikában. Nem elsősorban mérete, hanem inkább geopolitikai és szakmai környezete predesztinálja erre. Az ország zaklatott múltja és konfliktusokkal teli kapcsolata a szomszédjaival hamar arra az útra terelte az országot, hogy minden téren erős védelmet építsen ki. Az USA-val való együttműködés stratégiai eleme a katonai fejlesztéseknek, de Izrael jóval hamarabb felismerte a kiberfenyegetésekkel kapcsolatos veszélyeket, mint például az olyan amerikai háttérrel rendelkező piaci óriások, mint a Cisco. Az ország létrehozta a saját kibervédelmi divízióit. Az USA-t nem számolva mostanra Izrael több kiberbiztonsági eszközt és szolgáltatást exportál, mint bárki más a világon. 2015-ös jelentések szerint a kibertermékek piacából 10%-ban részesült, a befektetések tekintetében pedig ez az arány 20% globálisan (Computerweekly.com, 2016). Szám szerint csak szoftver tekintetében 60 milliárd dollárt jelentett 2014-ben (Fortune.com, 2015).

Az izraeli kiberipart a hadseregből kikerülő (a kötelező katonai szolgálatot kibervédelmi szakemberként is leszolgálhatják az állampolgárok) nagy részben tehetséges szakemberek által alapított startupok adják. Ezek elindításában, támogatásában a hadsereg is aktív részt vállal. A nagy amerikai kibervállalatok jelentős összegeket fektetnek be az itt induló izraeli startupokba, például a Cisco legalább 10 izraeli startupot vásárolt fel, többek közt az Intucellt 213-ban 475 millió dollárért. Szintén 2013-ban a Google vásárolta meg a népszerű Waze-t 1 milliárd dollárért (Techrepublic.com, 2016). És vannak a mai napig izraeli tulajdonban lévő, olyan világszinten jelentős kiberbiztonsági vállalkozások, mint a Checkpoint.

Az **Egyesült Királyság** a GCHQ (Government Communications Headquarters, amely a titkosszolgálat egy kiberbiztonságra szakosodott ágát is működteti) kiberbiztonsági területének létrehozásával és a 2011-ben bejelentett 750 millió font átcsoportosításával a klasszikus katonai kiadásokról a kiberbiztonságra alapozta a helyzetét. 2013-ban létrehozott egy keretrendszert a kiberbiztonsági információk megosztására a civil és katonai szféra közt (Cybersecurity Information Sharing Partnership), ami segítette az ország megerősödését a kiberharctéren. 2016-ban az Egyesült Királyság növelte a területre koncentrált kiadásait, 1,9 milliárd fonttal többet kívánnak elkölteni 2020-ig. Ez 1900 új szakember hadrendbe állítását jelenti 3 hírszerző ügynökség keretein belül, és létrehozzák a nemzeti kibervédelmi központot is (NCSC – National Cyber Security Centre), ami otthont ad majd az ország első kiberhaderejének (gov.uk, 2016). A szervezet létrehozásával Anglia reméli, hogy egy olyan dinamikus, a modern piaci viszonyoknak megfelelően működő szervezetet hoz létre, ami vállaltan strukturáltan kommunikál a kormányzat szándékairól, őszinte és együttműködő párbeszédet kezdeményezve a piaci szereplőkkel. (gov.uk, 2016)

3.3. SOC-megoldások

A SOC alapvetően a cég azon részlege, amelyik a rendszer kiberbiztonságáért felel. Az itt dolgozó szakemberek, a hardverek, szoftverek és know-how összessége. A már meglevő kibervédelmi rendszer ernyője alatt dolgozó csapat, akinek a feladata az illegális hozzáférések, malwarek megkeresése, azonosítása, majd kezelése. A SOC feladatkörébe tartozik a már meglévő fenyegetések analizálása,

„kriminalisztikai" elemzése, esetleg az adatok bizonyítékként való felhasználásra való felkészítése és a bekövetkező incidensekről jelentések készítése.

3.3.1. Nemzeti SOC-ok

A SOC-októl megszokott rendszerben működő nemzeti eseménykezelő központ a CERT (Computer Emergency Response Team) vagy CSIRT (Computer Securitiy Incident Response Teamnek). A jelentősebb, informatikai értelemben fejlettebb országok majdnem mind rendelkeznek saját CERT-csapattal (a teljes lista itt megtekinthető: www.cert.org, 2016), amiknek a fő feladata hogy az ország kibervédelmét ellássa vagy legalább figyelmeztetni tudjon a veszélyre. Sokszor kommunikációs és tájékoztatási feladatokat is ellát. Mint sok állami szervnek, a nemzeti CERT-eknek is kérdéses az értéke és az is, hogy milyen mértékben támaszkodhatnak rá az államok a kibervédelmük megszervezésében; a legnagyobb szereplők a nemzetközi kiberszíntéren magáncégeket is megbíznak.

Egy CERT feladata szinte teljes mértékben megegyezik a SOC-al, a legjelentősebb különbség talán a rá háruló felelősség és a feladatkör nagysága. Egy nemzeti CERT/CSIRT a teljes ország infrastruktúrájáért felel, a kormányzati szerverek, honlapok biztonságáért, esetleg kritikus infrastruktúrák kiberbiztonságáért vagy a kommunikációs biztonságért. Míg a SOC-ok általában egy területre vagy vállalatra koncentrálnak. Ugyanakkor ebből a szempontból egy csendes átrendeződés jelei bontakoznak ki az elmúlt pár év változásaiból, amely a CERT-ek feladataiból egyre többet enged át a privát vagy nemzetileg üzemeltetett SOC központoknak.

A különböző országok kiberbiztonságért felelős hivatalai között létezik szakmai együttműködés, például a NATO-tagállamok külső támadás esetén segítenek egymásnak, vagy például a kínai-orosz kiberpaktum, melynek célja az USA dominanciájának csökkentése a kibertérben. Ez persze nem azt jelenti, hogy ezek az országok nem támadják egymást, időről-időre kipattannak kisebb-nagyobb botrányok, de ahogy a kibervilágban mondják: aki nem ellensége az embernek, az szinte a barátja…

A magyar kibervédelem, mely a 2010-es évek elején a világ élmezőnyébe tartozott, ma már nincs ebben az állapotban. „Az információbiztonsági törvényt inkább átírták, hogy új szervezeti felépítést hozhassanak létre. Sokáig

azonban nem történt semmi, a régi intézmények megszűntek, elvesztették szerepüket, az újak pedig nem jöttek létre. A védelem biztosítása ideiglenesen a titkosszolgálatokhoz került, amelyeknek a támadás is feladatuk, így feloldhatatlan dilemma elé kerültek." Írja az Index egy 2015 végi cikke. Több országban végigmentek ezen a folyamaton (például Thaiföld), először a titkosszolgálatok kezelték a nemzeti kiberbiztonságot aztán „liberalizálták" éppen az információmegosztás érdekében. A jelenlegi magyar modellnek, noha az információmegosztás korlátai miatt vannak hátrányai, de komoly előnyei is jelentkeznek. A titkosszolgálatok eleve rendelkeznek operatív felhatalmazással, ezért komoly kiberbiztonsági incidens esetén nagyobb eséllyel tudnak gyorsan és hatékonyan beavatkozni a nemzet biztonságának érdekében.

3.3.2. A SOC-ot specifikusan az alábbi célokra tervezték:

- Központi helyet biztosít a cég forgalmának vizsgálatára, a fenyegetések elkülönítésére és kezelésére.
- Felkészül arra, hogy válaszoljon a kiber-incidensekre.
- Lehetővé teszi az üzleti tevékenység folytatását és a hatékonyság visszanyerését. A Ponemon tanulmányban vizsgálta, hogy a külső költségeken belül az üzleti tevékenység megzavarása (szerver-leállás ideje, belső rendszer összeomlasztása, kommunikáció ellehetetlenítése) volt a legmagasabb. (Ponemon, 2015, 16. oldal)
- Megakadályozza, hogy az üzleti infrastruktúrát károsítsák a kiberfenyegetések.
- Részletes szakértői jelentésekkel járul hozzá a vállalat működéséhez.
- Biztosítja, hogy azok a csoportok, akik a kritikus védelmi rendszereket figyelik (tűzfalak, behatolás-védők, jogosultságkezelők, naplóelemzők, hálózati infrastruktúra routerek) potenciális fenyegetés esetén hamar tudjanak reagálni.

3.3.3. A SOC feladatai még specifikusabban:

- Megfigyelés, analizálás, korrelációk észrevétele és a behatolási események feltárása.
- Mintázatok feltárása a fenyegetésekben és a potenciális hatásuk elemzése az üzleti tevékenységre.

- Megfelelő védelmi eljárások kifejlesztése védekezésre, elhárításra és válaszra.
- Incidenselemzés lefolytatása és a behatolás bűnügyi elemzése.
- A krízishelyzeti eljárásokban és kommunikációban való részvétel.

3.3.4. Mi az MSSP, és SOC-ra vagy MSSP-re van-e szükség?

Az MSSP tulajdonképpen egy külsős szolgáltató cég, a SOC-ok működtetésére specializálódik. Specializálódásuk okán sokkal hatékonyabban tudják ellátni ezt a feladatot, mint azok a hagyományos IT cégek akiknek házon belül kell ezt megoldani. Egy MSSP szolgáltató lényegében plusz kapacitást jelent anélkül, hogy a cégnek foglalkoznia kelljen egy teljes rendszer kiépítésével és működtetésével.

Hogy melyik megoldást kell választani, sok tényezőtől függ, ezért egymagában a CEO, CTO, CIO vagy a biztonságért felelős CISO és CSO nehezen tudják eldönteni. Jellemzően nincs egyértelmű válasz arra, hogy az olyan globális kiberbiztonsági kérdésekben, mint a kiberbiztonsági kapacitás kiépítése, pontosan kinek kell a döntéseket meghozni, az IT szakembereknek vagy pedig az üzleti vezetőknek. Nagyon ritka, hogy egy vezető átlátja a cég „globális" működését üzleti, adatvédelmi és kiberbiztonsági aspektusból is, és minden szempontból kompetens. Mind a SOC, mind az MSSP megoldás jár előnyökkel és hátrányokkal, ezeket fogjuk a következőkben taglalni.

3.3.5. Belső SOC előnyei

- Specifikus belsős csapat, magasan képzett szakemberek értékes tudással (egy tanfolyam ára akár 5-6 ezer dollárra is rúghat) (sans.org, 2016), akik mindig elérhetőek.
- Jobban ismeri a cég belső működési mechanikáit, mint egy third-party partner (ez egyébként az egyik legnagyobb előnye a belső SOC-nak, nem véletlenül szoktak nagyobb szervezetek a saját erőforrásból felépített SOC mellett dönteni).
- A megoldások sokkal személyre szabhatóbbak.
- Nagy valószínűséggel hamarabb észreveszi az összefüggéseket a belső csoportok között, például ha az egyik divízió működése potenciálisan kiszolgáltat egy másikat, támadhatóvá teszi azt.

- A logokat helyileg tárolja, az adatok kiszolgáltatása sok esetben lehet törvényellenes (nemzetbiztonság), vagy ütközhet a cég belső adatkezelési szabályaival. A logok kezeléséről bővebben: csrc.nist.gov, 2006.

3.3.6. A belső SOC hátrányai

- Sokkal nagyobb egyszeri befektetés (a fizikai berendezések, a szoftverek, a képzések ára könnyedén elérheti a félmillió dollárt is).
- Nagyobb a nyomás, hogy jobb befektetés-arányos megtérülést mutasson.
- Nagyobb az esély, hogy az elemző közvetlen találkozik a támadóval.
- Valószínűtlenebb, hogy a finom mintázatokat észreveszik a nagyméretű rendszerekben.
- Nehéz jó szakembert találni, képezni és megtartani.

3.3.7. Kérdések, amiket érdemes feltenni

- A csapatunknak megvan a képessége (tehetsége és tudása) arra, hogy egy SOC-ot hatékonyan tudjon üzemeltetni?
- Ha megvannak ezek a képességek, hogyan akarjuk ezeket kiaknázni?
- Hajlandóak vagyunk az időt és energiát fektetni a SOC összes folyamatának és módszerének dokumentálásába?
- Ki fogja a képzési programot elkészíteni?
- Ki fogja a fizikai berendezéseket összeállítani?
- Képesek vagyunk arra, hogy elég embert felvegyünk és egy hatékony csapatot fenntartsunk?
- Ha ezek az összetevők hiányoznak, nem érdemes belevágni, mivel jelentős források árán hamis biztonságérzetet teremtenénk, ami később valószínűleg visszaütne.

3.3.8. A siker összetevői

- Profi csapat.
- Jó SOC menedzsment.
- Elégséges büdzsé.
- Hatékony folyamatok.
- Az incidenskezelésbe való bevonás.

3.3.9. Az MSSP előnyei

- A nagy kiadások elkerülése – a hardver- és a szoftver-megoldás egyben.
- Potenciális új ügyfelekkel való megismerkedés.
- Gyakran olcsóbb, mint házon belül megoldani.
- Kisebb az esély arra, hogy a támadó és az elemző összeütköznek.
- Nem részrehajló.
- Potenciálisan rugalmas és skálázható
- Nagy tapasztalat megfigyelésben és SIM (Security Intelligence Management) eszközök terén.
- SLA – Service Level Agreement (szolgáltatási szint biztosítása).

3.3.10. MSSP hátrányai

- Szerződéses partner soha nem fogja olyan jól ismerni a rendszert, mint egy belsős csapat.
- A munkák kiszervezése csökkentheti a belső morált.
- A dedikált belső csapat hiánya.
- Az adatok hanyag kezelésének veszélye (ezt auditokkal karban lehet tartani).
- A logok nem elérhetőek bármikor.
- Rugalmatlan szerkezet, az MSSP-k standard módszereket alkalmaznak a minél nagyobb kliensbázis lefedése érdekében.

3.3.11. Általános kérdések a potenciális MSSP felé

- Milyen a reputációja?
- Kik az ügyfelei?
- Vannak-e már ügyfelei az iparágunkban (ez akár állami vagy nemzeti is lehet)?
- Skálázható-e a cégünk / feladat méretéhez?
- Milyen régóta partnerei a jelenlegi ügyfelei?
- Milyen arányú közöttük a szerződésbontás, szerződésmegújítás elmaradása?
- Hogyan védik meg az adatokat, milyen szintű a biztonság az ő SOC-üknél?

3.3.12. Az MSSP belső csapata felé releváns kérdések

- Mennyire tapasztalt a csapat? Felfogadnak-e etikus hackereket?
- Ellenőrzik-e az új alkalmazottak hátterét?
- Kiszervezik-e bármelyik munkafolyamatukat?
- Az alkalmazottak elég szigorú titoktartási szerződést írnak-e alá?
- Milyen a tapasztalt mérnökök aránya a kliensekhez képest?
- Milyen képesítésekkel rendelkeznek a senior/junior alkalmazottak?
- Milyen az alkalmazotti felmondási arány?

Tekintettel arra, hogy az eseményszám nagyobb szervezetnél elérheti akár a 20 milliós nagyságrendet is (nextgov.com, 2013), ezért a kapacitás tervezése kulcsfontosságú, amikor kiberbiztonsági eseményeket akarunk kezelni. A probléma súlyát érezhetjük, ha egy pillantást vetünk két professzor Doug Altner és Les Servi matematikai mélységű tanulmányára (A Two-Stage Stochastic Shift Scheduling Model for Cybersecurity Workforce Optimization with On Call Options), amelyben a kiberbiztonsági erőforrások időbeli optimalizálására dolgoztak ki modelleket ismeretlen és bizonytalan munkaterhelés mellett (Doug Altner és Les Servi, 2016).

Költségek lebontása	Naplóelemző megoldás (SIEM)	Távfelügyelet (MSSP)	Megtakarítás	%
Eszközök (Termék ár) SOC infrastruktúra (a termék vásárláshoz)	$400,000			
MSSP (távfelügyeleti) díjak / induló költségek	$100,000	$30,600		
Teljes / Kezdeti	$500,000	$30,600	$469,400	94%
Éves / Folyamatos kiadások				
Erőforrások (2FTE azaz 2 db teljes munkaidős munkatárs)	$212,500			
Vezetői költségek	$106,250			
Biztonsági szakmérnöki költségek	$78,750			
Oktatás	$11,250			
Eszközök és karbantartás	$90,000			
SOC működtetési költségek	$9,200			
Értékcsökkenés és Amortizáció	$166,667			
Folyamatos tanácsadói költségek	$12,500			
Hálózati behatolásvédő (IDS / IPS)	$10,000			
MSSP (Távfelügyeleti) díjjak		$511,240		
Teljes (folyamatos, megújuló)	$697,117	$511,240	$185,877	27%

(Forrás: Wyndham Worldwide, 2012)

3.3.13. Ha úgy döntünk szükségünk van egy SOC-ra

A cégnek muszáj megterveznie a kiépítés folyamatát. Ez a tervezési fázis gyakran csak az emberekre, folyamatokra, technológiára terjed ki, míg az alapvető motivációk feltérképezését – hogy miért hozzuk létre pontosan a SOC-ot és mire fogjuk használni – kihagyja. A sikeres munkához a fentiek nélkülözhetetlenek. A kezdeti, tervezéssel töltött idő hosszú távon megtérül. Mielőtt a cég kiépítene egy SOC-ot, fontos hogy megválaszolja tehát a következő kérdéseket:

- A szervezet milyen szükségleteit elégíti ki majd a SOC?
- Pontosan milyen feladatok tartoznak majd a SOC-hoz?
- Kik dolgozzák majd fel a SOC által gyűjtött információt? Mit várnak ők el a SOC-tól?
- Ki képzi majd ki és milyen anyagok mentén a SOC használatára a cég többi részlegét?
- Ki lesz az, aki a döntéshozóknak bemutatja a költségeket, megtérülést és a várható előnyöket?
- Milyen jellegű biztonsági eseményekkel foglalkozik majd a SOC?

A HP Building a successful SOC Business Whitepaper-ében (HP, 2013) részletesen ír a SOC rendszer kiépítésekor szükséges összetevőkről. Az építés során a kiadási- és megtérülési tervet is el kell készíteni.

Az alábbi lista jó kiinduló pontot adhat ezek elkészítéséhez:

Felszerelés

Bútorok, számítógépek, speciális fizikai biztonsági rendszerek, telekommunikációs rendszerek, áram, fűtés, légkondicionálás.

SOC-munkaerő

Biztonsági elemzők, műszakvezetők, SOC menedzserek.

Támogató munkaerő

Hálózati támogatás, rendszertámogatás, adatbázistámogatás, telekommunikációs támogatás, biztonságieszköz-menedzsment.

Oktatás és képzés
Tanórák, konferenciák, folyamatos képzés. Az összköltség jelentős százalékát adja (lásd a táblázatban).

Threat Intelligence előfizetések
Mindig up-to-the-minute információkkal kell rendelkezni a legújabb fenyegetésekről. Megfigyelési technológiák: hardver, szoftver, tárhely és megvalósítási szolgáltatások.

További technológiák
Probléma- és változásmenedzsment, e-mailek, tudásmegosztás. Ezeken nehéz spórolni, az alábbi pontokban a költségek csökkenthetőségével, ROI-val foglalkozunk:

Költségelkerülés
Egy SOC kiépítése valószínűleg kisebb költségvonzattal jár, mint nem észlelni és nem megakadályozni a kibertámadásokat.

Költséghatékonyság
Nagy rá az esély hogy a SOC-folyamatok és technológiák segíthetnek automatizálni és hatékonyabbá tenni már meglévő funkciókat a vállalaton belül. Bizonyos fenyegetéstípusokban az új adatfolyam befogadásával, az ebből nyert adatok elemzésével, valamint az automata jelentési rendszer felállításával, a manuális feladatok csökkentésén keresztül a SOC költséget takaríthat meg a vállalatnak.

Javított biztonsági ROI
A legtöbb cég számos különböző biztonsággal kapcsolatos technológiába fektet (DLP, AV, IDPS stb.). A maximális hatékonyság elérése érdekében az összegyűjtött adatok feldolgozása és analizálása kulcsfontosságú. A korreláló adatok a technológiák közt tovább növelik a befektetés értékét és hatékonyságát.

Költségmegosztás
Néha már létező csoportok végeznek olyan tevékenységet, melyet később a SOC lát majd el. Ezek a csoportok kihelyezhetik ezeket a feladatokat a SOC-hoz. Esetleg egy partner céggel együttműködve csökkenthetők a kiadások.

Kereskedelmi előnyök
Az információbiztonság talán még soha nem volt olyan fontos kérdés, mint manapság. Egy jó SOC jelenléte a cégen belül segítheti az ügyfelek vagy állampolgárok bizalmának elnyerését, bizonyos piacokra való belépést és a konkurenciával szembeni előny megszerzését.

A csapat
Amint az eddigiekben taglalt alapokat lefektettük, a SOC kiépítése folytatódhat a hagyományos IT projekthez szükséges eszközök (emberi erőforrás, folyamat-szervezés, technológia) előteremtésével. Ezek egyenlő fontosságúak; a cégek leggyakrabban a megfelelő munkaerő alkalmazása és megtartása során vétenek hibát.

Kiválasztás
Belső SOC kiépítésekor a leggyakoribb hiba a nem megfelelő munkaerő alkalmazása. A vállalatok gyakran túl alacsonyra teszik a mércét az elemzők kiválasztásakor. Egy SOC elemző az információbiztonsági közösség gyalogosa, az az egyén, aki napi szinten száll harcba egy kemény és kreatív ellenséggel. Ez az ellenség pontosan ismeri az elemző munkájának nehézségeit, azt, hogy milyen nehéz egy monitor előtt ülve ezernyi jelentésből kiemelni a valóban fontos rosszindulatú támadásokat. A hatékony SOC elemzőinek végtelen türelemre van szüksége, és arra, hogy képes legyen észrevenni a problémákat és nyugodtan kommunikálni stresszes időkben is. Ez több, mint amit egy belépő szintű IT alkalmazottól várhatunk.

Az elemző pozícióba érkezhet akár korábban help-desk operátorként dolgozó munkatárs is, de jobb kiindulópont lehet, ha a rendszeradminisztrátorok vagy rendszerüzemeltetők közül választunk. Az ideális személy tapasztalatot szerzett rendszerüzemeltetésben, szerverekben és támogatásban, általában rendelkezik a szükséges problémamegoldó képességgel, és jól

működik elemző feladatkörben, melynek része a TCP/IP protokollok kezelése és a különböző behatolásra utaló jelek felfedése. A fenti kvalitások mentén összeállított csapat létrehozása önmagában is problémát jelenthet (bérköltség, kulturális konfliktusok stb.). Ezt sok cég úgy oldja meg, hogy a kezdő SOC-csapatot később folyamatos képzés során juttatják el a minimálisan elvárt tudásszintre.

4. A Threat Intelligence

4.1. Mi az a Threat Intelligence?

A Threat Intelligence-nek nehéz pontos magyar fordítást találni, talán a fenyegetettségi hírszerzés áll a legközelebb hozzá. Kiberbiztonsági cégek által nyújtott szolgáltatásról beszélünk, amelynek elsődleges feladata, hogy előrelátóan számolni tudjon a kockázatokkal (threat actors) és a lehetséges támadásokat időben észlelje, illetve együttműködve a biztonsági központokkal esetleg megállítsa azokat.

Ezek szolgáltatásaikkal a SOC és MSSP csapatokat támogatják, tájékoztatják őket a fennálló veszélyek és a jövőben várható támadások természetéről, ismerhető paramétereiről. Mindemellett hálózatvédelmi tanácsadást is nyújtanak, hogy a már felfedezett hibákat a lehető leghatékonyabban orvosolni tudják.

Miután a hálózatot fenyegető veszélyekről sikerült reális képet kialakítani, már könnyebb eldönteni, hogy pontosan milyen védelemre lesz szükség és mekkora anyagi forrást érdemes a hálózatvédelemre fordítani. Biztonsági cég alkalmazása és a „threat actor"-ok (fenyegető felek) felfedése ma elengedhetetlen, máskülönben az esetleges támadásokból származó veszteségek bizonytalanná tehetik a cég pénzügyi jövőjét, veszélyeztetik az üzleti és gazdasági növekedést vagy kiszolgáltatottá tesznek egy államot a kibertámadásokkal szemben. Noha a védelmi rendszer felállítása és folyamatos frissítése költséges lehet, még mindig kevesebbe kerül mint a kiszivárgott adatok és az ebből adódó problémák megoldása.

Ahogy a jelenlegi állapot áttekintésében is láthattuk, ma mindent az informatika segítségével irányítunk, így informatikai eszközeink védelme meg-

kerülhetetlen, kritikus ponttá vált. A kockázat és veszélyek szintje egyre nő, ahogy a világ halad a digitalizáció útján. Gondoljunk csak egy állam olyan kritikus infrastruktúráira, mint a vízellátás, közlekedés és bankrendszerek, hogy csak néhányat említsünk. Ha ezeket éri komolyabb támadás (ahogy az például 2016 elején Ukrajnában történt), az könnyen megbéníthatná egész régiók, az ország normális működését.

4.2. Mivel dolgozik a Threat Intel?

A fejlesztők elsősorban esettanulmányok alapján dolgozzák ki a threat intelt, az eddigi támadások technikái alapján próbálnak megfelelő védelmi rendszert kiépíteni. Emellett kalkulálnak a hackerek támadásainak eddigi gyakoriságával és a használt módszerek változásaiból próbálják megjósolni, hogy a jövőben milyen irányba fejlődnek tovább az alkalmazott technikák. Ismert módszerekre készülnek fel, ugyanakkor próbálnak rugalmasak maradni, hogy látókörük minél szélesebb legyen, ezzel is növelve az elemzők hatékonyságát.

A hálózat védelme érdekében a Threat Intelligence által szállított információnak relevánsnak kell lennie a jelenlegi működő struktúrára. Ha a cégnél Threat Intelligence-t állítanak szolgálatba, előzetesen képben kell lenniük, hogy milyen veszélyeztetett rendszereik vannak és meg kell, hogy ismerkedjenek a saját hálózatukkal, annak pontos felépítésével, működésével és mindennapos műveleteivel. Ezek után van lehetőség a Threat Feed-ek megfelelő fogadására. A biztonsági programok analizálják a hálózat működését, és olyan művelet esetén, mely még nem fordult elő vagy szokatlan, a megszokottól eltér, riasztják a SOC üzemeltetőit. Ezzel jelentősen növelik a fejlett eszközöket használó adatlopásra vagy információszerzésre szakosodott hacker csoportok lebukási esélyeit. A Threat Intel táplálkozhat Big Data állományokból vagy naplóelemző rendszerek adataiból.

4.3. A Threat Intelligence fejlesztése, finomítása és alkalmazása

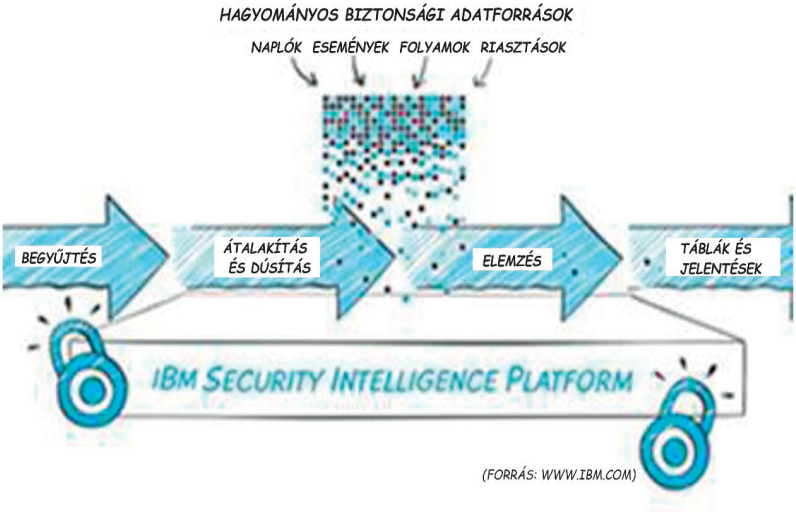
A Threat Intelligence központjában az észlelt támadások és egyéb információk kielemzését követően a Threat Intelt használó munkatársaknak lehetőségük nyílik az esetleges új módszerek, újfajta kémprogramok megismerésére, megértésére. Ezáltal fogást lehet találni azokon és a „betörési" módszerek fejlődési

sebességére is lehet következtetni abból, ahogy az előző támadáskor alkalmazott módszerekhez képest miben térnek el az új események során tapasztaltak, illetve milyen új alkalmazásokat használtak. A folyamatos biztonsági tesztelések szintén lehetővé teszik, hogy a Threat Intel mindig napra kész legyen és a lehető legjobb információt szállítsa a hálózatok számára.

Ahogy a kiberbiztonsági rendszerek egyre több támadást lepleznek le, a biztonsági cégek egyre többféle hackerek által használt alkalmazással és módszerrel találkoznak. Ezek segítségével a későbbiekben a már leleplezett támadásokat azonosítani tudják, felhasználva a már ismert kódrendszereket egyfajta „ujjlenyomatként". Hogy hatékonyabban tudjunk védekezni a támadások ellen, sokat segít, ha tudjuk, hogy támadóink mit keresnek, mi a motivációjuk és egyáltalán kikkel állunk szemben. A legtöbb esetben lekövethetetlenek a támadások, viszont ha ismert alkalmazásokat, módszereket és kódrészleteket fedezünk fel valamely esemény során, következtethetünk a támadóra és céljaira.

Ez az információ hozzásegíthet minket ahhoz, hogy a veszélyforrásokat hamarabb észleljük és az esetlegesen okozott károkat hamarabb helyreállítsuk, illetve ezek segítségével kaphatunk teljesebb képet akár a saját hálózati környezetünk sérülékenységeiről és fenyegetettségi szintünkről is.

A Threat Feedek megbízhatóságától és pontosságától függően a Threat Intelligence három fontos tényezőre ad rálátást: a múltra, a jelenre és a jövőre. A részletes jelentés egy észlelt támadásról új réseket fedhet fel a hálózatot védő kiberbiztonsági rendszeren, melyek javításával egy „ütésállóbb" rendszert hozhatunk létre. Riasztást is ad az aktuális támadásokról és fenyegetettségről, hogy azonnal le lehessen reagálni azokat. Ha szerencsénk van és megfelelően fejlett kiberbiztonsági architektúrával és csapattal rendelkezünk, akkor a megszerzett információt felhasználva megelőzhetjük, hogy akár egy szélesebb, akár egy célzott adatlopási kampánnyal a cégünket vagy hivatalunkat is sikeresen találják meg a Threat Intel által jelentett aktív hacker csoportok. Segít abban is, hogy a jövőben olyan infrastruktúrát és védelmi rendszert lehessen kiépíteni a hálózathoz, mely a lehető legnagyobb kihívást biztosítja a hackerek számára.



(Forrás: www.ibm.com)

4.4. A Threat Intelligence rendszer felhasználási lehetőségei

Érdemes arról szólnunk, hogy mi igen és mi nem a Threat Intel, mivel viszonylag új területként sok megoldással és módszerrel rendelkező szolgáltatókkal akadhat dolgunk.

A Threat Intel nem összekeverendő a Threat Feeddel. Ez utóbbit a legtöbb kiberbiztonsággal foglalkozó cég szolgáltatni tudja és tulajdonképpen arra szolgál, hogy táplálja az informatikai biztonsági rendszereket aktuális, friss információkkal, amelyek segítik a biztonsági rendszerek üzemeltetőit, hogy – lehetőleg automatikusan – elkerüljenek komolyabb hacker támadásokat. Ezek a feed-ek segíthetik a munkát és az észlelést, például nem megbízható IP címek, osztályozások, geográfiai jellemzők átadásával, de nem árulnak el sokat a fenyegetések motivációjáról, a támadók profiljáró célpontjairól és módszereiről. Az olyan Threat Intel megoldások vagy szolgáltatások tudnak nagyságrendekkel jobb minőségű segítséget nyújtani, amelyek

- képesek azonosítani a fenyegetést jelentő hacker csoportot (vagy ehhez elegendő információt szállítanak),
- körberajzolják a támadók lehetséges motivációit,
- iparágakra vagy állami szektorokra jellemző információkat adnak a hackerek tevékenységéről,

- információt adnak a használt malware-ekről, azok felépítéséről, használatuk jellemzőiről,
- meghatározzák a hacker csoportok elsődleges célpontjait,
- megmutatják az adott fenyegető csoportok támadási és cselekvési képességeit (pl. milyen anyagi vagy támogatási háttérrel rendelkeznek),
- rendelkeznek adatokkal sikeresen végrehajtott támadások elemzéssel megtámogatott részleteiről
- adatokkal rendelkeznek a csoportok által megcélzott sérülékenységek természetéről,
- tudnak historikus információkat biztosítani a csoportok tevékenységéről vagy a felhasznált malware-kről.

Egy komplex Threat Intel platformtól elvárható, hogy támogatja az együttműködést az alábbi rendszerekkel (FireEye – iSight, 2016):
- Threat Intelligence Platform (TIP): fenyegetettségi információk átadása;
- Végponti védelem: védelmi profilok meghatározása;
- Naplóelemzők (SIEM): esemény priorizációk, riasztások validálása;
- Hálózati védelem: riasztások validálása;
- Elemzési megoldások (GRC): események elemzése, mi, miért és ki követte el;
- Nyomrögzítés és nyomozás: háttérinformációk szállítása.

Amennyiben sikerül megfelelő elemző csapatot összeállítani a Threat Intel feldolgozására, és be tudjuk kötni a lehetséges információforrásokat a lehető legtöbb biztonsági eszközbe, akkor joggal remélhetjük, hogy hatékonyabb védelmi rendszert tudunk kialakítani, és jóval az események bekövetkezte előtt esélyünk lesz az elhárításra vagy a védelem megerősítésére.

4.5. Szakértői gondolatok a kiberbiztonsági cégek szolgáltatásairól

A jelenlegi megoldásokban nagyon nagy mértékben keverednek a biztonsági védelmi funkciók és a Threat Intelligence. Ezért nehéz általános véleményt adni arról, hogy mely megoldással érdemes egy vállalatnak vagy állami szervezetnek kezdenie. A megfelelő szolgáltatás vagy termék kiválasztása attól is nagy mértékben függ, hogy rendelkezik-e már az adott szervezet működő

SOC-al és fejlett védelmi technológiákkal amelyek a Threat Intel-től érkező információkat sikerrel be tudják fogadni és fel is tudják dolgozni.

Ed Tittel szakértő véleménye szerint kiberbiztonság téren a Cyveillance Cyber Threat Center és a FireEye képes a legnaprakészebb szolgáltatást nyújtani. Ezek a megoldások magas hatékonysággal védekeznek a legújabb támadási és behatolási módszerekkel szemben is, illetve a fenyegetési források leleplezése terén is kiemelkedően teljesítenek, különösen azért, mert rendszeresen hívják segítségül őket kiberbiztonsági incidensek felderítéséhez és utólagos nyomozásához. A FireEye Mandiant csapatát például a Sony Pictures elleni 2014-es támadás körülményekire felderítéséhez használták sikerrel.

Az ActiveTrust egy más típusú szolgáltatást nyújt. A legújabb fenyegetésforrások technikai hátteréről gyűjt össze adatot és tapasztalatot, majd az illetéktelen behatolás megelőzése érdekében hatékony és effektív tanácsokkal és információval szolgál. Ezzel az információval ezután segítségére lehet a klienseinek, akik tovább tudják bővíteni saját Threath Intelligence védőhálójukat.

A LogRhythm Security Intelligence egyszerűbb, felhasználóbarát felületével igyekszik különbözni társaitól. A platform hardware bázisú, integrált szoftverrel dolgozik. A felhasználónak lehetősége van választani több eszköz és kialakítás közül, a védeni kívánt hálózat mérete és infrastruktúrája függvényében (searchsecurity.techtarget.com, 2015).

Természetesen sok cégnek van még hatékony megoldása: az Intel Security, a Cisco, az RSA, a Trend Micro, a Checkpoint, a Fortinet és sokan mások kínálnak még Threat Intelt, de abban már eltérnek, hogy milyen elemző háttérrel rendelkeznek, és valójában milyen mélységig és sebességgel képesek információkat szolgáltatni.

5. Rövid kitekintés a viselkedés alapú megfigyelési technikákra

5.1. Behavior Base Cyber Security

A Behavior Base Cyber Security forradalmian új irány a kiberbiztonság területén. Ez az új technológia, ahelyett, hogy falakkal próbálná megakadályozni

a hackerek bejutását a hálózatba, azon dolgozik, hogy azonosítsa és felismerje őket akár már a támadás első perceiben is.

A viselkedés megfigyelésének több szintjét értelmezhetjük:

- biztonsági rendszerekben összegyűlt adatok elemzésével az egyes rendszerek és felhasználók viselkedési furcsaságainak jelzése,
- az üzleti és irodai alkalmazásokban fellelhető logikai inkonzisztenciák és szokatlan felhasználói viselkedések kimutatása,
- a hálózatokon, operációs rendszerekben vagy adatbázisokban zajló tevékenységben előforduló nem jellemző viselkedések észlelése,
- a felhasználók számítógépén vagy mobiltelefonján végzett tevékenységében fellelhető anomáliák, a megszokottól eltérő viselkedések kimutatása.

A kinyert adatok feldolgozására új technológiájú a Big Data elemzési módszereket és gyakran már mesterséges intelligenciát is felhasználó keresőmotorokat dolgoznak ki, elsősorban az erre a piacra belépő új cégek.

A fenti felsorolás valamennyi kategóriájában komoly fejlesztések zajlanak. Az utóbbi szinttel, vagyis a felhasználók kliens gépeken történő viselkedését elemző megoldással foglalkozik egy új startup vállalat programja a BioCatch, amely eddig már több mint 11 millió dollár támogatást kapott.

A BioCatch programja úgy dolgozik, hogy létrehoz egy mintát a számítógép felhasználójának „viselkedése" és számítógéphasználati paraméterei alapján, majd a későbbi bejelentkezések folyamán ehhez viszonyítva ellenőrzi a műveletek lefolyását a számítógépen.

Ha bejelentkezés történik a számítógépbe, a program elkezdi figyelni a kurzor mozgásának tulajdonságait és a gépelésünk sebességét, a mi saját paramétereinket. A BioCatch képes lesz meghatározni, hogy valóban az account tulajdonosa használja-e a profilt vagy esetleg egy külső behatoló. Ez a program attól függetlenül is tudja a jogosulatlan használatot azonosítani, ha a felhasználó saját belépési adataival léptek be a rendszerbe. Egy felhasználó viselkedését sokkal nehezebb utánozni, lemásolni, mint meghackelni egy védelmi rendszert. Ebben rejlik a módszer hatékonysága.

Hasonló elven működik, mint a bankkártyakezelés. A bank látja, hogy ha szokatlan helyen használjuk a kártyát, például külföldön, és ilyen esetekben

felveszi velünk a kapcsolatot, hogy igazolja a kártyahasználat jogosultságát és beazonosítsa a tranzakció indítóját. A BioCatch technológiája is így működik, kivéve, hogy ebben az esetben a felhasználó számítógépkezelési mintájától eltérő viselkedés esetében jelez. Ilyen indikátor lehet a gépelés, az egérmozgatás, kattintások sűrűsége vagy éppen a megnyitott dokumentumok száma. Ez a program pár belépés után megtanulja, megjegyzi a felhasználó stílusát, és a továbbiakban ez alapján ellenőrzi a műveleteket.

A rendszerben hatalmas potenciál rejlik, globális alkalmazása esetén a biztonság megsokszorozódna és a kibervédelem jelenlegi szintjét is komolyan növelhetné. Paradox módon épp ez gáncsolja az új technológia terjedését. Az általánosan elfogadott privacy policy alkalmazási gyakorlat miatt jelenleg egy szervnek sincs lehetősége legálisan felülvizsgálni globális szinten a számítógépeket és felhasználóikat. Noha a Gartner a kiberbiztonság jövőjét vizsgáló elemzése (Gartner, 2013) szerint 2020-ra már létrejöhetnek olyan iparspecifikus kiberdomainek (pl. pénzintézeti), amelyek akár jogosultságokat is szerezhetnek hasonló tevékenységekre a védelmi szint növelése érdekében. Jelenleg mindenki csak a saját területén mozoghat, szigorúan csak a saját rendszerének felhasználóit tudja figyelemmel kísérni. Szintén kérdés az információ megosztásának lehetősége is. Az összefogás nagyobb cégek és szervezetek között elengedhetetlen lenne ahhoz, hogy a viselkedés megfigyeléséből származó információk „összeérjenek". Viszont tisztában kell lennünk azzal, hogy ez jelenleg még nagyrészt csak elméletben működik. Az információ megosztására vannak jó gyakorlatok is, mint például az amerikai CitiBank kezdeményezései (CitiBank, 2014). Azonban a különböző országok titkosszolgálatai közül senki sem akarná megosztani az információit másokkal, mindenki lépéselőnyben kíván maradni a többiekkel szemben.

6. Összefoglalás

Összegezve láthatjuk, hogy a világban az egyik legfontosabb tényező jelenleg a kiberbiztonság. A hiánya évente több mint 400 milliárd dollár kárt okoz és sok milliárd dollárt költenek rá világszinten, hogy ezt a kárt enyhítsék. Még mindig sok probléma van a biztonsági rendszerekkel, sok rés található rajtuk,

melyeket a szakemberek próbálnak beazonosítani és befoltozni, illetve újfajta technikákkal igyekeznek a lehető legnehezebb feladat elé állítani a hackereket. Ez egyelőre a nemzetek és a vállalatok szintjén is strukturált szélmalomharc, mert ahogy létrejön egy új típusú védelem, azonnal megjelenik mellé egy új módszer, mely megtalálja a sebezhetőséget, és kezdődik minden előröl. A védelmi rendszerek általában csak néhány hónap előnyben vannak támadóikkal szemben, már persze, amikor épp nem néhány hónap hátrányból indulnak.

Éppen a megnövekedett tempó és adatmennyiség – valamint az informatikai rendszerek vitális feladata a létfontosságú rendszerek irányításában elkerülhetetlenné teszi a kiberbiztonsági szakemberek csapatokba és központokba történő szervezését és a SOC létrehozását nemzeti és vállalati szinten is. Az ilyen központ minden szervezetnél létfontosságú, létrehozásához és működtetéséhez nagy mennyiségű technológia és emberierőforrás-beruházásra van szükség. A hatékonyság érdekében működését szükséges megtámogatni Threat Intelligence-szel is, melynek naprakész és használható adatbázissal kell rendelkeznie, hogy a szervezet a legfejlettebb, legújabb behatolási technikákat is képes legyen felismerni, hatékonyan reagálni rá és megfelelő Threat Intel csapat felállításával akár a megelőzésben is eredményeket elérni. Ehhez épülhet hozzá a védelmi technológiák oldalán a Behavior Based Cyber Security, hogy a saját ellenőrzésünk alatt tartott számítógépek és azok felhasználói aktivitásából és tevékenységéből következtethessünk a veszélyekre, fenyegetésekre és időben megelőzhessük azokat. A technológia lehetőséget kínálna arra is, hogy nemzeti szinten ráláthassunk a nemzetbiztonságot veszélyeztető gyanús kiberbiztonsági eseményekre is, azonban ehhez még fejlődnünk szükséges az információmegosztás jogi és gyakorlati alkalmazásának területén.

Ha ezekben előre tudunk lépni, talán képessé válhatunk megvédeni magunkat 2016-ban a kibertérben.

Felhasznált irodalmak jegyzéke

Bhaskar Chakravorti, Christopher Tunnard, Ravi Shankar Chaturvedi: Bhaskar Chakravorti, Digital Planet: Readying for the Rise of the e-Consumer http://fletcher.tufts.edu/eBiz/Digital-Planet, 2014.09 (Utolsó letöltés: 2016. 07.22.)

2017 DOD budget calls for 15 percent increase in military cyber security spending. http://www.militaryaerospace.com/articles/2016/02/cyber-security-dod-budget.html, 2016. (Utolsó letöltés 2016.07. 31.)

Zoe Li What we know about the Chinese army's alleged cyber spying unit http://edition.cnn.com/2014/05/20/world/asia/china-unit-61398/, 2014. (Utolsó letöltés 2016.06.20.)

Paul Szoldra: These are the most-feared hacker groups in the world http://www.techinsider.io/advanced-persistent-threats-2016-7, 2016 (Utolsó letöltés 2016.07.02.)

Cyber threats prompt Estonia to set up UK data centre, http://www.ft.com/cms/s/0/be26fbd2-5005-11e6-88c5-db83e98a590a.html#axzz4FzcB9cuM, 2016.07.22 (Utolsó letöltés 2016.07.31.)

Sam Thielman: DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach, https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2, 2016 (Utolsó letöltés 2016.07.02.)

Ashley David E. Sanger arker Donald Trump Calls on Russia to Find Hillary Clinton's Missing Emails, http://www.nytimes.com/2016/07/28/us/politics/donald-trump-russia-clinton-emails.html?_r=1, 2016. (Utolsó letöltés 2016.07.31.)

Adam Butler: US nuclear force still uses floppy disks, http://www.bbc.com/news/world-us-canada-36385839, 2016. (Utolsó letöltés 206.07.07.)

David E. Sanger: U.S. and China Seek Arms Deal for Cyberspace, http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html?_r=1, 2015.09.19 (Utolsó letöltés: 2016. 07.31.)

Nincs szerző: List of National CSIRTs, https://www.cert.org/incident-management/national-csirts/national-csirts.cfm, 2016. (Utolsó letöltés 2016.07.31.)

Karen Kent -Murugiah Souppaya Guide to Computer Security Log Management, http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf, 2006. (Utolsó letöltés 2016. 07.02.)

Nincs szerző: What it means to have cybersecurity capacity, https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/capacity_dimensions, 2014. (Utolsó letöltés 2016.06.20.)

Antal Lajos: Tudtán kívül bárki segítheti a kibertámadások elkövetőit, http://www2.deloitte.com/hu/hu/pages/risk/articles/barki-segithet-a-kibertamadoknak-sajtokozlemeny.html, 2016.05.02 (Utolsó letöltés: 2016.07.02.)

Daniel Cooper: China accused of hacking US firms even after cyber-peace treaty https://www.engadget.com/2015/10/19/china-accused-hacking/, 2015. 10 19. (Utolsó letöltés:2016.07.02.)

Larry Alton Next-Gen Cybersecurity Is All About Behavior Recognition, https://techcrunch.com/2015/08/23/next-gen-cybersecurity-is-all-about-behavior-recognition/, 2015. (Utolsó letöltés: 2016.07.02.)

Ed Tittel: Security threat intelligence services: A buyer's guide (2015.), http://searchsecurity.techtarget.com/buyersguide/Threat-intelligence-services-A-buyers-guide, 2015. (Utolsó letöltés: 2016.07.31.)

Dustin Volz: U.S. government concludes cyber attack caused Ukraine power outage, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K, 2016.02.25 (Utolsó letöltés : 2016.06.20.)

IBM Security Intelligence with Big Data, http://www-03.ibm.com/security/solution/intelligence-big-data/, 2013. (Utolsó letöltés: 2016.07.28.)

Paul Szoldra: Here's how the US military is beating hackers at their own game, http://www.techinsider.io/us-military-cyberwar-2016-5, 2016. (Utolsó letöltés: 2016.07.31.)

JANOBI 65 Million Tumblr Passwords for Sale on TheRealDeal, https://www.deepdotweb.com/2016/05/31/65-million-tumblr-passwords-sale-therealdeal-market/, 2016. (Utolsó letöltés: 2016.07.20.)

Stan Schroeder: Someone is selling 33 million Twitter passwords on the dark web, http://mashable.com/2016/06/09/twitter-password-leak/#c73Vk3DcP5q7, 2016.(Utolsó letöltés: 2016.07.31.)

Microsoft Secure Blog Staff Microsoft Secure Blog Staff, https://blogs.microsoft.com/microsoftsecure/2016/02/29/anatomy-of-a-breach-how-hackers-break-in/, 2016. 02.29. (Utolsó letöltés: 2016. 07.31.)

Global Cyber Security Capacity Centre, University of Oxford Cyber Security Capability Maturity Model (CMM) v1., https://www.sbs.ox.ac.uk/cyber-

security-capacity/system/files/CMM%20Version%201_2_0.pdf, 2014. (Utolsó letöltés: 2016. 05.28.)

The Institute of World Politics Cyber Security: Why Is This (Still) So Hard?, https://youtu.be/47zJPU0VHSQ, 2016.05.27. (Utolsó letöltés: 2016.07.31.)

Nincs Szerző Security Operations Center Summit, https://www.sans.org/event/security-operations-center-summit-2016/courses/, 2016. (Utolsó letöltés: 2016.07.30.)

Brian Fung How Many Cyberattacks Hit the United States Last Year?, http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/, 2013. (Utolsó letöltés: 2016.07.20.)

Waqas Anonymous Hacks Philippines Election Commission, Leaks 55 Million Voter Data, https://www.hackread.com/anonymous-philippines-hacks-leaks-voters-data/, 2016.04.09. (Utolsó letöltés: 2016.07.31.)

Jon Fingas The US and China want to set ground rules for cyberwarfare, https://www.engadget.com/2015/09/19/us-china-cyberwarfare-treaty-talks/, 2015.(Utolsó letöltés: 2016.05.22.)

Samantha White Global cyber-attacks up 48% in 2014, http://www.cgma.org/magazine/news/pages/201411089.aspx?TestCookiesEnabled=redirect, 2014. (Utolsó letöltés: 2016. 07.20.)

Global Cyber Security Capacity Centre, University of Oxford Cyber Security Capability Maturity Model (CMM) v1.2, https://www.sbs.ox.ac.uk/cyber-security-capacity/system/files/CMM%20Version%201_2_0.pdf, 2014. (Utolsó letöltés: 2016.07.31.)

Steve Morgan Cybersecurity job market to suffer severe workforce shortage, http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-, 2015. 07.28. (Utolsó letöltés: 2016. 07.31.)

James Cook Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far, http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12, 2014.12.16 (Utolsó letöltés: 2016.07.30.)

Doug Altner Les Servi A Two-Stage Stochastic Shift Scheduling Model for Cybersecurity Workforce Optimization with On Call Options, 2016.04.10 (Utolsó letöltés: 2016.06.20.)

HP: A HP Building a successful SOC Business Whitepaper, 2013. (Utolsó letöltés: 2016.07.31.)
FireEye: iSIGHT Partners Introduction, 2016. (Utolsó letöltés: 2016.06.20)
Gartner Gartner: 2020 study on cyber security, 2013. (Utolsó letöltés: 2016. 06.20.)
CitiBank: Fighting cyber-crime together, https://www.citibank.com/tts/about_us/articles/docs/2014/article_fighting_cybercrime.pdf, 2014.12.01. (Utolsó letöltés: 2016.07.31.)

Barsy Miklós
(barsy@vipmail.hu)

A digitális gazdaságról

Lektorálta: Dr. Eszes István Ph.D.

Absztrakt

Mára felnőtt egy digitális generáció, és a mindennapok részévé vált a digitális kommunikáció, a digitális média és a digitális kereskedelem. Természetes elvárás az informatikai eszközök és szoftverek ismerete, mindennapi használata és a magánszemély online imázsának építése. A hagyományos gazdasági és kereskedelmi modellek egy része összeomlott, és a digitális gazdaság meghatározó trendjeit kihasználó online kereskedelmi honlapok forgalmazzák a termékek és szolgáltatások meghatározó részét. Előtérbe kerültek a közösségi médiaalkalmazások, amelyek determinálják a piaci szereplők és a vásárlók reakcióit. Új digitális kereskedelmi, banki és fizetési rendszerek jöttek létre. Az online kereskedelmi portálok és a kapcsolódó digitális fizetési mechanizmusok tértől és időponttól függetlenül biztosítják a digitális vásárlás élményét. A gazdasági társaságoknak ugyanebben a kibertérben kell piacot nyerni, értékesíteni és fejlődni. Drasztikusan át kellett alakítani a gazdálkodási modelleket, a vezetési stratégiákat. Alkalmazkodni kell az új piacrajutási és kommunikációs és marketing módszerekhez. Ki kell fejleszteni a vállalatoknak a korszerű kereskedelmi, fizetési és adatelemzési módszereket biztosító informatikai rendszereket.

Ha a kibertérben nem sikerül permanensen alkalmazkodni, megnyerni és megtartani a piaci részesedést, a kibertérrel rohamosan fejlődő konkurencia rövid időn belül átveszi a piacot és a vevőkört. Tudomásul kell vennünk, hogy a kibertér velünk vagy nélkülünk fejlődik, és vagy fel tudunk zárkózni és kihasználni előnyeit, vagy rövid időn belül drasztikusan le fogunk maradni.

Abstract

A whole new digital generation has grown up now, and digital communication, digital media and digital commerce have become part of our everyday life. Knowledge and everyday use of IT devices and software are considered a natural expectation, as well as the maintenance of a private individual's online image. Certain conventional economic and commercial models have collapsed, and a considerable proportion of products and services are traded

through commercial websites taking advantage of the key trends of digital economy. Community media applications have stepped up to determine the behaviour and responses given by market players and customers. New digital commercial, banking and payment systems have come to existence. The online commercial websites and their related digital payment mechanisms ensure the experience of digital shopping regardless of space and time. Business enterprises must also gain market, sell their goods and develop in this cyber space. Business management models and governance strategies were required to be restructured drastically. New market access, communication and marketing methods were to be adapted to. Companies need to develop information systems providing modern commercial, payment and data analysis methods.

If one fails to permanently adapt to new methods, as well as to gain and maintain market share in this cyber space, rapidly developing competitors, by taking leverage of the cyber space, will shortly take over one's market share and customer portfolio. We have to understand that the cyber space will keep going ahead, either with or without us, and we can either catch up and take advantage of its advantages, or we will be left behind drastically very shortly.

1. A digitális gazdaság jelenlegi helyzete

A digitális gazdaság az utóbbi években exponenciális fejlődésen ment keresztül. Több aspektusból is megváltoztak a gazdasági körülmények és módszerek és a jogi szabályozások. A digitális gazdaság fejlődésével részben megszűnnek a hagyományos területi értelemben vett állami határok, az egyén, illetve a társaságok részére is elérhetővé válnak az internet segítségével olyan szolgáltatások, áruk, illetve tudásforrások, amelyek eddig lehetetlenek lettek volna már csak néhány év vonatkozásában is. A kommunikáció és az azt biztosító eszközök, valamint az ezek kiszolgálását ellátó hálózatok ugrásszerű elterjedésével az áruk és szolgáltatások globális igénybevétele a napi igények kielégítésének részéve vált. Ez azzal jár, hogy a gazdaság immáron jelentős és robbanásszerűen terjeszkedő szegmensét egyértelműen determinálja a kibertér, annak infrastrukturális kiépítettsége, az elérés anyagi és technikai lehetőségei és ebből kifolyólag a fejlett technikai eszközökkel való ellátottság. Tipikus példa a mobiltelefonok és a számítógépek számának és lehetőségeinek fejlődése és változása. A mobiltelefon egy szűk kiváltságos réteg luxus eszközéből a mindennapi élet elválaszthatatlan kellékévé vált. Egy új típusú gazdaságban élünk, amelyet egyre kisebb méretű (mára karóra méretű okostelefonok) és egyre nagyobb tudású kommunikációs eszközök irányítanak.

Mára egyértelműen kimondható, hogy a gazdaság jelentős része hálózati gazdaság, a fennmaradó rész lehetőségeit és fejlődési irányait determinálja, még ha a gazdasági szereplők nem is tudnak róla. A gazdasági szereplők potenciálisan függnek a kommunikációtól és a hálózati gazdaság fejlődési irányától. Jól jellemzi egy összefoglalás a kérdést Jekler Rudolf az információs hálókról írt tanulmányában miszerint „három fő jellemzője van ennek a gazdaságnak. Globális; a kézzel nem fogható dolgokat, ötleteket, információt és a kapcsolatokat értékeli; végül szövevényesen összekapcsolt. E három jellemző teljesen új típusú piacot és társadalmat hoz létre, olyat, amelyik a mindenütt jelen lévő elektronikus hálózatokra épül". (Jekler Rudolf, 2009)

A kommunikáció fejlődésével területileg, országok szintjén és fizikailag elkülönült emberek, gazdasági szereplők között létrejön a kibertéren keresztül egy olyan egységes környezet, amelyben az emberek, gazdasági társaságok, dolgozók és technológiák – függetlenül tényleges földrajzi helyzetüktől – ját-

szanak vagy éppen szoftvert fejlesztenek, anélkül, hogy érzékelnék a földrajzi távolságot, időkülönbséget vagy a tényleges helyzetüknek megfelelően őket körülvevő kultúrát és államot. Jó példák erre az online kereskedések és a multinacionális vállalatok felhőbe applikált alkalmazásai és rendszerei. A kibertérben gyakorlatilag minden egyforma távolságban van, csak az alkalmazott hardverek és szoftverek szabnak határt a tevékenységnek. Az informatikai eszközök alkalmazásával gyakorlatilag megszűntethetőek a földrajzi távolságok és időbeli különbségek.

Ennek megfelelően a konkrét gazdasági kibertér értelmezése is igen nehéz feladat. A gazdasági kibertér abban tér el a többi tértől, hogy gazdasági célból veszik igénybe és az ehhez fejlesztett szoftvereket alkalmazzák. A gazdaság különböző szintjein akár egyszerre is számtalan kibertér létezhet, és ezek a terek részben egymásba csatlakozva, részben egymástól függetlenül önálló életet élnek. Gondoljuk végig, példaképpen, hogy egy amerikai multinacionális vállalat vezetője limuzinjában kelet-európai üzleti útja során notebookjával a telepített vezetői döntési rendszereivel hozhat olyan gazdasági döntést, amely érinti mind az amerikai gazdaság egyes szereplőit, mind a vele kapcsolatban álló magyar vállalatok lehetőségeit és szerződéseit, esetlegesen egy nemzetközi bankkonszern hitelezési lehetőségeinek megnyílását. Gyakorlatilag ezzel, ha fizikailag nem is azonos időben, de néhány percen belül képes rendelni okostelefonja app-jaival egy kínai internetáruházon keresztül terméket, amelyet bárhová a világba elszállítanak. Mindezt oly módon teszi, hogy fejlett technológiája révén csatlakozni képes egy számára idegen ország infokommunikációs szolgáltatójára menet közben az autópályán gépjárművéből. Miközben lehet, hogy tőle csupán néhány kilométerre a hegyekben fekvő munkanélküliséggel küzdő falu napi megélhetésükért küzdő lakossága számára gyakorlatilag ismeretlen az infokommunikáció fogalma, és erősen determináltak a tanulási és életviteli és kommunikációs lehetőségeik. Gyakorlatban a környezetet eközben behálózták az egymástól független, de ugyanazon személyt vagy céget kiszolgáló kiberterek, amelyek részben addig éltek, amely felhasználójuk csatlakozott hozzájuk, részben – például mobilinternet és mobiltelefon szolgáltatás – továbbra is fennmaradt a térségben.

A gazdasági életben a kiberterek lehetnek kis területi átfogású és rövid ideig létező (pl. tranzakció végrehajtására alkalmas) terek és lehetnek komplex,

több földrészt átívelő gazdasági és egyéni érdekeket kiszolgáló globális, hosszú távon fenntartott terek (pl. amazon.com, alibaba.com, google.com, facebook.com) is. Valamint ezek között bármilyen változat, melyek lehetnek egymástól függetlenek, vagy egymással időbeli és informatikai kapcsolatban álló terek.

Az infokommunikációs fejlődés több olyan kérdést is felvet, amely a hagyományos gazdaságirányítási eszközökkel nehezen kezelhető, ellentétes a hagyományos gazdasági elvekkel, illetve nemzetközi jogi szabályozást kíván.

A hálózati gazdaságban „egy-egy helyen összegyűlő adattömeg újabb és újabb látogatókat vonz, s ezáltal tovább nő az itt felhalmozott információ, s rajta keresztül a hely értéke" (Cégvezetés, 2000). Ellentétben az eddigi gazdasági modellel, ahol is ritkasága miatt az arany drága, az interneten, ha a látogatottság kevés, a honlap nem ér semmit. A gazdasági mechanizmus itt fordítottan működik esetenként. A nagyobb látogatottság értékteremtő hatással bír. Az internetes alkalmazás akkor ér el sikereket és teremt magas értéket, vagy hoz egyre növekvő bevételt, ha nagy a látogatottsága, sokan alkalmazzák vagy töltik le megvásárlásukkal. A kibertér és az internetes alkalmazások fejlődésével hagyományos szakmák piaci részesedése eshet vissza vagy mehetnek tönkre (lehetőség pl. vonalas telefon, könyvnyomtatás, taxi-szolgáltatás, tartós használati cikkek helyi értékesítése), ugyanakkor iparágak indulhatnak fejlődésnek (pl. e-kereskedelem, adatbányászat, webbányászat, pay-pall fizetési módszerek).

2. Google-hatás

A keresőrendszerek mindennapjaink részévé váltak. A Yahoo-val kezdődött, azonban ma már senki nem kérdőjelezi meg a Google vezető szerepét a világon. Az internetes keresőmotorok ugrásszerű fejlődésével az emberek többségének internetes nyitólapját egy kereső jelenti. Egyre hajlamosabbak vagyunk rá, hogy inkább néhány jellemző kifejezés beütésével megkeressük a minket érdeklő témát az interneten, mintsem gondolkozzunk rajta, visszaemlékezzünk vagy kommunikáljunk. Gyakorlatilag néhány másodperc alatt több ezer, esetleg millió találatot kapunk az adott témáról világviszonylatban. A találatok szinte azonnali megjelenése miatt nem is foglalkozunk a találat valóságtartalmának tényleges tartalmáról, megfelelőségéről, és az sem merül

fel bennünk, hogy esetleg egy profitérdekelt cég szisztematikusan kialakított marketingrendszerének elemévé válunk lekérdezésünk beütésével. A keresőmotorok megjegyzik (Adam Raff and Shivaun Raff, 2015) minden lépésünket, keresésünket, érdeklődésünket, a weboldalakon töltött időnket és azt is, hogy merre hagytuk el az általuk megjelenített weboldalt. Ez alapján gyakorlatilag teljes érdeklődési körünket, tudásunkat és szokásainkat feltérképezik, és a számukra legnagyobb bevételt jelentő találatok felé terelnek minket, tekintve, hogy az oldalak fizetnek azért a kereső cégeknek, hogy rájuk irányítsák az érdeklődést. Egyrészről az átlag internethasználó nem foglalkozik a saját kiberkitettségével, másrészről többségében nem vizsgálja a megjelenő adatok valóságtartalmát. Feltétel nélkül elfogadja a kapott adatokat az esetek többségében és feltételezi azt is, hogy ha valami nincs az adatok között, az nem is létezik. Egyrészről az internet körülvesz és jelen van, és a keresőkön gyorsabb megtalálni a választ, mint kérdezni, visszakeresni szakirodalomban vagy felidézni a saját tudást. „Mindez azonban gyengíti motivációnkat a tények megtanulására, megjegyzésére. Ezt nevezzük Google-hatásnak, vagy teljes kiteljesedésével digitális amnéziának." (Wtop, 2015). Azt is meg kell említeni a hatások között, hogy egyrészről az hisszük, hogy többet tudunk – mint régebben –, ami részben igaz, részben pedig nem igaz. Jelentős tudásanyagok vesznek el a nyomtatott szakirodalom háttérbe szorulásával és azzal, hogy digitálisan keresünk, és nem memorizálunk, amely hosszú távon jelentős helyzeti tudáshátrányba hozhat minket. Másrészről azt is el kell ismerni, hogy a nyelveket beszélő internetezők részére a felhő alapú keresőrendszerek mindennapi alkalmazásával megváltozik az érzékelés és emlékezés. Kinyílik a világ tudástárának jelentős része és olyan alkalmazásokhoz, digitális szakanyagokhoz is tömegével hozzájuthatnak, amely még pár évvel ezelőtt is elképzelhetetlen lett volna. Az internet „az Ön memóriájának külső meghajtójává vált" (Daniel M. Wenger, 2013), fogalmazta meg honlapján a Scientific American. A tudományos vizsgálatok szerint az internetet egyféle „tranzaktív memória rendszerként" fejlesztjük, és amikor szükséges, előhívjuk. Nem a konkrét információt tároljuk, hanem a leggyorsabb elérési lehetőségét. Mivel az információ kérésére a válasz gyors, sok esetben nem is vizsgáljuk annak teljességét vagy megfelelőségét.

További jellemzője a Google-nak, hogy a nemzetközi kibertér mind totálisabb lefedésével új lehetőségeket teremt (google view, google maps, google

translate) a megismerésre, és lassan, de magabiztosan legyőzi a tájékozódás során a hagyományos GPS-es technológiájú tájékozódási rendszereket és alkalmazásokat. Ugyanígy napjaink szerves részévé vált a fordító- és szótár-alkalmazás és a dokumentumkezelő-alkalmazás, amivel bármikor bárhonnan a felhőből lehívhatóak digitális anyagaink. A szótár sok embernek annyira a mindennapjába integrálódott, hogy – megítélésem szerint – a hagyományos szótárok lassan elvesztik jelentőségüket. A levelezőrendszeréről, a GMAIL-ről pedig nyugodtan kijelenthetjük, hogy világ legnagyobb létszámú levelező-rendszere.

Azt is tudomásul kellene vennünk, hogy ez a cég mára totálisan feltérképezi, befolyásolja, irányítja és dokumentálja kiberszokásainkat, digitális viselkedésünket, tárolja kereséseinket, leveleinket és dokumentumainkat is. Sőt, egyértelműen tudja kontrolálni mozgásunkat a világban. Ugyanakkor totális egyeduralomra törekszik saját szakterületén, úgy hogy gigantikus bevétele után a tényleges bevételt hozó országok részére nem kíván adózni. Az erre irányuló törekvések eddig kudarcba fulladtak. Ennek fényében megjósolhatatlan, meddig jut a GOOGLE a kibertér uralma feletti küzdelemben, de észre kell vennünk, hogy a világ egyik legerősebb és legbefolyásosabb cégéről beszélünk.

3. Az egyén és a digitális gazdaság

A *google* és a *facebook* fogalmak egy évtizede a többség számára még nem voltak ismertek, mára már elsősorban a tizen- és huszonéves generáció részére a napi élet elválaszthatatlan részévé vált. Az az IT-eszközökkel támogatott generáció, amely már nem tudja életét elképzelni a modern kommunikációs eszközök nélkül, kizárja életéből a hálózati kapcsolatok megszakadásának alternatíváját, és a fejlett országokban napi több órán keresztül tart fenn több csatornán digitális kapcsolatokat. Napi életvitele során folyamatosan használja telefonján, tabletjén vagy számítógépén a kommunikációs és a közösségi-média alkalmazásokat. Megfigyelhetők, hogy az utazások során, a közösségi terekben és a baráti kapcsolatokban is dominál az infokommunikációs kapcsolattartás. Embereket, sorsokat, barátságokat és üzleti kapcsolatokat határoz meg. Ma már több munkaadó is ellenőrzi a facebook-profilt és sok esetben

a szakember-kiválasztás is a kibertéren keresztül (pl. LinkedIn) zajlik nemzetközi viszonylatban, mint az a Kellys egyik 2014-es tanulmányából is kitűnik. De ma már az egyén számára a mindennapi élet is nehezen képzelhető el a kibertér rendszeres alkalmazása nélkül. Az egyénnek is aktívnak kell lenni a közösségimédia-tereken, és egy komolyabb üzleti pozícióhoz saját profilt kell építenie és fenntartani, hogy elérje célját. Az állam, a gazdaság és a személyes kapcsolattartás is ezen keresztül valósul meg. Az infokommunikációs hálózatok, a személyi számítógépek, notebookok, tabletek, okostelefonok és újabban az egyéb okoseszközök egyre inkább mindennapjaink elválaszthatatlan részévé válnak; kezdve a világhálón kereskedő e-áruházaktól a közösségi hálózatokon keresztül megvalósuló kapcsolattartáson keresztül. Mára a bankok, valamint az állami intézmények is a digitális kapcsolattartást preferálják. Ez pedig egyet jelent a mindenütt jelenlévő hálózatokkal, az új típusú életformával és a mind szélesebb formában alkalmazott digitális kommunikációval. A kibertér körbefonja életünket. Egyre gyakrabban teremtünk kapcsolatokat, sokszor globálisan, egyre szélesebb spektrumban vásárolunk és végzünk elektronikus pénzügyi műveleteket. Miközben sokan nem számolnak azzal, hogy digitális lábnyomot hagynak, amelyek felhasználhatóak ellenük, és ezzel idegen szervezetek által (állam, bankok, kereskedőcégek) ellenőrizhetővé válnak, és ezt a szuverenitásukat ért támadást sokszor nem is ismerik fel időben. A magánszemélyek ritkán és csak korlátozott mértékben érzékelik és ismerik fel sebezhetőségüket a digitális térben. Egyre többen és egyre gyakrabban a kibertérben működő bűnözők vagy támadás áldozatává válnak. Adataik, pénzük vagy vagyonuk gyakran sebezhetővé válik. Sok esetben a természetes személyek fel sem fogják, hogy a „számukra célzottan *felugró* reklámok és „igen kedvező" ajánlatok valójában már a „teljes személyiségük, vásárlási és fizetési szokásaik feltérképezése után érkeznek meg". (Kellys, 2014)

4. A vállalat és a kibertér

A vállalatok számára az informatika világméretű fejlődése, a kibertér napi szintű alkalmazása új kihívásokat jelent, illetve a gazdaság egy teljesen új dimenzióját nyitja meg. Ez jelenthet megfelelő alkalmazkodás esetén egy hatal-

mas lehetőséget és versenyelőnyt, vagy jelentheti már rövidtávon is a vállalat által gyártott termék(ek) vagy szolgáltatás(ok) eladhatatlanná válását és a cég megszűnését. A vállatoknak tudomásul kell venniük, hogy vagy jelen vannak a kibertérben és alkalmazkodnak piaci kihívásaihoz, vagy megszűnnek létezni a gazdaság többsége számára. A hagyományos kereskedelmi modellek mára jelentősen átalakultak vagy összeomlottak, és más típusú, a kiberteret használó, a hagyományos földrajzi és gazdasági teret és a szűk gazdasági mikrokörnyezetet semmibe vevő kereskedelmi rendszerek jöttek lére. Míg 20 évvel ezelőtt egy családi üzem terméke maximum a helyi piacra vagy az országos kereskedelmi láncokkal megegyezve kis mennyiségben tudott termelni és regionális piacokon értékesíteni, mára az ebay-en saját maga vagy csatlakozva valamelyik internetes kereskedelmi lánchoz, gyakorlatilag a nap 24 órájában jelen van a világ kereskedelmi terében és globális piacon értékesít. Mindemellett a „kibertér elősegíti a globalizált kultúra terjesztését, amelynek egyértelmű társadalmi hatásai vannak. Például a kibertér megkönnyíti és segíti a fogyasztási cikkek termelését és fogyasztását, mert elősegíti a nagy iparvállalatok globalizációját szerkezetátalakításában, és segít egyre jobban behatolni a piacokra is". (Mészáros, 2014)

A kibertér nemzetközi kereskedelmi alkalmazásával lerombolódtak a hagyományos értelemben vett földrajzi és gazdasági határok. Olyan termékek és technológiák is ismertté váltak, amelyek eddig gyakorlatilag ismeretlenek voltak, és mára jelentős vásárlói igényt támasztanak a gyártók és kereskedők felé. Másrészről a világon bárhol legyártott termékek gyakorlatilag a piacra kerülés időpontjában vagy online előre megrendelésre, eladhatók a világ bármely pontjára. Mára jelentősen átalakultak az emberek vásárlási szokásai és igényei. A hagyományos vásárlói kosár mellett jelentős igénybővülés jelentkezik az informatikai és audiovizuális eszközök iránt. Még a gazdaságilag fejletlenebb államok állampolgárai számára is – anyagi lehetőségeik függvényében – napi igényként jelenik meg a mobiltelefon, az okostelefon, a tablet, a notebook és az LCD tv. Gyakorlatilag a létszükségleti cikk érzéséig juttatva használóikat, rövid egy évtized alatt sikerült integrálódni a mindennapokba a GPS-eszközöknek, az okostelefonoknak vagy a notebookoknak. A technológia fejlődése során a számítógépek egyes generációi kimaradnak sok helyen. A mára 30-50 éves generáció az asztali gépektől eljutott a notebookokig, míg

a fiatalabb generáció az internetet eleve már telefonján és tabletjén használja. Komplett informatikai rendszerek alakulnak át gyakorlatilag 10-20 éven belül, és válnak felesleges és elavult technológiává. Gondoljunk vissza a fekete-fehér televíziózás egykori sikerére. A vállalatoknak technológiailag folyamatosan alkalmazkodniuk kell a permanensen változó vásárlói technológiai igényekhez, és meg kell felelniük a globalizálódó piac elvárásainak.

A vállalatoknak több szinten is meg kell felelniük a kibertér kihívásainak. Egyrészről a külső kibertér már említett kihívásainak, másrészről a belső informatikai fejlettség és alkalmazott információtechnológiai rendszerek kihívásának. Mára nem elhanyagolható szempont a vállalatok szintjén a kiberbiztonság kérdése. A hagyományos vírusok és informatikai adatok elvesztésével járó problémakörön kívül megjelent egy sokkal súlyosabb problémakör is, amely komoly biztonsági kockázatot jelent. A SailPoint kutatása rámutat, hogy a modern technológiát és fejlesztéseket végző, valamint a pénzügyi szolgáltatási szektorban működő cégek egyik legkomolyabb IT-kockázata a dolgozó. A dolgozók egy része már viszonylag alacsony összegekért is kiadja vállalati jelszavát vagy a hozzáférést biztosító technológiai adatokat, vagy egyszerűen felelőtlenül kezeli az informatikai biztonsági kérdéseket. Meglepő, hogy „44 százalékuk kevesebb, mint ezer dollárral is beérné az információért cserébe". (Market Pulse Survey, 2016) Még ha a megállapítás csak a digitális gazdaság egyes részterületeire vonatkozóan igaz, akkor is IT-intézkedések sorozatát igényli az érzékeny információk védelme a gazdálkodó szervezetek részéről. Egy korszerű technológia dokumentációjának idő előtti kijutása a konkurenciához vagy a pénzügyi szolgáltató ügyfelei belépési adatainak nem megfelelő kezekbe kerülése, a piaci versenyben utolérhetetlen hátrányba hozhatja a céget, vagy egy pénzintézetet örökre tönkretehet és a jövőre nézve megkérdőjelezi a cég megbízhatóságát. Ehhez még hozzájárulhat jelentős veszteségként az esetleges kártérítés mértéke, amely csődbe viheti a pénzintézetet.

Meg kell említeni még egy területet a kibertérben, ahol a vállalat veszélyeknek van kitéve. A cégek az úgynevezett informatikai ipari kémkedés miatt Németországban „legkevesebb 50 milliárd eurót veszítenek évente (SG.hu, 2014), de a teljes nemzetgazdasági kár ennél jóval nagyobb is lehet" – mondta Hans-Georg Maassen, a német alkotmányvédelmi hivatal (BfV) elnöke.

A Deutsche Telekom 2013-ban publikált kiberbiztonsági riportjában (Deutsche Telekom: Cyber Security Report, 2013) foglalkozott a témával. A megkérdezett vállalatok csupán 13 százalékát nem érte addig – általuk ismert – informatikai támadás, amelybe bele kell érteni a lehallgatást is. Egy idegen kormány, kormányügynökség vagy konkurens vállalat, illetve hacker által megszerzett adatokat és a technológiát immáron rövid időn belül más ország ipara vagy éppen a konkurens társaság használja fel saját célja számára. Ez különösen magas kockázati szintet jelent és igen veszélyes lehet a nukleáris, hadiipari, vagy információtechnológia szempontjából.

A cégeknek egy, a korszerű technológia kihívásának megfelelő és a folyamatos fejlődést biztosító informatikai rendszer kiépítésével, meg kell szervezniük belső kiberhálózatukat és információbiztonságukat úgy, hogy az biztosítsa a piaci versenyben való részvételt. Meg kell teremteni a külső kibertér felé bradjukat, kapcsolati portáljaikat, hogy azok megfeleljenek a gyorsan változó vásárlói és piaci igényeknek kiber biztonságuk fenntartása mellett. Itt kell még megemlíteni a dolgozók informatikai képességei permanens fejlesztésének szükségességét. A mai világban csak az informatikailag képzett management és dolgozók képesek fenntartani a versenyelőnyt ezen a globális digitalizált piacon. Sok esetben ennek feltételeiről gyakran megfeledkeznek a cégek. Nem fordítanak rá vagy keveset fordítanak a magasan képzett informatikusok és egyéb informatikailag képzett szakemberek alkalmazására a magas bér miatt, vagy nem támogatják a fejlett informatika oktatását az oktatással együtt járó, sokszor valóban horrorisztikus mértékű oktatási és technológiai költségek vagy éppen a kieső munkaidő miatt. Fel kellene végre ismerni, hogy a fentiek biztosítása nélkül hosszú távon nem tartható fenn a versenyelőny vagy versenyhelyzet a digitális befolyás alatt álló piacon. A Horváth & Partners felmérése is jól prezentálja a helyzetet és a digitális megfelelés egy fontos mérföldkövét. A tanulmány megfogalmazza a digitalizációval szemben követendő management-szemléletet, és a projekt- és informatikai managerek stratégiával követendő kapcsolatát. A digitalizációban rejlő lehetőségek kihasználásához (Horváth & Partners, 2016) „a CIO-nak kell »támogató«-ként (Enabler) pozícionálnia magát. És nem utolsósorban az IT-architektúra és folyamatok kiépítéséhez is szükség van egy »digitálisan gondolkozó« projektmenedzsmentre, amely a klasszikus nagy projek-

tek mellett lehetővé teszi a digitális, agilis projekteket is. Ehhez innovációs kultúra szükséges, amelyben a felmerülő ötleteket felkarolják, hamar tesztelik és nyomják előre, de ha nem sikeresek, akkor le is állítják őket.

A vállalatok fennmaradásának egyik fő feladata az alkalmazkodás a kibertér kihívásaihoz. A vezetés részére a gazdasági döntésekhez szükséges digitális adatok biztosításán át az ügyfelekkel való érintkezés módszeréig át kell alakítani a vállalatok működési mechanizmusait, feltérképezni a digitális térben élő és vásárló ügyfelek elektronikus vásárlási szokásait, reklámelérhetőségüket és célzott reklámokkal el kell érni őket. Fel kell ismerni, hogy az egyik legfontosabb adat és érték az ügyfél adata, és a megismert ügyfél tapasztalata.

Teljesen új vállalatirányítási és stratégiai szemléletet adva a digitális technológia és ügyféladatok kapcsolatrendszerét kutatja Cristina Mercer tanulmánya a vállalatok digitális térhez való alkalmazkodása terén. Bemutatja, hogy a kiber térben teljesen újra kell gondolni, hogyan használjuk a digitális technológiát, milyen informatikai eszközöket és metódusokat használunk, mely piacon és milyen módszerekkel értékesítünk, különös tekintettel a hagyományos piaci metódusok rohamos átalakulásra. Kiemelt figyelmet kell fordítani arra, hogy hogyan biztosítunk komplex vásárlási és ügyfélélményt az általunk kialakított kibertérben. Az esetek többségében csak a digitálisan elért, és komplex vásárlási élménnyel meggyőzött elégedett ügyfélből lesz rendszeres vásárló.

„Ahhoz, hogy ez biztosítva legyen, a vállalatoknak és különösen a pénzintézeteknek létre kell hozni egy új pozíciót a felsővezetés tagjaként a Chief Digital Officer (CDO) szerepkörét." (Cristina Mercer, 2015) A management új tagját fel kell ruházni azokkal a jogokkal és informatikai háttérrel, amely biztosítja, hogy rugalmasan tudjon dönteni a digitális adatok és trendek alapján projektekről és szervezet átalakítási lehetőségekről, biztosítva a vállalat túlélését és alkalmazkodóképességét a kibertérben. A CDO-pozíciót a legtöbb multinacionális bank és társaság már integrálta management rendszerébe.

5. Digitális városok

Az urbanizáció egyre jelentősebb a világban. A városok lakosságának, illetve az agglomeráció lakóinak informatikai igénye egyre jobban növekszik a digitális szolgáltatások irányában. Az informatikai eszközök elterjedésével a polgárok joggal várhatják el a megválasztott vezetőiktől, hogy biztosítsák számukra az információt a kormányzati és helyi szervek működéséről, a gazdasági lehetőségekről, és digitális eszközökkel is legyenek képesek ügyeiket intézni. Ugyanakkor a gazdaság, így különösen a turizmus és a vállalkozó szektor igényli a digitális lehetőségek mind teljesebbé tételét. Ezek az igények vezettek a 'digitális város' (Wikipedia.org: Smart_city; 2016) informatikai megoldások létrejöttéhez.

„A korszerű infokommunikációs technológiák és szolgáltatások alapjaiban segíthetik egy város életének megszervezését a közszolgáltatásoktól kezdve a városi közlekedésen, az egészségügyön, az oktatáson és a kereskedelmen át egészen a helyi, önszerveződő közösségek támogatásáig." (T-system: A jövő élhetőbb városaiért, 2016).

Az adatok szabadon hozzáférhetővé válnak, a lakosok így hozzáférhetnek az őket érdeklő és érintő adatokhoz informatikai eszközeiken. A digitális platformok és adatok szabadon letölthetők és biztosítják az interaktív kommunikációt. Létrejön a valós idejű kommunikáció a város vezetői, a kormányzati szervek és az állampolgárok között. Ezzel jelentősen javítható a közszolgáltatás ellátási hatékonysága. Új infokommunikációs csatornákat lehet kiépíteni a „lakossággal való kapcsolattartásra, amelyek lehetőséget adnak a gyors és költséghatékony tájékoztatásra vagy éppen a lakossági bejelentések gyors kezelésére. A komplex biztonsági rendszerekkel lényegesen erősíthető a település közbiztonsága, ami hozzájárul egy élhetőbb, szerethetőbb város megteremtéséhez. Gyors és egyszerű az ügyintézés bárhol, bármikor. A Digitális Város koncepciójában találkozik egymással a technológiai innováció, a gazdasági versenyképesség-növelés, a fenntarthatóság és az emberközpontú városvezetés." (Microsoft CityNext: Városfejlesztés XXI, 2016)

A digitális város informatikai megoldásait bevezető városokban jelentősen gyorsul a technológiai innováció, könnyű és gyors az információszerzés, gyorsabb és hatékonyabb az ügyintézés, nő a közbiztonság. További előnye,

hogy jelentős a versenyképesség növekedése és megnő a befektetési hajlandóság az előnyös gazdasági környezet miatt. A digitális kompetencia folyamatos növekedésével egyre jobbak a város gazdasági környezetének versenyképességi esélyei, a beruházások és a képzett munkaerőt megtartó lehetőségek, amely mind a vállalkozások, mind az egyének vonatkozásában igaz.

6. A Közösségi Gazdaság térnyerése

A „Közösségi Gazdaság" (Wikipedia: Sharing Economy, 2016) térnyerésének lehetünk tanúi az elmúlt néhány évben. Ez a hibrid üzleti modell, a közösségi média elterjedésével párhuzamosan jelent meg, és mára már a gazdaság egy jelentős szegmensének tekinthető. Jellemzője, hogy az üzleti modellben a felhasználók egy online felületen a tényleges fogyasztói igény felmerülésekor megrendelik a szolgáltatást vagy terméket a digitális platformon az igényelt javakkal rendelkezőktől és megosztóktól, bizalmi alapon ellenérték megfizetése mellett. Térnyerése rendkívül heves fogadtatású. Hatalmas előnyei mellett sok helyen országok vagy helyi hatalmi szervezetek az állam és a jog eszközeivel lépnek fel ellene. Kétségtelen előnyei a fenntarthatóbb gazdaság és a meglévő infrastruktúrák és eszközök hatékony kihasználása, az igénybevevők részére a jelentős költségmegtakarítás mutatkozik a profi szolgáltatók áraival összevetve. Ugyanakkor hátránya, hogy hagyományos iparágak (taxizás, utazásközvetítés, ingatlan bérbeadása, ingatlan közvetítése) gyakorlatilag versenyképtelenné válnak a *sharing economy* alkalmazások elindulása után rövid idővel. Az állam részéről pedig jelentős hátrányok mutatkoznak, mivel az állami adminisztrációt megkerülő gazdasági szereplőkhöz kapcsolódó bevételek és pénzügyi tranzakciók ellenőrzése adózási szempontból nehéz. Problémát okoz az adózás helyének megállapíthatatlansága és a rendszerszerű adóelkerülés megjelenése. Több helyen emiatt, többek között hazánkban is, az állami jogrend legkeményebb eszközeivel lépnek fel a résztvevők ellen (törvényi fellépés a résztvevők ellen, betiltás, internet alkalmazások blokkolása). Kétségtelen előnye azonban, hogy a meglévő eszközparkok és infrastruktúrák hatékonyabban és olcsóbban használhatóak fel. Jelentősen csökkentené a ennek a természeti energiaforrás felhasználását hibrid internetes erőforrás

megosztási módszernek jogilag szabályozott keretek közötti elterjedése, tekintve, hogy a hiányzó javakkal nem rendelkező személyek viszonylag olcsón hozzájutnának a gazdasági társaságok, személyek és háztartások meglévő infrastruktúrájának szabad kapacitásához.

Egyik legjelentősebb és legismertebb alkalmazása az Uber startup cég, amely már a világ 45 országában szervez taxi megosztást a sofőrök és az utasok között. Több országban is felléptek ellene: pl. az USA egyes államaiban, Ausztráliában, Nagy-Britanniában, Belgiumban, Németországban (Sarnyai Gábor, 2016) és hazánk is többek között a tisztességtelen versenyelőny, az adómegkerülés és az állami szabályozások megkerülése miatt. Mindezek ellenére ez a cég mára már 50 milliárd dollárt (Douglas MacMillan, 2015) ér, és tovább fejleszt. A fent ismertetett, és nyilvánvalóan az államok és egyes szakmacsoportok számára jelentős bevételkiesést okozó hátrányok mellett az internetes iparág rohamléptekkel fejlődik. De mára Boston, San Francisco és New York is együttműködést írt alá az Uber-rel. Minden állami tiltás és megtörési kísérlet ellenére az internet nagy cégei lehetőséget látnak benne, és a digitális fejlődést előtérbe állító államok támogatják és fejlesztik a területet. Kínában az Apple (theverge.com, 2016) részesedést vásárolt Didi Chuxing gépjármű közvetítő cégében, ezzel bevásárolva magát a kibertér potenciálisan egyik legjobban fejlődő piacára egy vezető iparágban.

Mint a PricewaterhouseCoopers Kft. tanulmánya is megállapítja, „az elmúlt és minden bizonnyal a következő évek egyik legfontosabb globális üzleti trendjéről és sikertörténetéről beszélhetünk, melyek – bár vitákkal övezettek – jelentősen meg fogják változtatni üzleti környezetünket." (PWC, 2016) Ugyanebben a tanulmányában a PWC azt is feltételezi, hogy 2025-re az általuk vizsgált piacok felét már ezek a cégek fogják uralni.

A megosztáson alapuló szolgáltatások legjelentősebb térnyerése a személyszállítás, a távolsági közlekedés (telekocsi alkalmazások), az ingatlanközvetítés, és az üdülési célú vagy albérlet jellegű szobafoglalás területén történt. De rohamosan fejlődik az ipari vagy háztartási eszközök és gépek, illetve a sporteszközök kölcsönzése területén is. Eddig nem is létező új lehetőségek jelentek meg, mint az alkalmi ruha vagy táska kölcsönzése magánszemélytől, vagy a parkoló és az alkalmi iroda bérlése területén.

Szintén pozitív és magas gazdasági és környezetvédelmi nyereséggel kecsegtető lehetőségek is megjelentek, mint a közösséginapelem-parkok, a szabad áramtárolási kapacitások virtuális megosztásának megoldásai.

A pénzügyi szektor fintech cégei sem maradtak ki ebből a versenyből. Mára már a közösségi hitelezés több formája tért nyert a gazdaságban. (bantrr.com: Four Types of Crowdsourcing, 2010) Rohamosan fejlődik a kibertéren bonyolított közösségi finanszírozás (Wikipedia.org: Crowdfunding, 2016), és a közösségi innovációs fejlesztések (Crowd Creation) és befektetések kibertéren keresztüli finanszírozása is meghatározó lehetőséggé bővült nemzetközi szinten. Ezek az előremutató és szinte a megjelenésükkel azonos időben már alkalmaz ott is kerülő és rohamosan terjeszkedő innovációk a merev állami bürokrácia, gazdasági és hagyományos vállalati struktúrák számára követhetetlenek, és többségében ellenállást és állami hatósági beavatkozást váltanak ki. Előnyüket a nem kellően rugalmas országok már csak akkor próbálják kihasználni – vagy egyáltalán engedélyezni működésüket, amikor a világpiacon az adott szabadalommal rendelkező cégek már régen monopolhelyzetben vannak, és multinacionális céggé váltak. Az államnak és a világpiacon fejlődni akaró cégeknek folyamatosan követni kellene az internetes gazdasági trendeket, és azonnal rugalmasan reagálni kellene a jogi és gazdasági feltételrendszer megteremtésével a számukra előnyt jelentő internetes alkalmazás megjelenésekor, és támogatni az innovációt a közös előnyök kihasználásával. Ezzel szemben sok esetben regionális vagy szűk gazdasági érdekcsoportok piaci helyzetének fenntartása érdekében törvényi eszközökkel akadályozzák az innovációk terjedését.

7. Digitális bankok a kibertérben

A bankoknak a megszokott piaci környezettel szemben az elmúlt 10 évben egy rohamosan fejlődő digitális pénzügyi szektorral kellett versenybe szállniuk. Mind az általuk megcélzott lakossági, mind a vállalati, de legfőbbképpen a pénzpiac átalakulásával kellett szembenézniük. Az államon belül és államközi piacokon történő pénzügyi tranzakciók monopóliumának kora lejárt. Egy új digitális pénzrendszerrel szemben kell kialakítaniuk saját versenyképes

kiberstratégiájukat, és kell kifejleszteni azokat az elektronikus termékeket, amelyek megjelenésére esetenként időben még reagálni sem tudtak, illetve nemhogy stratégiai időtávban, de még a rövidtávon sem ismert, hogy milyen digitális megoldásokkal rukkol elő a piac. A vásárlók szinte azonnal elkezdik alkalmazni a digitális szolgáltatásokat megjelenésük után. Arra, hogy a pénzpiac is alkalmazkodjon ehhez, rendkívül rövid idő áll rendelkezésre az eddigi management döntési módszerek figyelembe vételével. A digitális startup fejlesztőcégek rugalmas nagysebességű és kockázatos döntésekre szakosodott managementjével kell felvenni a versenyt. Sok esetben, mire a pénzintézetek felmérik a piacot és reagálnak, az eddigi alkalmazások vagy termékek már elavulttá váltak és újak jelennek meg. Tóth Péter prezentációjában kihangsúlyozza, hogy a digitalizálódó világ fogja meghatározni a hitel boom-ot, amely magában foglalja a hitelezés és gyors a kifizetések digitális átalakítását. (Tóth Péter, 2014) A bankok csak 3-5 év távlatában szereztek többségében jártasságot a digitalizációban. Ez akkut problémát okozhat a pénzintézeti rendszerben. Ha nem tesznek sürgősen lépéseket, azt kockáztatják Broders and Khanna szerint, hogy belépnek egy csökkenő spirálba, amely az elkövetkező években 30-40%-os növekedést prognosztizáló digitális piacból az adott szervezetet a növekedés vagy csökkenés oldalára állítja. „Azok a pénzintézetek fognak a nyereséges oldalra vándorolni a digitalizáció által megzavart piac értékteremtési láncában, amelyek sikeresek használják a digitális technológia eredményeit, és kifejlesztenek automatizált új termékeket és rugalmasan alkalmazkodnak a technológia fejlődéséhez." (McKinsey, 2015)

A globálisan innovatív piacon lévő bankok gyorsan reagálnak a digitális kihívásokra, komoly erőfeszítéseket tesznek a tranzakció s migráció területén – bitcoin elszámolási technológia, PayPal csatolás stb. –, és jelentősen képesek megújulni a mobil-, a webes technológiák, és képesek innovációt folytatni az alkalmazásprogramozás és kommunikáció területén. A változás üteme várhatóan gyorsul a következő öt évben és kiterjesztődik, mind földrajzi, mind vásárlói szegmens értelemben. Várhatóan az újonnan beáramló bevételek 40 %-a a digitális piacról érkezik. A digitalizáció jelentheti hosszú távon a bankok és a pénzintézetek számára az inflexiós pontot. Csak néhány évük van alkalmazkodni. Ki kell dolgozni a digitális stratégiát. A folyamat érinteni fogja minden szempontból a banki műveleteket, a termékfejlesztést, a kockázatkezelést és

a humántőke-menedzsmentet. Világosan meg kell érteni, hogy a digitalizáció értéket teremt, és fel kell tárni a potenciálisan értékteremtő perspektívákat a fogyasztói magatartás, a piaci dinamika, a több száz potenciálisan megjelenő digitális beruházási lehetőség és az óvatos felsővezetés között.

Mindezek mellett számolni kell, hogy folyamatosan újonnan belépő startup cégek és -technológiák fognak mozogni a digitális pénzügyi szolgáltatási iparágban, úgy hogy az eddig már versenyelőnyt szerzett cégek komoly digitális eszközökkel és jogokkal fogják megpróbálni korlátozni a versenyt. A bankoknak el kell mélyíteni és fel kell használni a digitális kapcsolatokat a mobil funkciókban, kiépíteni saját brandjukat, ismertté válni a közösségi médiák területén és folyamatosan jelen lenni az online interaktív fizetési megoldások területén. A folyamatban megkapott mennyiségű digitális adatokat fejlett elemező, modellező valamint adat- és internetbányász szoftverekkel kiterjeszteni, és finomítani az üzleti döntéshozatal során. Automatizálni kell a kis értékű, ismétlődő és alacsony kockázatú folyamatokat.

Fontos területté vált a közösségi marketing adatok gyűjtési és digitális piaci adatok modellezése. Ki kell alakítani a felhasználó központú ügyfélkapcsolatokat és ügyfél portfóliókat. Ezeknek differenciáltnak, egyszerűnek, az ügyfélnek vonzónak, ugyanakkor személyre szabottnak kell lenni, hogy miként tudja kihasználni legjobban számláját és hitellehetőségeit.

Tovább kell fejleszteni a célzott digitális marketinget, a mikroszegmentálást és dinamikusabb testreszabott árazást kell biztosítani (Tunde Olanrewaju – McKinsey's, 2015). A továbbfejlesztett adat- és web bányászaton alapuló ügyfél specifikus célzott digitális marketinggel el kell érni a termék árukapcsolást, lehetőség szerint harmadik fél integrációját (például a Facebook). Csatolni kell lehetőség szerint befektetési utazási, biztosítási, ingatlan és keresztértékesítési ajánlatokat is. Csak így érhető el az ügyfél digitális élménye és motivációja a pénzpiaci termékek mind teljesebb körű igénybevételére.

Azonban látnunk kell a másik oldalt is. A digitális banknak a kibertérben folyamatosan léteznie kell, ahhoz, hogy piacképes maradjon. Éppen ezért folyamatosan számolni a kell az üzletfolytonosság fenntartásának kötelezettségével, valamint azzal, hogy potenciális célpontként szerepel az internes csalók, hekkerek számára. Széleskörű folyamatosan fenntartott adatkapcsolataival, online felületével és egy időpontban jelentkező jelentős mennyi-

ségű ügyfélkapcsolatával, a kapcsolódó érzékeny adatok tömegével ellátott szervereik igen vonzó célpontok lehetnek pénzügyi csalások digitális támadások számára. Szintén jelentős üzleti kockázatot jelent, – mint a portfólió.hu tanulmánya bemutatja –, hogy a hagyományos bankoknak jelentős problémát jelent, hogy technológiailag lépést tartsanak a startup és fintech cégek technológiai fejlődésével. Egyrészről a pénzintézeteknek egyre nehezebb lesz a képzett technológiai szakembert magukhoz csábítani (Portfolio: Cunami közeleg, 2015), másrészről a következő tíz évben a pénzügyi szektorban elkerülhetetlenek lesznek a konszolidációk és az összeolvadások. Harmadik akadályozó tényező lesz az egyre inkább monopol helyzetbe kerülő internetes nagyvállalatok és bankok higtech technológiai felvásárlásai és azok azonnali applikálásai, jogi licencei és a piaci szereplők fejlődését korlátozó magatartásuk.

8. Fizetési megoldások a kibertérben

Az elmúlt évek jelentős változásokat hoztak a digitális fizetési módokban, és globális szinten hozott változásokat a pénzforgalmi rendszerekben. Ezek a változások részben a bankok előnyeire, részben pedig jelentős részben a bankok hátrányára fejlődtek ki. Az azonban egyértelmű tendencia, hogy a készpénz fizetése az elektronikus fizetési rendszerek előtérbe kerülésével több területen jelentősen háttérbe szorult, míg az elektronikus fizetési eszközök tért nyertek. A globális kereskedelmi és szolgáltató cégek jelentős piaci szegmensekben előretörtek és ezekhez kapcsolódóan az elektronikus fizetési rendszerek mind technikai megoldásokban, mind módszerekben jelentősen fejlődtek, és mindennapjaink részévé váltak. A készpénzes fizetések helyett dominálnak a kártyás, érintős és internetes alkalmazások a tranzakciók során. Ezek az irányok egyértelműen a hagyományos és államilag ellenőrzött banki megoldások hátrányos helyzetbe kerüléséhez vezettek. Mára az alkalmazások hatására a bankrendszernek fel kell ismernie piaci helyzete romlását és a digitalizálódó piacon kell felvenniük a versenyt a globális pénzügyi szolgáltatókkal. Azonban több területen immáron szinte monopol helyzetben lévő (pl.: PayPal) üzleti megoldásokhoz voltak kénytelenek csatlakozni az eddig a saját piacukon monopol helyzetben lévő bankok és pénzintézetek.

8.1. PayPass

A PayPass a Mastercard termékismertetése alapján „egy érintés nélküli fizetést lehetővé tevő elektronikus megoldás" (Mastercard 2015). Előnye, hogy az ügyfélnek nem kell átadnia a kártyáját és kisebb összegek esetén a terminálhoz való kártya érintés jóval gyorsabb a hagyományos kártyás fizetésekhez képest. A bizonylatot csak a pénztárnak kell megtartania. Világszinten rohamosan elterjedt. Előnyei mellett azt is fel kell ismerni, hogy az ügyfélnek az érintés és a fizetés csak egy mozdulat, és nem jár tényleges pénzforgalommal, és sokkal nehezebben ismeri fel a pénze kiadásának tényét, ezzel gyakoribb és nagyobb összegű vásárlásokra sarkal.

8.2. PayPal

Az internetes vásárlások egyre dominánsabb szereplője a PayPal fizetési megoldása. PayPal mind a vevő, mind az eladó részére a fizetési folyamatot meggyorsítja és leegyszerűsíti. A PayPal lehetőségeit jól bemutatja a Mobilaréna tanulmánya, amely részletesen prezentálja a webshopok (Mobilarena, 2015) üzemeltetőinek a komplett rendelési folyamat automatizált végrehajtását. A felhasználó kiválasztja a terméket és beteszi a kosárba, majd a fizetésnél a PayPal-t választja, akkor a PayPal felületén tölti ki a címet és küld visszaigazolást a rendelésről és intézi a fizetést. Ezzel még több kisvállalkozás számára biztosítanak egy olyan komplex fizetési megoldást, amely tovább növelheti a PayPalt használó weboldalak körét. A vásárló részére előny, hogy a számlára átutalja egy összeget vagy bankkártyát csatol (Tóth Péter, 2015) és arról folyik a tranzakció. A paypal fizetésnek hátránya a magas tranzakciós díj illetve a %-okkal magasabb váltási árfolyam, amely átállítható a saját bank árfolyamára, de legtöbben nem ismerik a módját. Hasonló immáron terjedő rendszerek Barion, Abaqoos, iziSHOP, StormPay rendszere is.

8.3. Bitcoin

Egy virtuálisan létező digitális fizetőeszköz, önálló árfolyamrendszerrel (Wikipedia: Bitcoin, 2016), amelyet alapvetően a kereslet határoz meg. Előszeretettel használják anonimitása miatt az internetes vásárlásokra, vagy akár tiltott szerek és eszközök ellenértékének kiegyenlítésre. A kapott, vagy utalt összeg anonim módon valós pénzzé váltható. Több nemzetközi tőzsdekereskedel-

mi cég is jegyzi árfolyamát és kereskedik vele. Előnye a teljes anonimitás és az állam előli rejthetőség. A megbízhatóságát jelzi, hogy nemzetközi tőzsdei jellegű kereskedelem van rá és mára felhalmozási eszközzé vált sok esetben. Annak ellenére, hogy ezen pénzhelyettesítő eszköz származása és mozgása az állami szervek elől rejtve marad az USA tőzsdéin jegyzett szervezetek, mint pl.: az Ebay elfogadja és kereskedik vele az amerikai hatóságok hozzájárulásával.

8.4. Digital Wallet rendszerek

A legtöbb online kereskedelmi cég saját kereskedésében bevezette a 'digital wallet' rendszert (Wikipedia: Digital Wallet, 2015), és üzemelteti honlapján. A vevők keretösszeget utalva kedvezményeket kapnak vásárlásaikra, illetve vásárlások alkalmával a kereskedők többsége pontokat és kedvezményeket ír jóvá, amelyek tényleges összeggé válthatók a következő vásárlás alkalmával.

9. A digitális piactér

A digitális piactér globális kifejlődése mára vitathatatlan és egyre nagyobb befolyást nyer a globális kereskedelem területén. A hagyományos üzletek és bevásárló utcák egyre kritikusabb helyzetbe kerülnek évről évre. Egy új kereskedelmi modell kialakulásának vagyunk tanúi. Igazából az e-kereskedelem évek óta 20-25 %-os (SZEK.org, 2015) permanens növekedése az e-kereskedelembe belépő új szereplők és új típusú kereskedelmi megoldások terjeszkedése nyilvánvalóan részben a hagyományos kereskedelmi módszerek és piac terhére történik, akik jelenleg nem képesek rugalmasan alkalmazkodni a piaci kihívásokhoz. Új típusú immár világőrületnek számít a 'Black Friday', amely során a világ vezető e-kereskedelmi portáljai magukhoz ragadják a kezdeményezést és 30-70%-os engedményekkel nyomott árakon értékesítik termékeiket, amikor is sok esetben elérik, hogy ezen a napon meghaladják addigi teljes éves bevételüket. Ez még hazai viszonylatban nem ilyen jelentős mértékű kedvezményekhez párosul, azonban jól jellemzi a vásárlói intenzitást, hogy a hazai egyik legnagyobb (Edigital) kereskedelmi portál összeomlott – mint vásárló személyes részese voltam – és napokra működésképtelenné

vált az első magyar 'fekete péntek'-en, majd a következő évben is csak súlyos problémákkal küszködve részlegesen működött, a vásárlók érdeklődése és böngészése, illetve a vásárlások száma és rögzítési hibák miatt.

A Fekete Péntek mind a vásárló, mind kereskedő számára jelentős hasznot hajt. Az immáron dömping áron kínált sokszor elfekvő raktárkészletek kiárusítása, jelentős mennyiségű kurrens cikkel kiegészítve a vásárlók számára jelentős engedményt, míg a kereskedők számára egy új vásárlói szegmens elérését jelenti. Az is igaz, hogy a digitális kereskedelem eme kiemelkedő napja elsősorban a piacvezető webshopok számra jelent kiugró bevételt, de a digitális őrületbe bekapcsolódó és a piacon megjelenő kisebb webshopok viszonylag alacsony marketing költséggel itt képesek megjelenni a kereskedelem kiberterében. Ilyenkor tudnak maguknak nevet, ismertséget kiharcolni és megszerezni az elinduláshoz szükséges vásárlói számot és magukhoz kötni a fizetőképes vásárlói potenciált. Azonban immáron nem csak ez a nap az akciók napja, elsősorban kínai hátterű webshopok meglovagolják a kínai újévet, és legújabban Red Friday néven több hetes akciókat hirdetnek. De módszereik között van az új vásárlók bombázása %-os és 10-50 dolláros kedvezményekkel, valamint a vásárlások utáni elektronikus kommentek 5-10 dolláros kedvezményekkel való dotálása is.

Mára megváltoztak a vásárlók szokásai. A folyamatos mobil hozzáférés, közösségi média reklámdömpingje, befolyásolási metódusai és a közvetlen ismerősök megosztásai és ajánlásai jelentősen determinálják a vásárlói döntések meghozatalának szempontjait. „Ranjit Gill, a Boots drogérialánc IT-igazgatójának értékelés szerint – A vásárló sokkal jobban informált, sokkal kevésbé lojális és úgy lett ár érzékeny, hogy közben elvárja a kényelmet is" (Ranjit Gill, 2014).

Jól fogalmazza meg a hagyományos kereskedelem fenntarthatóságának lehetőségét – mintegy vészharangot kongatva a hagyományos kereskedelmi modellek felett – „Ian McGarrigle, a Kereskedelmi Világkongresszus elnöke: A következő évek igazi kérdése az lesz, hogy hogyan válik a digitális technológia a hagyományos üzletek központi tevékenységének részévé" (Balla, 2014). Jól jellemzi a jelenlegi helyzet megváltozását és jövő vásárlási szokásainak metodikáját Pat Bakey, az SAP kiskereskedelmi üzletágának globális vezetőjének előadásán elhangozott mondat: Ahhoz, hogy meghozzanak egy vásárlói döntést, ma már a legtöbben a telefonjukat veszik először kézbe" (Pat Bakey, 2014).

Itt szeretném bemutatni a teljesség igény nélkül a globális e-kereskedelmi piac főbb szereplőit.

9.1. eBay

Az eBay Incorporated az USA-ban bejegyzett internetes aukciókat lebonyolító weboldal, amelyen globálisan bárki eladásra felajánlhatja termékét (speciális kereskedelmi eljárás alá tartozó terméket kivételével), szolgáltatását aukcióra vagy promt áron. 1995-ös alapítás óta jól teljesítette saját jelmondatát: The World's Online Marketplace (Wikipedia: Ebay, 2015)' Fejlődését két számmal jellemezném 1995-ös indulása után 2004-ben 3.27 míg 2014-ben 17.09 milliárd dollár forgalmat bonyolított le (The Statistics Portal , 2014).

9.2. Alibaba

Kínai érdekeltségű, a világ második legnagyobb kínai érdekeltségű online kereskedelmi viszonteladói oldala. A világ 240 országában (Wikipedia.org: Alibaba_Group 2015) forgalmaz árukat. 1999-es alapítása óta elérte, hogy cégcsoport értéke 2015-ben már 212 milliárd dollárt. Azonban az Alibaba.com már jóval meghaladja az e-kereskedelem hagyományos határait. A busines-to-business platfromjaival Kínában és a kapcsolódó vásárlók számára a hagyományos kereskedelmi szolgáltatásokon felül komplett szolgáltatást nyújt. Biztosítja az egyének és kisebb cégek részére a nagykereskedelmi áron való vásárlást, szállítási rendszerével, ebank-jának hitel lehetőségeivel, és a csatlakozott felhasználók számára felhő- és adatbányászati szolgáltatások biztosításával. Gyógyszer kereskedelmi oldala is rendelkezik, amely a kínai gyógyszeripar termékeit juttatja el a világ számos pontjára, illetve bevezette saját flash oldalát, amely akciós termékek forgalmazását látja el. Rendelkezik saját ár-összehasonlító rendszerrel, illetve magántőke befektetési szolgáltatásokat is nyújt. Az alibaba.com és kapcsolódó oldalai az első komplex busines-to-business kereskedelmi, szolgáltatási és befektetési és e-bank platform a világon.

9.3. Amazon

Az Amazoon.com (Wikipedia.org: Amazon.com, 2015) 1994-ben indított egyik első internetes kereskedelmi platform. Kezdetben könyvek forgalmazását bízta a kibertérre, de ma is egyik fő profilja kibővítve az e-könyvek,

ebook readerek, és dvd-k forgalmával. Ezen felül gyakorlatilag az elektronikus eszközök teljes választékát forgalmazza. A Mobilpocket.com üzemeltető technológiai cég felvásárlásával 2005-ben megalkotta saját e-book reader formátumát és e-book standardokat, amelyek mai napig is piacvezető e-book formátumok. Az Amazon ebook reader-jei mint a Kindle (Amazon.com: Kindle, 2015) mai a világ élvonalába tartozó digitális formátum olvasók és lejátszók. Az amazon azonban mára továbbterjeszkedett a művészet, a játékok területére is. A vezető pozícióban lévő világcég időben felismerte az online zene és a felhőszolgáltatások szerepét a digitális világban és mára a világ egyik legnagyobb online zene szolgáltatója és a magánszemélyek és cégek részére pedig a világon is meghatározó felhő szolgáltójává vált. Várható éves forgalma 2017-ben eléri a 129,954 millió dollárt (Reuters: Amazon.com, 2015). A befektetőnek is egyik kedvelt célpontja a tőzsdén. A 2011 áprilisában még 181,58 dollárt érő részvény mára 556,29 dollárt ér (Reuters: Amazon.com, 2015). Jól jellemzi a céget, hogy ' logóján 2000 óta egy nyíl mutat az A-tól a Z-hez' (Wikipedia.org: Amazon.com, 2015) jelezve, hogy bármilyen terméket képesek szállítani.

9.4. Google play

A Google Play Store régebben Android Market (Wikipedia.hu: Google_Play, 2015) a Google kereső és szoftver rendszerének digitális tartalmat értékesítő szolgáltatása, amely részben online bolt, amely szoftvereket, könyveket, filmeket, és zeneket árul, részben egy felhőben futó online médialejátszó. Sajátossága (Wikipedia.org: Google_Play, 2015), hogy a vásárlás után a termék elérhető a vásárló összes birtokolt eszközén. A szolgáltató 2009-ben 2300 tartalom szolgáltatásával indult mára 2,051,820 tartalom (App Brain, 2016) tölthető le a felhőből. A hozzátartozó google.play digitális tartalom rendszer lejátszó az egyik legelterjedtebb hang és média lejátszó a világ számítógépein, telefonjain és tabletjein.

A fentiek csak kiemelkedő cégei a digitális kereskedelemnek, de mára már az online kereskedelmi cégek és applikációi gombamód szaporodnak versenyre kényszerítve a nagyokat. A feltörekvő cégek, mint az Everbuying.net, vagy a Gearbest.com kidolgozva a teljes világhálóra reklámstratégiájukat és kedvezményrendszerüket – pl. ingyenes szállítás- lassan felosztják és átfor-

málják a világháló kereskedelmi rendszerét –, de nyugodtan állíthatjuk, hogy a teljes kereskedelem hagyományos modelljét is romokba fogják éveken belül dönteni. Csak ha belegondolunk, hogy 2016-ban a Black Friday forgalma az elemzők szerint 11,6 milliárd dollárt volt (Swarup Gupta, 2015). Összehasonlítva Magyarország GDP-jével, ami 2013-ban 138,4 milliárd dollár volt (KSH: GDP, 2014), az jelenti, hogy az internetes világkereskedelem egy kiemelt napja alatt, – amely tulajdonképpen sok esetben az első órákat jelenti – meghaladja egy közép-európai ország 1 havi GDP-jét. Az Alibaba.com a kínaiak Single Day-en 2015-ben már 14,2 milliárd dollár forgalmat (Paul Carsten, 2015) bonyolítottak.

Jól jellemzi a helyzetet Hegyeshalmi Richard tanulmányában, a pozíciók változását tanulmányában miszerint letarolja a világot a kínai Ebay. „A 'U.S. Securities an d'Exchange Commission-hez benyújtott üzleti jelentések szerint csak az Alibaba kiskereskedelmi részlege tavaly 11,3 milliárd megrendelést kapott; 231 millió aktív vásárlójuk volt; 36,7 millió regisztrált felhasználójuk van, több mint 240 országból; 2,8 millió online üzlettel dolgoztak együtt; 5900-nál több termékkategóriában kínáltak árukat; 248 milliárd dollárt költöttek náluk összesen. Ez több, mint amennyit az Amazon és az Ebay együtt összehoztak" (Hegyeshalmi Richard, 2014). A számokból is látható, hogy az Alibaba Group egy év alatt több forgalmat bonyolított le, mint hazánk GDP-nek duplája. Közel annyi online céggel állt üzleti kapcsolatban, mint az EU és NATO tag Litvánia (2,956 millió) összlakossága.

9.5. Business-to-business (B2B)

A B2B alapvetően üzleti élet gyártók és kereskedői között folyó elektronikus kereskedelem (Wikipedia.org: Business-to-business; 2016). Ebben az összetett termelői és kereskedő hálózatban egy adott cég egyszerre lehet vevő és eladó is.

A B2B üzleti szféra kereskedelmének jelentős részét adja. A kereskedelem egy szabályozott keretek között működő kereskedelmi platformon történik. Az üzletben a legfontosabb szereplők az eladó- és vevő vállalatok, elektronikus közvetítő cégek, szállítók és bankok.

A business-to-business összetett termelési láncolatok sokasága, ahol ugyanaz a fél lehet ajánlattevő és elfogadó is. Az „így forgalmazott áruk, termékek, szolgáltatások sokszor keretszerződésekben körvonalzódnak, ebből követ-

kezően nem probléma, ha azokat nem lehet a helyszínen megnézni, kipróbálni" (Cégvezetes.hu: Elektronikus kereskedelem; 2016).

Egy B2B platform létrehozása és üzemeltetése jelentős költséggel jár és a szolgáltatásért kapott illeték sokszor a működés költségei is nehezen téríti meg. Ezért alakultak ki az iparágban koncentrált és szakosodott nagy árumennyiséget hirdető és közvetítő kereskedelmi platformok. A cégek sok esetben csak rövid informális platformot hoznak létre.

A szereplőkön kívül szükség van még megfelelő infrastrukturális háttérre, kommunikációs csatornákra és vállalati belső információs rendszerekre, melyekhez kapcsolódnak a kereskedelmi alkalmazások. Ezek a platformok biztosítják a kereskedelmi tranzakciók objektív és emberi befolyástól mentes lebonyolítását. Előnye, hogy a világ bármely részének áruihoz, vevőihez kapcsolatot teremt a platform időponttól függetlenül, és képes a szállítást, sok esetben a finanszírozást is megoldani a rendeléssel egy időben. Alapvetően három formája alakul ki, mint a nyilvános piactér, a magán e-piactér és a konzorcionális e-piactér. Az utóbbi sajátossága, hogy egy iparágba tartozók próbálják egymás között kereskedelmi kapcsolataikat optimalizálni. A nyilvános piacterek egyre nehezebben boldogulnak, mivel a vállalatoknak egyre fontosabb a beszállító ismerete, ha pedig már ismeri, akkor közvetlenül rendel tőle.

10. Közösségi média a kibertérben

10.1. Facebook hatás

Még egy évtizede elképzelhetetlennek tűnt, hogy a világon önkéntes csatlakozással létrejöjjön egy olyan egymással kommunikáló, életstílust és az életviteli és magán adatokat megosztó, befolyásoló szervezet, amely mára 1,59 milliárd embert tömörít a kibertérben, és ez a szám 2030-ra 5 milliárd emberre tehető (Mark Zuckerberg, 2016) a jelenlegi növekedési ütem tartásával. A „fészező" eleinte tizenéves, mára már minden generációt összefogó közösség egyik jellemzője, hogy életvitelének szoros részévé vált az alkalmazás. Munkahelyüket, kapcsolataikat, szerelmeiket, pihenésüket, nyaralásaikat és egyéb számukra fontos képeket, híreket, vagy recepteket megosztó emberek számára nélkülözhetetlen a kapcsolatok tartása és visszajelzése digitális kom-

munikációs csatornán. A „posztolás" vagy „lájkolás" mára az mindennapi élet fogalommá vált. De már a digitális média is részben ezek alapján ítéli meg egy ember, egy hír, egy feltöltött videó vagy egy szervezet virtuális értékét a digitális térben. Mára már ezek a fogalmak sok százmillió ember életvitelét változtatták meg részlegesen beleépülve a nyelvükbe, társadalmi szokásaikba és determinálják társadalmi elfogadottságukat, sőt befolyásolják karrierjüket is. Ez a generáció nem csak csatlakozik az internethez, hanem gyakorlatilag folyamatos netkapcsolatot tart fent, és ezen kommunikál és ezen követi figyelembe kapcsolati körtébe tartozó emberek, életét, véleményét, kapcsolatainak alakulását, szokásait, vagy éppen jelenlegi helyzetét. A rendszer alkalmas, hogy az egyénhez tartozó minden emberrel egyszerre online kapcsolatban legyen és több emberrel is fenntartsa párhuzamosan a kommunikációs kapcsolat. Jól jellemzi az ismeretségi körömbe tartozó fiatalok mondata a jelenleg Facebook-generációnak nevezett fiatalok megítélését a helyzetről miszerint „Ha nem vagy fenn a Fészen NEM LÉTEZEL!"

A Facebook nem csak a személyek szociális kapcsolatinak hálóját térképezte fel, hanem beleivódott a mindennapjaink gazdasági rendszereibe is. Mára a Facebook komoly üzleti sikereket ér el marketing tevékenységével célzott reklámjaival és az ahhoz kapcsolódó a Facebook profilon értékesítő web-áruházak láncolatával. Ismeri igényeinket, pihenési, utazási, vásárlási szokásainkat, a hozzánk kapcsolódó háló tagjainak szokásait, igényét és mindezt adatbányászati módszerekkel felderítve folyamatosan bombáz minket a kapcsolódó hálózatunk szintjén célzott reklámjaival. Sok esetben felugró kapcsolódó lapokkal, amelyek lezárása komolyabb odafigyelést igényel, tehát még egyszer át kell nézni a hirdetést, hogy le lehessen zárni, ezzel elérve, hogy biztos tudatosuljon bennük a megcélzott termék vagy szolgáltatás, vagy szolgáltató. Ha egyszer valaki megnyit valamit érdeklődési körében az biztos lehet benne, hogy a következő napi csatlakozáskor a téma értékesítéséhez kapcsolódó internetes kapcsolat meg fog jelenni. A Facebook gyakorlatilag mindent megjegyez tagjairól, akár akarják, akár nem.

Amikor Max Schrems osztrák joghallgató beperelte a Facebookot, hogy adják ki részére engedélye nélkül milyen adatokat gyűjtöttek róla, a per megnyerése után a Facebooktól megkapott információk 1222 oldalt tettek ki nevezett személyről. A bíróság előtt kimondásra került a „Facebook egyszerűen

nem kér hozzájárulást a magánadataink „sokoldalú" felhasználásához, csuklás nélkül átadja a felhasználók adatait, képeit, videóit, közösségi tevékenységének információit az NSA-nak, az általunk törölni vélt anyagokat valójában nem törli, folyamatosan elemzi a felhasználói szokásokat, keresőjét nyugodtan tekinthetjük kémszoftvernek is" (Hirado.hu, 2015).' Egyre több gondja van a Facebook-nak a személyi- és biometrikus adatok gyűjtésével. Az arcfelismerő rendszert alapfunkcióban bekapcsolva vezették be anélkül, hogy ténylegesen a felhasználók hozzájárultak volna. Bárki, mind a felhasználó, mind, aki a felhasználók által feltöltött képeken szerepelt gyakorlatilag azzal kellett szembesülnie, hogy biometrikus adatait engedélye nélkül feldolgozták és eltárolták. Ettől a pillanattól kezdve a világon bárhol felismerhetővé és azonosíthatóvá vált. Először az Európai Unióban kellett kikapcsolni a biometrikus adatok gyűjtését, mára már a BIPA (ilga.gov: BIPA, 2016) alapján az amerikai bíróságok befogadták a Facebook-ot perelők beadványát (Sruthi Shankar, 2016).

A Facebook alkalmazás(ok) betörése a mindennapi életbe, jelentősen megváltozattam kommunikációs szokásainkat. Ez mára már mind a magánéletben, mind a politikában érvényesül. A 'Facebook generáció' rengeteg időt tölt a képernyőt bámulva, amely a hagyományos értelemben vett emberi kommunikáció rovására történik. Folyamatosan változik a digitális alkalmazások hatására a barát és az ismerős fogalma. Régebben barátságok alapvetően csak személyes kontaktusokon alakultak ki, mára úgy is kialakulnak barátságok, sőt párkapcsolatok is, hogy előtte természetes személyként nem is ismerték egymást. A személyes aktivitás folyamatos posztolása, az érdeklődési kör, a munka és a személyes kapcsolatrendszer publikálása révén létrejövő kiber kapcsolatok lehetővé teszik, hogy későbbiekben kialakuljanak személyes kapcsolatok is. „Két dolog viszont nagyon is megváltozott, ha ismerősről, ha barátról van szó. Egyrészt a folyamatos tájékozottság: mindent tudunk még a legtávolabbi ismerősről is. Kivel jár éppen, hol dolgozik, szereti-e a munkáját, gyereke született-e, milyen zenét hallgat, melyik koncerten járt vagy éppen hol ebédelt és kivel. már nincs szükség személyesen fitogtatni, hogy ki mit ért el az életben, azt úgyis tudja mindenki. valódi kapcsolatok sokkal intenzívebbek lettek. Folyamatosan információt küldünk és kapunk célzottan, az üzenő falon kevésbé célzottan, de mégis állandó a kapcsolattartás. Ezzel együtt azonban

sokkal könnyebb megszakítani is egy ismeretséget. Elég törölni az ismerősök közül, vagy egyszerűen nem keresni többet, így nem kell bajlódni a szálak elvarrásával" (Árki Noémi, 2015).

Ha megnézünk egy átlagos profilt megállapíthatjuk, hogy legtöbb facebookozó megadja email címét, telefonszámát, lakhelyét, születési idejét, iskolai végzettségét, hobbiját, érdeklődési körét mindezzel megkönnyítve a már fent említett marketing információ gyűjtését és a célzott reklám tevékenység hatásossá tételét. A legtöbb felhasználó posztolja képeit, szórakozását, kirándulásait, nyaralásait és hangulatát, kapcsolati állapot változását. Ezek az információk valójában barátainak vagy azoknak hitt facebook kapcsolatainak szólnak, akik ezek alapján ítélik meg, fogadják el vagy utasítják el a személyt.

Sok esetben azonban ezen információk akaratlanul is olyan kezekbe kerülnek, amelyeket a facebookozó nem is gondol. Mára a munkahelyek sok esetben ellenőrzik dolgozóik profilját, és döntenek esetleges alkalmazásukról vagy elbocsájtásukról. Ezeket az információkat adatbányászati technológiákat alkalmazó cégek részére eladják és ezzel sok esetben potenciális piaci vagy politikai célok elérésének piaci szegmensei lehetnek, vagy éppen állami nyomozati szervek vizsgálatának részeseivé válhatnak. Egy akaratlan információval akár segíthetik a bűnözőket is bűncselekményeik elkövetéséhez anélkül, hogy felfognák, hogy barátaiknak szóló fénykép, videó, személyes adat vagy véleménynyilvánítás milyen elektronikus folyamatokat indít el és milyen információhalmazt biztosít tulajdonképpen illetéktelenek részére.

Sok esetben azonban a felhasználók szándékosan hamis információkkal posztolják ki énjüket és szokásaikat. Ezek hatásairól a mai napig nem sok felmérés jelent meg.

Az elmúlt 10 évben egy teljesen új iparág jött létre a közösségi média és keresőrendszerek elterjedésével, anélkül, hogy valójában nem is ezek a cégek teremtették meg, hanem a gazdasági és politikai igény hívta létre ezeket. Az adat-, szöveg-, és webbányászat, valamint a hálózatelmélet és a virtuális valóság alkalmazása a mindennapok részéve vált a kibertérhez kapcsolódó cégek piacán. „A márkák nem engedhetik meg maguknak, hogy ne legyenek jelen, ami magával hozta olyan szakmák, területek megjelenését, mint a közösségi média marketing, a célzott reklámozás, vagy a kifejezetten közösségi médiára specializálódott ügynökségek. Azért a Facebook sem járt rosszul ezzel, bevé-

teleinek 46%-át ugyanis a reklámok szolgáltatják. „A márkák tehát könnyen elérik közönségüket, a Facebook ezzel jól keres, viszont ott van a másik oldal is, a célpont: a felhasználó, aki mostantól ha elégedetlen, egyetlen Facebook poszttal lejárathat egy márkát az egész világ, de legalábbis több száz ismerős előtt, így a játék kétoldalúvá válik" (Árki Noémi, 2015).

Mára a politikai élet szereplői is aktívan használják a kinyert felhasználói vélemény adatokat. Ha közvetve is, de sok esetben mind a gazdasági társaságok, mind a politikai céljukat megvalósítani kívánó politikai szereplők kihasználják, hogy a hírportálok a Facebook alapján döntik el a hír jelentőségét. Tudomásul kell venni, hogy a felhasználók többsége az internetet használja mindennapi tájékozódásra, és mára már a folyamatosan a mobil eszközein a Facebookon lógó 1,5 milliárd ember innen kapja az információt és természetesen a fontos hírekkel együtt megjelenő jól megfizetett reklámajánlatot is.

Egy másik olyan jelenségre is fel kell hívni a figyelmet, amely a nagy sebességű elektronikus kapcsolattartás és széleskörű kapcsolati háló kapcsán megjelent. Mind a politika részéről, mind a civil szervezetek vagy szerveződések részére megnyílt a nagy sebességű és az állami kontrolt viszonylagosan elkerülő szerveződés lehetősége. Ilyenek a voltak hazánkban a hallgatói önkormányzatok tüntetése, vagy az internet adó elleni tüntetés önszerveződése, de az illegális gyorsulási versenyek szervezői előszeretettel használják ezt a formát a helyszín utolsó pillanatban való megadására.

Az elektronikus kapcsolattartásnak az állam azonban az előnyeit is évezi, mivel sok esetben civil önszerveződések jönnek létre, egy-egy téma (környezetvédelmi, jótékonysági összefogások), érdeklődési kör, vagy területi egység (pl. lakóhely) kapcsán. Jó példák a városvédő, vagy kulturális önszerveződések, azonos érdeklődési körű személyek tematikus szerveződései is.

10.2. Chat eszközök

Olyan online elektronikus társalgási forma (Wikipedia.org: Online_chat, 2016), amely a publikus chat csatornákon (internet, vagy szövegküldési társalgási forma, amely két vagy több ember között jön létre. A chat programok egy része hang alapú, más részük szöveg alapú, vagy ezek keveréke. Egyik fontos jellemzőjük, hogy a felek kölcsönös jóváhagyása szükséges hozzá. Ilyen prog-

ramok a Windows Live Messenger, Google Talk, Viber. Egyik legjobban fejlődő világszerte elterjedt részben ingyenes alkalmazás a Skype (Wikipedia.org: Skype, 2016), amely a video kapcsolat lehetőségét is tartalmazza. Mára üzleti alkalmazásával videó-konferencia hívható össze és elő szóban lebonyolítható gyakorlatilag a szükséges adatbiztonság megteremtésével. Ez a lehetőség biztosította az üzleti életbe történő széleskörű elterjedését, valamint az, hogy a drága roaming mobil rendszereknek ingyenes vagy jelentősen olcsóbb konkurenciájává vált. Jó minőségű kép- és hang kommunikációt biztosítva korlátlan számú végpont között, gyakorlatilag bármilyen időtávban. Meg kell még itt említeni az egyre agresszívebben növekvő 'Facebook Messenger'-t, amely, mint a chat lehetőség beépítésre került Facebook alkalmazásba, ezzel azonnal kommunikációt biztosítva az alkalmazók között. Ezzel a chat funkcióval egy csapásra létrejött egy olyan informatikai hálózat, amely potenciálisan képes összekötni közel másfél milliárd embert. Érdemes végig gondolni, hogy milyen potenciálok vannak egy másfél milliárd embert összekötő kommunikációs hálózatban, vagy ennek kiesése, blokkolása milyen zavarokat okoz a gazdaságban, a kommunikációban, vagy esetlegesen az állam vagy pénzintézetek működésében.

11. A felhő alapú számítástechnika

A felhő alapú szolgáltatások (Wikipedia.org: Cloud_computing, 2015) az utolsó évtized informatikai egyik leggyorsabban fejlődő területe. Lényege, hogy a felhőt igénybe vevőnek nem kell adatait saját informatikai eszközein tárolnia, azok üzemeltetéséről, védelméről gondoskodnia. Utolérhetetlen előnyt nyújt a nemzetközi gazdasági életben, hogy „nem vagyunk egyetlen számítástechnikai eszközhöz kötve. Ugyanígy eltűnik az a régi félelem is, hogy elfelejtünk magunkkal vinni a gépen egy fontos dokumentumot, nem találunk egy kiemelt fotót, vagy hiányzik az otthon felhalmozott lemezgyűjteményünk" (humansoft.hu/Alkalmazas_szolgaltatas). A felhő lehet egy helyi hálózaton vagy az interneten. A felhőt általában a http protokolon keresztül biztosítja a szolgáltató. Ugyanígy a szükséges szoftvereket és platformokat is biztosítja a felhő üzemeltetője. A hardvereket, a szoftverek nagy

részét, illetve az üzemeltető személyeket sem kell a felhő igénybe vevőjének biztosítania. Így a felhővel jelentős humán és hardver költség takarítható meg. Ugyanakkor mivel a felhőszolgáltatások általában nagy nemzetközi cégek, így a szolgáltatások színvonalának is folyamatosan fejlesztésével és a beruházások biztosításával a felhőszolgáltatás is a nemzetközi élvonalban marad.

A felhő lehet publikus, privát, hibrid vagy közösségi felhő. Igény szerint privát felhő is kiépíthető, ahol a privát felhő tulajdonosa biztosítja a szükséges eszközöket, illetve az informatikai személyzetet. Speciális lehetőség a tárhely szolgáltatás, ahogy a szolgáltató a tárhelyet biztosítja.

Előnyei közé sorolható, hogy helyfüggetlen és bárhonnan könnyen elérhető, amely nagy előnye a nemzetközi üzleti életnek. A felhő méretezhető. A cégek növekedésével a bérelt felhő mérete is rugalmasan növelhető, vagy igény esetén privát felhővé alakítható, illetve igény esetén a szükséges többletkapacitás projektekre vagy időszakokra is bérelhető. A felhő további előnye, hogy megbízható, biztonságos, és jogtiszta. A felhőszolgáltatás igénybe vevője megtakarítja a hardvereszközök megvásárlásának és az üzemeltetésének költségeit azonban azt is figyelembe kell venni a kialakításánál, hogy a hálózati forgalmi költségek és a bérelt kapacitás költségei megjelenik.

A felhő-élmény létrejötte új perspektívákat nyit meg a tudásmegosztás, a közös munka, a közösségben való létezés és a kommunikáció területen. A felhőszolgáltatások „jelentősen kevesebb kockázati tényezővel viszont több beépített garanciával bírnak" (Humanszoft.hu: Felhőszolgáltatások; 2016).

12. A virtuális valóság

Virtuális valóságon a „multimédiás eszközökkel vagy számítógéppel szimulált valóságot értjük" (Wikipedia.org: Virtual_reality; 2016).

A VR eszközt viselő személy(ek) számára egy fizikai jelenlét van szimulálva egy nem létező elképzelt digitális világban, amely lehetővé teszi számukra, hogy kölcsönhatásba lépjenek az elképzelt világ elemeivel. Virtuális valóságban mesterségesen manipulálhatók az érzékszervi tapasztalatok, amely magában foglalja a mozgást, a látást, a tapintást, a hallást és a szaglást.

Virtuális valóság alkalmazása már csak a 2016 évet alapul véve is exponenciális fejlődésen ment keresztül. Még egy két éve csak kevesek speciális oktatási és tervezési eszközéből jelenleg mára már számos területen elérhetővé vált annak köszönhetően, hogy 100$-tól megkaphatók a 3D virtuális szemüvegek. A fejlődéshez hozzájárult nagy mobilgyártók és szolgáltatók appjai, valamint a GO-PRO jellegű és 360 fokos rögzítésű kamerák és 3D mobiltelefon kamerák elterjedése. Mára már az orvostudomány VR alkalmazásai, az oktatás, az esemény és élményrögzítés módszerei is gyökeresen átalakulóban vannak ebbe az irányba. Megjelentek azok a VR és 3D alkalmazások, ahol más helyszínen tartózkodó orvos team-ek közvetlenül is beavatkozhatnak a műtét során, vagy más kontinensen tartózkodó orvosok és nézők élőben 3D-ben és 4K felbontásban nézhetik a műtétet, mintha jelen lennének a helyszínen.

Igen érdekes alkalmazások a kerültek kifejlesztésre, a Samsung és Facebook együttműködéséből (Lauren Hockenson, 2016), amelynek terjesztése reklámozása természetesen elsősorban a Facebook közösségi média megosztására és a youtube-ra épül. A „360 fokban rögzített filmek és eszközök és a VR eszközök elterjedése gyökeres változást hoz az elkövetkező évek tartalomfogyasztási szokásaiban." (24.hu: Tériszonyos videóval kampányol a Facebookon a Samsung, 2015). Kifejlesztésre került a Samsung Gear VR 3d szemüveg és alkalmazások a BeFearless projekt (Samsung.com: Launching People #BeFearless, 2015) keretében, amely segítésével néhány hét alatt legyőzhetővé válik az eddig nem vagy nehezen gyógyítható tériszony (Vrscout.com: Projects Overcoming Your Fear of Heights with Samsung Gear VR 2016); vagy szorongó emberekben kifejleszthető a tömeg előtti beszéd (Youtube: Launching People, 2016).

Érdekes látni, hogy a Samsung 3D virtuális teret előállító csúcstermékének terjesztését a közösségi médiára, elsősorban a Facebookra és a youtube-ra bízza, és itt kampányol a témában. Mára tudomásul kell venni, hogy ez egy 1,59 milliárd főt összefogó digitális szervezet (Mark Zuckenberg, 2016), ahol a megosztások révén a Higtech termékek néhány óra alatt közismertté válhatnak megfelelően célozott célközönséghez eljuttatott reklámmal, vagy baráti megosztással és a megfelelő minőségű youtube video reklám anyagokkal megtámogatva. Ilyen esetben mire a konkurencia elkezdené a fejlesztést, már le is cseng a projekt vagy közel monopolhelyzetben van a gyártó.

A VR alkalmazások fogják rövidesen determinálni a mobil kommunikációt, a játékipart, oktatást, a kiképzést, a tervezést (pl., tárgyakt, épületek, várostervezés), a filmipart, a terápiás módszereket és az orvosi alkalmazásokat.

Azonban más területeken is beszálltak a cégek a VR robbanás versenybe. Ugyanígy piacra dobta saját termékét a HTC is VIVE (Htcvive.com, 2016) néven. Itt szeretném érzékeltetni ennek a piacnak az intenzitását és nagyságát. A VIVE piacra dobását követően „10 perc alatt 15 ezer darabot adtak el digitálisan 12 millió dollár" (Pcword, 2016) értékben.

A Microsoft Hololens (HVG: Minden kiderült, 2016) kamerák és érzékelők teljes repertoárját beépítette a szemüvegbe, sőt teljesen önállóan működő számítógép is került a HOLOLENS-be, amely alkalmasság teszi, hogy viselője órákon keresztül helyétől függetlenül összemossa a virtuális teret a valódival. Ezzel újabb fejlesztések és távlatok nyíltak meg virtuális valóság bármely környezetben való alkalmazása előtt.

A VR robbanása során teljesen ismeretlen cégek léptek elő a semmiből és rohamléptekkel fejlesztik eszközeiket – mint a Zhuoyuan 9D Virtual Reality VR Simulator a teljes körűen reális élmény nyújtó autó (Guangzhou Zhuoyuan Group, 2016). Ugyancsak roham léptekkel fejlődik a „VR oktatás" (Cybersceince3d: Bringing Learning to Life in VR 2016) is, mint az oktatás egy új igen hatékony dimenziója. Előnye, hogy az oktatott személy érzékelését kontrol alatt tartja. Az oktatott személy nem a tanul a hagyományos értelemben, hanem a megtanulni szánt folyamat terében létezik, mozog, kommunikál és érez. Így átéli a tényleges tevékenységet, amely rögzítődik emlékeiben, mintha valóban megtörtént volna vele. A „VR eszközei" számítógépekhez (Getfove.com:The World's First Eye Tracking virtual reality headset, 2016), mobiltelefonokhoz (Samsung.com:gear-vr 2016), illetve már a játékkonzolokhoz Morpheus-projekt (Wareable.com: Project Morpheus Feature, 2016) keretében kifejlesztett olyan kisméretű 3D szemüvegek, amelyek létrehozzák bárhol a felhasználó számára virtuális valóságokat, még akkor is, ha mozgásban van.

A megjelenést követően az eszközökhöz a gyári alkalmazásokon kívül a külső fejlesztő cégek részéről haladéktalanul megkezdődnek a fejlesztések. Elsősorban a játék és filmipar, de a geológia, orvostudomány, oktatás, GPS és térképes és nyilvánvalóan a katonai alkalmazások sem késlekednek. Gyakorlatilag egy hónapon belül legtöbb esetben már kész alkalmazáscsomagok

kaphatók az eszközökhöz. A fenti fejlődési sebességet látva mára megjósolhatatlan a fejlődési kimenetele és iránya a VR és 3D eszközök és alkalmazások területén. Az azonban biztosan állítható, ha időben nem csatlakozunk a piaci trendekhez és lehetőségekhez, mind hardver mind szoftver területen jelentős piaci hátrányba kerülhetünk, amelyre a speciálisan garantált jogok miatt rövid időn betörni már lehetetlen lesz. Csak a piac vásárlói lehetünk és nem aktív szereplői.

Azonban fel kell ismerni a negatív oldalt is, hogy az a függőség, amelyet a számítógépek és a telefonok alkalmazási jelentenek a virtuális valóságban még fokozottabban függővé és befolyásolhatóbbá tehetnek alkalmazókat. Ez különösen abból a szempontból lehet veszélyes, hogy a virtuális valóságban érzékelésük és valóság megítélésük elektronikusan manipulálásra kerül.

Azt azonban nyugodtan kijelenthetjük, hogy ezen eszközök jelentősen elősegítik az oktatást, a képességfejlesztést, és a kommunikáció hatékonnyá tételét, és jelentősen felgyorsíthatják a tudományos kutatást.

13. Adatbányászat és big data eszközök alkalmazása politikai és gazdasági célok érdekében

Az e-kereskedelmi forradalom hátterében egy új iparág is megszületett, és mára már kitörve a kereskedelem holtteréből, immáron a gazdaság több területén is megjelent, és a mára egyre jelentősebb a szerepe a stratégiai-, és az operatív üzleti döntések során. A nagy mennyiségű kereskedelmi tranzakció online adatainak feldolgozása, és a tömegesen megjelenő internetes keresések adatainak gyakorlatilag online értékelése és a vevői szokások elemzésének igénye jelentősen előtérbe helyezte a statisztikai programok alkalmazását és létrehozta az adatbányászati eszközöket, majd az hatalmas mennyiségű online adatfeldolgozás igénye kialakítottat a Big Data (Wikipedia.org, 2016) programok alkalmazását. Ezek a gazdasági adatfeldolgozó és elemző programok gyakorlatilag évek alatt szétterjedtek a gazdaság minden területére. Mára már a kereskedelmen kívül a bankrendszer, a biztosítás, az egészségügy valamint a gazdaság egyéb területein is teret nyertek a Big Data, adat-, és szövegbányász programok és komplex alkalmazások. Mára ezek az alkalmazások az informatikai eszközök jelentős technikai fejlődésének, a felhőszolgáltatások megjelenésének illetve az alkalmazott programok elterjedésének és részben ingyenessé tétele következtében az üzleti alkalmazások szintjén megjelentek

a kkv-szektorban és tért nyertek az informatikai- és gazdasági oktatásban. A mind szélesebb szakember gárda megjelenésével prognosztizálható a gazdasági alkalmazások mind szélesebb körben történő alkalmazása és elterjedése. Ezek az adatbányász programok (Wikipedia.hu: Adatbányászat, 2015) alkalmasak arra, hogy a nagy mennyiségű adatokban megfelelő szakembergárda közreműködésével és a beépített algoritmusok mentén feltárják az összefüggéseket a numerikus adathalmazokban és előre jelezzék a szükséges gazdasági információk elérésének lehetséges megoldásait.

Ilyen megoldások a strukturált adatbányászat, amely a meglévő adatok alapján mintákat és trendeket keres (Dr. Bodon Ferenc, 2010), a webbányászat (Jaideep Srivastava, 2015), – amely pl. a web folyamatok, kattintások időbeli egymás követések mintáit elemzi-, a szövegbányászat (Dr. Kovács László, 2015), amely a kommunikáció és média kommentek kommunikációk szöveg és adatelemzése alapján alkot képet a potenciális vevőkről vagy termék megfelelősségről. Ide tartozik még a biometrikus adatok bányászata (Francisco Gutiérrez, 2016), amely az egér mozgás vagy billentyűzet leütések alapján azonosítja a célszemélyt vagy a potenciális vevőt és a megfelelő marketingcél irányába tereli. Eszközeik közül egyre jobban fejlődik a prediktív elemzés, amelynek segítségével a „speciális jellemzők alapján kategóriákba sorolva adatainkat, a múltbeli viselkedést alapul véve valószínűsítünk („előre megmondunk"– innen a prediktív elnevezés) egy jövőbeli viselkedést adott helyzetben" (Adattudomany.blog.hu, 2014).

A szakterület egy speciális eszköze a HADOOP (Sas: Hadoop, 2016), nyílt forráskódú adattárolási- és feldolgozási technológia, amely különösen alkalmas eltérő adattípusok befogadására. Osztott file kezeléssel és alkalmazásokkal képes arra, hogy egy átlagos méretű számítógépekre is telepíthető legyen és alkalmazható legyen akár magán, akár kisvállalati környezetben a szükséges adatok kinyerésére és elemzésére. Az adatbányászat gyors elterjedését és oktatását egyre több szabad licencű és forráskódú eszköz segíti. Ilyen a szabad forráskódú szakterület specifikus programozású 'R-nyelv' (Wikipedia.org, 2016), illetve a részlegesen szabad felhasználású adat-, és szövegbányász programok, mint a Data Miner illetve Weka programcsalád.

13. A hálózat elmélet fejlődése, tevékenységek előre jelezhetősége, egyén és gazdaság behatárolhatósága, sebezhetősége

A kibertér kutatásának és egyik legjelentősebb hazai sikerének a hálózatelmélet megalkotásában kulcsszerepet játszó Barabási Albert-László (Energiapedia.hu: Barabási Albert László 2016) professzorhoz köthető, aki a Northeastern Egyetem Komplex Hálózati Kutatóközpontjának (Center for Complex Network Research) vezetője, és mind az Amerikai Fizikai Társaság, mind a MTA tagja. A fizikus kutató a skála független hálózatok felfedezésével és a komplex hálózatok kutatásával vívta ki hírnevét az informatika és a tudomány világában. Könyvei a „Villanások" (Barabási Albert-László 2010) és a „Behálózva – a hálózatok új tudománya" alapműként szerepel a világ vezető informatikai oktatási intézményeiben a hálózatkutatás oktatása területén. A Word Wide Web topológiájának bemutatása, és a nem lineáris hálózatok szisztémáinak feltérképezésével feltárta a hálózati komponensek összefüggéseit és kapcsolatrendszereit. Egy szociológiai, gazdasági, biológiai, sejtszerkezeti, orvosi tudományterületeken is alkalmazható új tudományág körvonalai bontakoztak ki a látszólag informatikai magyarázat mögött. Többek között alkalmazzák a DNS lánc és a sejtkapcsolatok leírása során is. Az internet feltérképezésével és a „Six degrees of separation" et felhasználó (Wikipedia.org: Six_degrees_of_separation 2016) gyakorlatban alkalmazható hálózatokat és kapcsolatrendszerüket elemző- és feltérképező elmélet és a kapcsolódó szoftverek létrehozásával bebizonyította, hogy bárki kapcsolatba hozható bárkivel egy ismeretségi láncon keresztül, melyben a két végpont között maximálisan öt elem van (Wikipedia.hu: Hat lépés távolság 2016). Felismerte, hogy „egy növekedésben lévő hálózatban akkor beszélünk preferenciális kapcsolódásról, ha egy csúcs kapcsolatgyűjtő képessége a már összegyűjtött kapcsolatainak számával arányosan növekszik" (Barabási Albert-László, 2010). Ezeket a hálózatelméleti alapösszefüggéseket alkalmazva éri el a Facebook hatalmas sikereit, ezekre alapulnak reklámkampányok, elektronikus kereskedelmek és banki értékesítési rendszerekben is. „A bankok biztosítók és kereskedelmi rendszerek részben ez alapján döntenek az ügyfelek megszerzése, az árazás és az ügyfélérték meghatározása kérdésében". (Benedek Gábor-Lublóy

Ágnes-Szenes Márk, 2007) Egyik fontos jellemzője, hogy nagy biztonsággal előre jelezhetővé váltak az egyén mérhető viselkedési szokásai, amelyet mind az állam, mind a kereskedelmi alkalmazások felhasználnak. A hálózatelmélet alkalmazható a turisták utazási szokásainak feltérképezésére, vagy a pénzmozgások figyelésre és előrejelzésére, de nem utolsósorban a terrorista sejtek felderítése is lehetővé vált a megfelelő alkalmazásokkal és matematikai módszerekkel.

14. Irányított kiber befolyásolás

Egy másik olyan jelenségre is fel kell hívni a figyelmet, amely a nagy sebességű elektronikus kapcsolattartás és széleskörű kapcsolati háló kapcsán megjelent. Mind a politika részéről, amely részére a vezető digitális hírportálok tulajdonjogának megszerzésével, illetve politikai eszközök alkalmazásával megnyílt a lehetőség a kiber térben mozgó embertömegek gyors tájékoztatására, politikai nézeteik befolyásolására vagy akár félrevezetésükre. A gyakorlatilag online hírportálok és digitális közösségi média azonnali hírszolgáltatása lehetővé teszi lakosság széles körének gyors politikai befolyásolási lehetőségét, a tények többségében objektív, de a politikai irányultságnak megfelelő megítélés szerinti bemutatását. A fenti módon megismert hírről alkotott nézet megváltoztatása komoly feladatot ró az igazságot más formában tálaló és sokszor a tényleges valóságot bemutató média elemek vagy személyek számára. Ugyanakkor mind a civil szervezetek vagy annak álcázott önszerveződések részére is megnyílt a nagy sebességű és az állami kontrolt viszonylagosan elkerülő szerveződés és gyors publikáció lehetősége. Gondoljuk itt például a magyarországi internet adó ellenes tüntetés megszervezésére, vagy az egyes politikusok illegális tevékenységét feltáró riportokra, vagy a mostani migrációs hullám melletti, vagy elleni állami és ellenzéki vagy éppen magán befolyásolás reklámjaira, posztjaira.

Itt azonban felmerül az a kérdés is, hogy valóban jól értékelik-e a szervezők az eredményeket, mert sok esetben már egy 'lájkot' is aktív csatlakozásnak ítélnek meg vagy annak, hogy a lájkoló ténylegesen szimpatizánsa a hírnek vagy eseményeknek. Sokszor az a valóság, hogy az adott híren, tevékenységen vagy csoporton megjelenő lájkolás pusztán a digitális médiaszokások rutinszerű

alkalmazása az egyén részéről. Másrészről a mai tizenévesek és közben felnőtt mára huszonéves generáció megítélésem szerint tévesen rögzült Közösségi kapcsolatokat kifejező eszköze részükről az állandó – sokszor értelem nélküli – lájkolás pusztán azért, mert Közösségi hálójába tartozó emberek már szintén kapcsolódtak. Valójában, ha a lájkolónak a tényleges politikai- vagy vásárlási döntését lemérjük hosszabb távon, a tények jelentős eltérést mutathatnak a lájkolási szokásaikhoz képest az esetek jelentős részében.

Vannak emberek, akik csatlakozásaikkal egy adott baráti társaság tagjához, egy adott témához vagy szervezethez csatlakozással szeretnének társadalmi ismertséget, vagy még inkább társadalmi elismertséget szerezni, és ezen keresztül vélt vagy valós előnyöket megszerezni, vagy ezen a módon az adott közösség részéve válni saját érdekeik érvényesítése érdekében. Ez mára egy adott személy megismerésétől, a nyilvános politika csatlakozásig mindenre kiterjed.

A kiber befolyásolás igen tág körű folyamat. Alkalmazható egy adott egyénhez való közeljutásra, egy termék eladására, személyek befolyásolásra gazdasági vagy politikai célok elérése céljából vagy akár személyes vagy ipari adatok megszerzésére. Az adott személyes-, gazdasági vagy politikai célok elérésére bevetésre kerül a teljes kiber eszköz struktúra, amelynek eszközeit gátlástalanul és sok esetben kontrolálatlanul felhasználásra is kerülnek semmibe véve az egyént, az egyén szuverenitását, vagy az egyén adatainak védelmét. Az egyént úgy jellemezhetünk legjobban a kiber térben, hogy az egyén csak egy adat, a kiber-tér egy felderítendő eleme, amelynek a megszerezhető adatait és szokásait többségében akaratán kívül felhasználják. Ez akkor is megtörténik, ha sok esetben látszólagos jogi belegyezése elektronikus csatlakozásával adott is, holott vagy nem erre, vagy nem teljes körűen minden adatára írta alá a jóváhagyását. Ugyanígy a kiber tér teljes spektrumában a cégek is adatait is felhasználják a konkurencia nyilvános adatainak elemzésétől kezdve, a működési terület kereskedelmi láncához csatlakozó cégként a szakterület megismerésére. Azonban, ezek az adatok a kiber tér árnyoldalán is felhasználhatóak gazdasági-, kereskedelmi- vagy politikai célok megvalósítására, vagy éppen az állami ügynökségek aktív- vagy hallgatólagos hozzájárulásával végzett ipari-, biztonsági-, és katonai kémkedés végrehajtására. A német hatóságok szerint több tízmilliárd eurós. (Sg.hu: Több tízmilliárd, 2014) nagyságrendű kárt okoz a német vállalkozásoknak az informatikai módszerekkel végzett ipari kémkedés.

15. Összefoglalás

A jelenleg élő generáció szemlélője és egyben résztvevője a digitális gazdaság rohamos elterjedésének. Közel két évtized alatt globálisan is mérhető drasztikus változások álltak be a kommunikációban, a digitális tartalmak elérése és a kibertér fejlődése területén. Új gazdasági modellek jöttek létre, ezzel párhuzamosan hagyományos iparágak mentek tönkre, vagy kellet a megújulniuk. Felnőtt egy digitális generáció, és mára már a mindennapok részévé tették a digitális kommunikációt, a digitális médiát, és a digitális kereskedelmet. Azonban az őket követő generáció már elképzelhetetlennek tartja életét a digitális technika és a folyamatos kapcsolattartás nélkül. A 'Facebook-generáció' életét, kapcsolatait, igényeit jelentős részben a digitális kapcsolattartás során ért impulzusok, reklámok, és kapcsolatok határozzák meg. Az emberek többségének igényeit az egyre nagyobb tudású kommunikációs eszközökön keresztül irányítják és befolyásolják. Ezt a hatalmas piacot követi le a digitális gazdaság. Mára a hagyományos értelemben vett földrajzi piacok beszűkültek és helyettük a kibertér globális piaca irányítja a nemzetközi kereskedelem jelentős részét. A hagyományos gazdasági modellek egy része összeomlott, és a digitális gazdaság meghatározó trendjei és értékesítési metódusai vették át a piac meghatározó része felett az uralmat. A gazdasági szereplők potenciálisan függenek a kommunikációtól, és a hálózati gazdaság fejlődési irányaitól függetlenül attól, hogy ezt tudomásul veszik, vagy megkésve már az összeomlás határán tudatosul bennük.

Új fogalmak és gazdasági metódusok jöttek létre. Előtérbe kerültek a közösségi média alkalmazások, amelyek determinálják a piaci szereplők és a vásárlók reakcióit. Egy-egy alkalmazás vagy honlap magas látogatottsága jelentős piaci értékkel bír. Egy jól sikerült internetes alkalmazással gyakorlatilag egy két év alatt a világ élvonalába lehet kerülni gazdaságilag. Új digitális fizetési rendszerek jöttek létre és gyakorlatilag 24 órán keresztül biztosított a javak kereskedelme, és a kapcsolódó digitális fizetési mechanizmus. Az emberek többsége naponta meglátogatja az internetet, de vannak, akiknek elektronikus kapcsolattartása folyamatos. Az emberek a kapcsolattartást általában egy keresővel, vagy közösségi média alkalmazással kezdik. Mára a hírportálok is a háttérbe szorultak, a híreket is a közösségi portálok határozzák meg. Az

emberek tudásukat nem saját elméjükben keresik többségében, hanem az internetet, mint egy tranzaktív memóriaként kezelik. Nem a tudást tároljuk, hanem a hozzáférés leggyorsabb lehetőségét. Azt is meg kell említeni, hogy a nyelveket beszélők számára egy hatalmas tudástár nyílt meg és kerül megosztásra.

Kommunikációs eszközök, számítógépek, laptopok, tabletek, ebook readerek, okostelefonok gyorsan elavuló és permanensen fejlődő generációi biztosítják a folyamatos kapcsolattartást és kommunikációt. Mára az internet technológia, alkalmazások és kapcsolódó szoftverek ismerete természetes elvárás, mind a bankok, mind az állami szervezetek, de még a munkakeresés területén is.

Azonban ez a mindennapi folyamatos kapcsolattartás során sokan nem veszik tudomásul, hogy szokásaik a vásárlás, az közösségi média, és a böngészés területén digitális nyomokat hagy. Ezek a digitális szokások megfigyelhetők, értékelhetők és vagyoni előnnyé válthatók. A célzott reklámok, kereskedelmi akciók, vagy éppen a szokások és kapcsolatrendszerek feltérképezése sok esetben jelentős előnyhöz juttatja az internetezőt. Ugyanakkor nem veszi tudomásul, hogy egy pusztán saját kereskedelmi és terjeszkedési céljait szolgáló digitális hálózat üzleti célpontjává vált. Ez jelenthet kedvező lehetőséget, de jelentheti, hogy szokásait, kapcsolatrendszerének digitális adatait értékesítik, és azt, hogy magánszférájába durván behatolva esetenként kiber bűnözők célpontjává válik.

A gazdasági társaságok ugyanebben a kibertérben kell, hogy gazdálkodjanak, értékesítsenek és fejlődjenek. Drasztikusam át kellett alakítani gazdálkodási modelljüket, vezetési stratégiájukat, a piacra jutási és kommunikációs módszereiket. Sok esetben nem, vagy nem eleget költenek a digitalizációval foglalkozó szakemberek és a piaci jelenléthez szükséges szoftverek költségeire, költségtakarékosság címen. A gazdasági társaságoknak meg kell találni az egyensúlyt a számukra még megengedhető optimalizált költségek és az digitális gazdaságban való elektronikus jelenlét között. Ki kell alakítani saját belső és külső digitális kapcsolati hálóikat, védett digitális rendszereiket, és ezeket folyamatosan üzemeltetni és fejleszteni kell. Időben fel kell ismerni a digitális piaci trendeket és ki kell dolgozni ezekhez való optimális alkalmazkodási stratégiát. Fel kell ismerni, hogy a vásárlást legtöbb esetben ma

már a digitális piactereken kezdik, és mára ezt a digitalizált piaci szegmest, és vevőkört kell megszólítni és megtartani. Létre kell hozni és fenntartani a digitális vásárlás élményét. Fel kell ismerni, hogy új iparágak, új fizetési és kereskedelmi rendszerek jöttek létre, amelyek gazdasági működése jelentősen eltér a hagyományos gazdasági modellektől. A Sharing Economy megjelenése alapjaiban forgatja fel a hagyományos ország vagy régió szinten szabályozott hagyományos piacokat. Gyors digitális és költségkímélő megoldásaival komplett piacokat lehetetlenít el, vagy komplett szolgáltatási szektorokat tesz tönkre vagy alakít át. A piacon maradni akaróknak meg kellett ismerni az adatbányászat, a szövegbányászat, az e-kereskedelem, az e-bank, a paypass, a paypall, és a célzott e-marketing fogalomrendszerével, alkalmazásaival és lehetőségeivel. Ehhez kell, hogy igazítsák stratégiájukat, szolgáltatási portfóliójukat, vevőelérési metodikájukat, és az informatikai rendszereiket.

Ha ez nem sikerül permanensen alkalmazkodni és piacot nyerni és megtartani a kibertérben, nem kell egy évtized, hogy a gazdálkodás feltételrendszerének megváltozása miatt a kibertérrel rohamosan fejlődő konkurencia átvegye a piacot és a vevőkört, gyakorlatilag a tönkretéve a lemaradt gazdasági társaságok piaci lehetőségeit.

A digitális városok módszereinek rohamos terjedésével állami szerveknek, helyi szolgáltató cégeknek csatlakozni kell a régiós információs rendszerekhez és alkalmazni kell az ott alkalmazott digitális metódusokat. De az állampolgároknak is fel kell nőni a digitális kihívásokhoz, hiszen sok esetben már csak elektronikusan képesek intézni ügyeiket az informatikai megoldásoknak köszönhetően, vagy jelentős hátrányba kerülnek, ha képtelenek azokat a napi gyakorlatban alkalmazni.

Tudomásul kell vennünk, hogy a kibertér velünk vagy nélkülünk fejlődik, és vagy fel tudunk zárkózni és kihasználni előnyeit, vagy rövid időn belül drasztikusan le fogunk maradni.

Irodalomjegyzék

BARABÁSI Albert – László: Villanások – a jövő kiszámítható (Nyitott Könyvműhely, 2010., ISBN 9789633100141)

Elektronikus tartalmak

24.hu: Tériszonyos videóval kampányol a Facebookon a Samsung; Letöltve: http://24.hu/media/2015/11/25/teriszony-felhokarcolo-facebook-samsung-360-fok/ (utolsó letöltés 25/11/2015)

Adadttudomany.blog.hu: Néhány szó a predektív analízisről. Letöltve:http://adattudomany.blog.hu/2014/06/02/nehany_szo_a_prediktiv_analizisrol (utolsó letöltés 22/02/2016)

Adam Raff and Shivaun Raff: How Google's Universal Search Mechanism Threatens Competition and Innovation on the Internet; Letöltve:http://www.foundem.co.uk/Foundem_Preferencing_Data_and_Arguments.pdf (utolsó letöltés 09/09/2015)

Amazon.com: Kindle; Letöltve:https://kindle.amazon.com/ (utolsó letöltés 17/11/2015)

App Brain: Number of Android applications; Letöltve:http://www.appbrain.com/stats/number-of-android-apps (utolsó letöltés 09/03/2016)

Árki Noémi: Hét dolog, amit a Facebook megváltoztatott, Letöltve: http://media20.blog.hu/2015/09/07/7_dolog_amit_a_facebook_megvaltoztatott (utolsó letöltés 07/12/2015)

Balla Zsolt: Így áll feje tetejére az egész kereskedelem 2014.09.15; Letöltve: http://www.uzletresz.hu/eladas/20140915-igy-all-feje-tetejere-az-egesz-kereskedelem.html (utolsó letöltés 15/11/2015)

Bantrr.com: Four Types of Crowdsourcing; Letöltve: https://bantrr.com/2010/05/08/four-types-of-crowdsourcing/ (utolsó letöltés 10/05/2010)

Benedek Gábor-Lublóy Ágnes-Szenes Márk: A hálózatelmélet banki alkalmazása 2007; Letöltve: http://epa.oszk.hu/00000/00017/00139/pdf/04vebenedekjav.pdf (utolsó letöltés 07/12/2015)

BIPA Illinois Compiled Statutes: CIVIL LIABILITIES(740 ILCS 14/) Biometric Information PrivacyAct.; Letöltve: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 (utolsó letöltés 23/05/2016)

Bmtoolbox.nex: Sharing Economy; Letöltve: http://bmtoolbox.net/model-patterns/sharing_economy/ (utolsó letöltés 23/05/2016)

Cast-pharma: virtual reality; Letöltve: http://www.cast-pharma.com/virtual-reality-pharma-biotech (utolsó letöltés 23/05/2016)

Cégvezetés: Elektronikus kereskedelem; Letöltve: http://cegvezetes.hu/2002/09/elektronikus-kereskedelem/ (utolsó letöltés 15/06/2016)

Cégvezetés: Hálózati gazdaság; Letöltve: http://cegvezetes.hu/2000/05/halozati-gazdasag/ (utolsó letöltés 22/12/2015)

Cristina Mercer: Digital and the CDO; Letöltve: http://www.cio.co.uk/insight/cio-career/chief-digital-officer-salary-job-description-cdo-role-3627790/?otc=103 (utolsó letöltés 23/12/2015)

Cunami közeleg: dolgozóik felét rúghatják ki a bankok; Letöltve: http://www.portfolio.hu/finanszirozas/bankok/cunami_kozeleg_dolgozoik_felet_rughatjak_ki_a_bankok.223057.html?utm_source=hirstart&utm_medium=portfolio_linkek&utm_campaign=hiraggregator (utolsó letöltés 19/12/2015)

Cybersceince3d: Bringing Learning to Life in VR for Education, Government, and Business letöltve: http://cyberscience3d.com/# (utolsó letöltés 01/04/2016)

Daniel M. Wegner: The Internet Has Become the External Hard Drive for Our Memories ; Letöltve: http://www.scientificamerican.com/article/the-internet-has-become-the-external-hard-drive-for-our-memories/ (utolsó letöltés 01/10/2014)

Deutsche Telekom: Cyber Security Report 2013; Letöltve: http://www.cybersecuritysummit.de/downloads/131106_Cyber_Sicherheitsreport_2013_final.pdf (utolsó letöltés 01/10/2015)

Dof-project.eu: Smartcities;

Letöltve:(http://www.dof-project.eu/index.php/mod.pags/mem.detalle/id.10/relcategoria.1077#.V3l_UZNGSJk (utolsó letöltés 01/05/2016)

Douglas MacMillan and Telis Demos:Uber Valued at More Than $50 Billion; Letöltve:http://www.wsj.com/articles/uber-valued-at-more-than-50-billion-1438367457 (utolsó letöltés 22/05/2016)

Dr. Bodon Ferenc:Adatbányszati algoritmusok 2010; Letöltve:

http://www.cs.bme.hu/~bodon/magyar/adatbanyaszat/tanulmany/adatbanyaszat.pdf (utolsó letöltés 07/12/2015)

Dr.Kovács László: Szövegbányászat és dokumentum kezelés; Letöltve: http://www.iit.uni-miskolc.hu/iitweb/export/sites/default/department/labs/iit-szolgaltatasok/www-db/Tantargyak/TextMining/ora_01.pdf (utolsó letöltés 07/12/2015)

Energiapedia.hu: Barabási Albert László; letöltve: http://energiapedia.hu/barabasi-albert-laszlo (utolsó letöltés 22/02/2016)

Encriyted-tbn: Bitconin; Letöltve: https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcREWXcOh-3DZya6jtKUzlCuMl3fy823U4R6zxLj6IL4Jc9wGuFjDg (utolsó letöltés 01/12/2015)

Humanszoft.hu:Felhőszolgáltatások; letöltve:http://www.humansoft.hu/Alkalmazas_szolgaltatas/Felho_megoldasok.html laszlo (utolsó letöltés 31/05/2016)

Francisco Gutiérrez: Biometrics and Data Mining Letöltve: http://cs.mty.itesm.mx/profesores/lsalgado/Publicaciones/lsalgado_bonsai.pdf (utolsó letöltés 22/02/2016)

Getfove.com:The World's First Eye Tracking virtual reality headset; Letöltve: http://www.getfove.com/ (utolsó letöltés 01/04/2016)

Guangzhou Zhuoyuan Group: Zhuoyuan F1 Racing Car Simulator 9D; Letöltve: http://www.xd-cinema.com/work/zhuoyuan-f1-racing-car-simulator/ (utolsó letöltés 01/04/2016)

Hegyeshalmi Richárd: Letarolja a világot a kínai Ebay; Letöltve http://index.hu/tech/2014/05/19/letarolja_a_vilagot_a_kinai_ebay/ (utolsó letöltés 07/12/2014)

Henk Broeders és Somesh Khanna McKinsey: Strategic choices for banks in the digital age; Letöltve:http://www.mckinsey.com/insights/financial_services/strategic_choices_for_banks_in_the_digital_age (utolsó letöltés 19/12/2015)

Hirado.hu. Olyan pofont kapott a Facebook, amilyet még soha; Letöltve: http://www.hirado.hu/2015/10/08/olyan-pofont-kapott-a-facebook-amilyet-meg-soha/ (utolsó letöltés 08/10/2015)

Hirado.hu: Olyan pofont kapott a Facebook, amilyet még soha 2015. 10. 08. letöltve: http://www.hirado.hu/2015/10/08/olyan-pofont-kapott-a-facebook-amilyet-meg-soha/ (utolsó letöltés 09/10/2015)

Hlács Ferenc: Pénzért elárulná céges jelszavát az alkalmazottak ötöde;

Letöltve: http://www.hwsw.hu/hirek/55357/vallalati-biztonsag-jelszo-alkalmazott.html (utolsó letöltés 24/03/2016)

Horváth & Partners: Digitalizáció és CIO;

Letöltve: http://www.controllingportal.hu/Tematikus_konyvtar/IT/Digitalizacio_es_CIO (utolsó letöltés 27/02/2016)

Htcvive.com: Vive; Letöltve: http://www.htcvive.com/eu/ (utolsó letöltés 01/04/2016)

Hvg.hu: Minden kiderült a Microsoft fantasztikus szemüvegéről 2016. március 01; Letöltve: http://hvg.hu/tudomany/20160301_microsoft_hololens_holografikus_szemuveg_ara_megjelenes (utolsó letöltés 01/03/2016)

Iinclusion.skoch: Digital Bank; Letöltve:http://inclusion.skoch.in/story/340/21st-century-digital-bank-640.html megjelenes (utolsó letöltés 01/03/2016)

Jaideep Srivastava: Web Mining; Letöltve: http://www.ieee.org.ar/downloads/srivastava-tut-pres.pdf (utolsó letöltés 07/12/2015)

Jekler Rudolf: A gazdaságformáló háló 2009– Vitacikk Letöltve: http://www.piacesprofit.hu/egyeb-cikkek/a-gazdasagformalo-halo-%C2%96-vitacikk/ (utolsó letöltés 28/01/2016)

Jesko Józse: Online mozgalmak határai; Letöltve: http://polblog.reblog.hu/cimke/h%C3%A1l%C3%B3zat (utolsó letöltés 01/03/2016)

Kellys: How to make Social Media work; Letöltve: http://www.kellyservices.de/uploadedFiles/Hungary_-_Kelly_Services/New_Smart_Content/How%20to%20make%20Social%20Media%20work_White%20paper3.pdf (utolsó letöltés 28/07/2014)

Központi Statisztikai Hivatal: Bruttó Hazai Termék (GDP) 2014; Letöltve: https://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_qpt015.htm (utolsó letöltés 15/01/2016)

Learnincloudcomputing: Cloud-computing, Letöltve: http://learningcloud-computing.com/better-information-about-the-cloud-computing/ (utolsó letöltés 15/01/2016)

Lauren Hockenson: Facebook brings 360 streaming video to Samsung Gear VR and invests in 'Social VR' Letöltve: http://thenextweb.com/facebook/2016/02/21/facebook-brings-360-streaming-video-to-samsung-gear-vr-and-invests-in-social-vr/#gref (utolsó letöltés 22/02/2016)

Mark Zuckenberg: Facebook in 2030; Letöltve: http://www.usatoday.com/story/tech/news/2016/02/04/facebook-2030-5-billion-users-says-zuck/79786688/ (utolsó letöltés 10/05/2016)

Market Pulse Survey 2016:Weak Security Practices Leave Organizations Exposed; Letöltve:http://img03.en25.com/Web/SailPointTechnologies/%

7B9a1ba317-f96c-46c5-9c14-0d4c00422135%7D_sailpoint-market-pulse-2016.pdf utolsó letöltés 27/03/2016)

Mastercard: Hogyan fizethetsz egyetlen érintéssel; Letöltve: http://www.mastercard.com/hu/consumer/mastercard-paypass.html (utolsó letöltés 23/11/2015)

Mészáros Rezsó: A kibertér és a globalizáció; Letöltve: http://www.pointernet.pds.hu/ujsagok/evilag/2004-ev/04/20070306122418315000000489.html (utolsó letöltés 28/06/2014)

Microsoft CityNext: Városfejlesztés Letölve:http://hirlevel.egov.hu/2013/07/18/microsoft-citynext-varosfejlesztes-xxi-szazadi-modszerekkel/ (utolsó letöltés 31/05/2016)

Mobilarena: Mobilfizetés blog: Hogy működik a PayPal? Letöltve:http://mobilarena.hu/hir/mobilfizetes_blog_hogy_mukodik_a_paypal.html (utolsó letöltés 11/12/2015)

Pat Bakey: SAP in Retail 2014; Letöltve: https://jenractechnologies.wordpress.com/tag/pat-bakey/ (utolsó letöltés 13/05/2016)

Noesissolutions.com: Data mining, Letöltve:www.noesissolutions.com/Noesis/design-optimization/data-mining/post-processing (utolsó letöltés 31/05/2016)

Paul Carsten: Alibaba's Singles' Day sales surge 60 percent to $14.3 billion; Letöltve: http://www.reuters.com/article/us-alibaba-singles-day-idUSKCN0SZ34J20151112 (utolsó letöltés 12/11/2015)

Pcworld.hu: 10 perc alatt 12 millió dollárt hozott az HTC VR-headsete; Letöltve: http://pcworld.hu/vr/10-perc-alatt-12-millio-dollart-hozott-az-htc-vr-headsete.html (utolsó letöltés 02/03/2016)

PWC: Osztogatnak vagyfosztogatnak? A sharing economy térnyerése; Letöltve: https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/sharing_economy.pdf (utolsó letöltés 21/05/2016)

Phishingsitedotnet:cyberspace; Letöltve: https://phishingsitedotnet.files.wordpress.com/2016/01/cropped-cyberspace-image.jpg (utolsó letöltés 21/05/2016)

PWC: The Sharing Economy; Letöltve: http://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/assets/pwc-cis-sharing-economy.pdf (utolsó letöltés 20/05/2016)

Ranjit Gill: Boots to roll out real-time stock visibility in coming weeks – 2014; Letöltve: http://www.computerweekly.com/news/2240230442/Boots-to-roll-out-real-time-stock-visibility-in-coming-weeks (utolsó letöltés 10/05/2016)

Reuters: Amazon.com; Letöltve: http://www.reuters.com/finance/stocks/analyst?symbol=AMZN.O (utolsó letöltés 17/11/2015)

Samsung.com: gear vr light is available now; Letöltve: http://www.samsung.com/hu/news/local/gear-vr-light-is-available-now (utolsó letöltés 11/12/2015)

Samsung.com: Launching People #BeFearless; Letöltve: http://www.samsung.com/ae/launchingpeople/ (utolsó letöltés 15/12/2015)

Samsung.com:gear-vr; letöltve: http://www.samsung.com/global/galaxy/wearables/gear-vr/ (utolsó letöltés 01/04/2016)

Sarnyai Gábor: Az Ubert egyre több országban tiltják be; Letöltve:http://mno.hu/gazdasag/az-ubert-egyre-tobb-orszagban-tiltjak-be-1279296 (utolsó letöltés 22/05/2016)

Sas:Hadoop; Letöltve: http://www.sas.com/en_us/insights/big-data/hadoop.html (utolsó letöltés 22/02/2016)

SG.hu Több tízmilliárd euró kárt okoz az ipari kémkedés; Letöltve: https://sg.hu/cikkek/101244/tobb-tizmilliard-euro-kart-okoz-az-ipari-kemkedes (utolsó letöltés 01/10/2015)

Sg.hu: Több tízmilliárd euró kárt okoz az ipari kémkedés 2014; Letöltve: https://sg.hu/cikkek/101244/tobb-tizmilliard-euro-kart-okoz-az-ipari-kemkedes (utolsó letöltés 07/12/2015)

Sruthi Shankar: Facebook loses first round in suit over storing biometric data; http://www.reuters.com/article/us-facebook-lawsuit-idUSKCN0XX08U (utolsó letöltés 07/05/2016)

Swarup Gupta: Why Did Black Friday Sales Fall by $1 Billion?; Letöltve:
http://www.zacks.com/stock/news/199560/why-did-black-friday-sales-fall-by-1-billion (utolsó letöltés 29/12/2015)

Szalay Dániel: Tériszonyos videóval kampányol a Facebookon a Samsung Letöltve: http://24.hu/media/2015/11/25/teriszony-felhokarcolo-facebook-samsung-360-fok/ (utolsó letöltés 25/11/2015)

Szövetség az elektronikus kereskedelemért Közhasznú Egyesület Elektronikus Kereskedelmi Évértékelő 2015; Letöltve: http://www.szek.org/hirek/elektronikus-kereskedelmi-evertekelo-2015/1302 (utolsó letöltés 31/12/2015)

The Statistics Portal:eBay's annual net revenue from 2004 to 2014 Letöltve: http://www.statista.com/statistics/266195/ebays-annual-net-revenue/ (utolsó letöltés 19/12/2015)

Theverge.com Why Apple's deal with China's biggest ride-sharing company is making Uber feel unloved; Letöltve: http://www.theverge.com/2016/5/13/11671042/apple-didi-china-uber-travis-kalanick-self-driving-car (utolsó letöltés 13/05/2016)

Tóth Péter: Alternatív fizetési módok; Letöltve: https://prezi.com/lgtfsavnrevz/alternativ-fizetesi-modok/ (utolsó letöltés 01/07/2015)

T-system: A jövő élhetőbb városaiért; Letöltve:http://www.t-systems.hu/innovacio/digitalis-varos/digitalis-varos/digitalis-varos-intelligens-megoldasokkal (utolsó letöltés 31/05/2016)

Tunde Olanrewaju McKinsey: The rise of the digital bank Financial Times on October 25, 2013 (ft.com); Letöltve: http://www.mckinsey.com/business-functions/business-technology/our-insights/the-rise-of-the-digital-bank (utolsó letöltés 22/11/2015)

Vrscout.com: Projects Overcoming Your Fear of Heights with Samsung Gear VR; Letöltve: http://vrscout.com/projects/fear-of-heights-samsung-gear-vr/ (utolsó letöltés 23/02/2016)

Wareable.com: Project Morpheus Feature; Letöltve: http://www.wareable.com/project-morpheus/sony-project-morpheus-release-date-price-games (utolsó letöltés 22/02/2016)

Wikipedia.hu: Adatbányászat; Letöltve: https://hu.wikipedia.org/wiki/Adatbányászat (utolsó letöltés 10/11/2015)

Wikipedia.hu: Ebay; Letöltve: https://hu.wikipedia.org/wiki/EBay html (utolsó letöltés 17/11/2015)

Wikipedia.hu: Google_Play; Letöltve: https:// hu.wikipedia.org/wiki/ Google_Play (utolsó letöltés 17/11/2015)

Wikipedia.hu: Hat lépés távolság; Letöltve: https://hu.wikipedia.org/wiki/Hat_lépés_távolság (utolsó letöltés 22/02/2016)

Wikipedia.org: Alibaba_Group; Letöltve: https://en.wikipedia.org/wiki/Alibaba_Group (utolsó letöltés 17/11/2015)
Wikipedia.org: Amazon.com; Letöltve: https://en.wikipedia.org/wiki/Amazon.com (utolsó letöltés 17/11/2015)
Wikipedia.org: Big data; Letöltve: https://en.wikipedia.org/wiki/Big_data (utolsó letöltés 12/05/2016)
Wikipedia.org: Business-to-business; Letöltve: https://en.wikipedia.org/wiki/Business-to-business (utolsó letöltés 15/06/2016)
Wikipedia.org: Cloud_computing; Letöltve: https://en.wikipedia.org/wiki/Cloud_computing (utolsó letöltés 10/05/2016)
Wikipedia.org: Crowdfunding; Letöltve: https://en.wikipedia.org/wiki/Crowdfunding (utolsó letöltés 12/05/2016)
Wikipedia.org: Smart_city; Letöltve: https://en.wikipedia.org/wiki/ Smart_city (utolsó letöltés 31/05/2016)
Wikipedia.org: Google_Play; Letöltve: https://en.wikipedia.org/wiki/Google_Play (utolsó letöltés 17/11/2015)
Wikipedia.org: Online_chat; Letöltve: https://en.wikipedia.org/wiki/Online_chat (utolsó letöltés 15/01/2016)
Wikipedia.org: R (programing language); Letöltve:https://en.wikipedia.org/wiki/R_%28programming_language%29 (utolsó letöltés 13/05/2016)
Wikipedia.org: Sharing Economy; Letöltve: https://en.wikipedia.org/wiki/Sharing_economy (utolsó letöltés 22/05/2016)
Wikipedia.org: Six_degrees_of_separation; Letöltve: https://en.wikipedia.org/wiki/Six_degrees_of_separation (utolsó letöltés 22/02/2016)
Wikipedia.org: Skype; Letöltve: https://en.wikipedia.org/wiki/Skype (utolsó letöltés 15/01/2016)
Wikipedia.org: Virtual_reality; Letöltve: https://en.wikipedia.org/wiki/Virtual_reality (utolsó letöltés 15/01/2016)
Wikipedia:Bitcoin; Letöltve: https://en.wikipedia.org/wiki/Bitcoin (utolsó letöltés 18/02/2016)
Wikipedia:Digital Wallet;
Letöltve:https://en.wikipedia.org/wiki/Digital_wallet (utolsó letöltés 02/12/2015)

Wtop: Study: Most Americans suffer from 'Digital Amnesia' Letöltve:http://wtop.com/health/2015/07/study-most-americans-suffer-from-digital-amnesia/ (utolsó letöltés 01/08/2015)

Youtube: Launching People | #BeFearless of Public Speaking; Letöltve: https://www.youtube.com/watch?v=bb8nORrS83k (utolsó letöltés 01/04/2016)

Youtube: Launching People | Be Fearless | Conquering Fear of Heights; Letöltve: https://www.youtube.com/watch?v=KOShftB2sXM (utolsó letöltés 23/02/2016)

Kilin Józsefné
(statresearch@cgeopol.hu)

A kibertér emberi erőforrásai

Absztrakt

A napjainkban zajló negyedik ipari forradalom, az Ipar 4.0 idején az informatika tudománya, a technológiák és az alkalmazások fejlesztése rohamléptekben halad, ami jelentős társadalmi és technológiai hatásokkal jár. A legtöbb társadalmat felkészületlenül érte ez a gyors ütemű fejlődés, az informatika-adta lehetőségek kiaknázásához jelentős mértékben kell fejleszteni tudásukat, kreativitásukat. A vállalati fejlődés számára elérkezett a Big Data (Nagy Adat) adatelemzési technológia, míg az IoT (Internet of Things) útján okosvárosok, okosautók, tanulni képes, intelligens robotok születnek. Az új eredmények átformálják a vállalkozások munkaerő-igényét éppúgy, mint a munkakörök tartalmát, új szakmák is születnek, mások eltűnnek. A változások a világon mindenütt szükségessé teszik az oktatási rendszerek, továbbá az oktatás tartalmának újragondolását.

Kulcsszavak: digitális tudás, ipar 4.0, informatika, munkaerő, oktatási rendszerek

Abstract

During Industry 4.0 – the fourth industrial revolution happening in our world today – information science, technologies and applications are developing at an enormous speed which has significant effects on both societies and technology. Many countries were unprepared for this fast development and must enhance their knowledge and creativity in order to effectively utilize new opportunities created by information technology. Companies have to face the challenge of analyzing Big Data, while through the Internet of Things intelligent cities, smart cars, and learning robots are emerging. As a result, companies' labor-force needs and job profiles are changing; new professions are born, others disappear. All these changes urge us to re-think the structure and content of education worldwide.

Keywords: digital knowledge, Industry 4.0, information technology, labour-force, educational systems

Bevezető

A kibertér virtuális világában a világhálóra feltöltött információk száma naponta exponenciálisan bővül. Az internetes publikálás költsége elenyésző, ezért számos olyan szolgáltatást lehetővé tesz, ami nem üzleti alapon működik, aminek nagyon szűk a célcsoportja, vagy olyanokat is, aminek egyszerűen csak a közhírré tétel a célja. (Wikipedia, 2011)

Ebben a virtuális térben tárolt információk típusa azonban nem egynemű. Adatbázisokban tárolt strukturált adatok, írott szövegek, táblázatok, grafikonok, álló- és mozgógépek egyaránt megtalálhatók a világhálón. Az interneten szenzitív és titkosított adatokat is tárolnak, a tanulmány azonban kizárólag a nyilvánosan hozzáférhető információkkal kapcsolatos témakörökre terjed ki, és kitér a közeljövőre prognosztizált munkaerőigényre, továbbá a különböző képzési formákra.

1. Az internet: a tudomány és a mindennapok támogatója

„A tudomány most válik nagykorúvá, manufaktúrából az ipari forradalom korába lép" (Szalay, 2016), ami a kibertér rohamos fejlődésének is köszönhető. Ennek a megállapításnak az alátámasztására saját példáját vázolta fel a Johns Hopkins Egyetem magyar származású professzora, aki szerint ma az adatok tárolása és feldolgozása a legfontosabb kérdés. Szalay professzor barátjával, a legendás számítógéptudóssal, Jim Grayjel együtt egy csillagászati adatbázist épített, ami társadalmasította és iparivá tette a csillagászatot. A projekt lényege, hogy 2000 óta egyetlen gigantikus adatbázisba rendezik azokat a csillagászati adatokat, amelyeket a projektjük saját távcsöve rögzít. Ez az adatbázis nyilvános, tehát a világon minden tudós vagy civil hozzáfér. Ha egy csillagász szeretne megfigyelni egy jelenséget, akkor először ennek az adatbázisnak a „virtuális távcsövével" tud körülnézni, percek alatt, teljesen ingyen. Ha a csillagászok meg akarnak figyelni egy jelenséget, akkor első körben már nem kell teleszkópidőre várniuk, majd maguknak kielemezniük a nyers adatokat. Így egy több mint egy évig tartó megfigyelési folyamatot tett ötpercessé az adatbázi-

suk. (Szalay, 2016) Sikerükkel bebizonyították, hogy a már a közeljövő tudósainak képzéséhez átrendeződik a tantárgyak népszerűsége, súlya az oktatásban: „Az MIT-n, a Harvardon, a Stanfordon mindig a lineáris algebra, a bevezető fizika voltak a legnagyobb létszámú osztályok, ma már a statisztika és számítógéptudomány. Ennek az új adattudománynak minden tudományba be kell épülnie a következő évtizedben. Az új adattudomány minden természettudomány alapja, és így kell beépülnie az oktatásba is." (Szalay, 2016)

Az internet útján támogatja a tudomány és a tanulás szabadságát a Massachusetts Institute of Technology (MIT), a világ egyik leghíresebb mérnöki és technológiai egyeteme is. Több mint 2400 kurzusának tananyagát töltötte fel a világhálóra. Az egyetem elsősorban mérnöki, fizikai és egyéb technológiai kutatásairól híres, de a feltöltött tananyagok listájára felfért a programozás és a kvantummechanika mellett az antropológia és más humán kurzusok is. (Eduline, 2016)

Európában hasonló, áttörést jelentő rendszeren gondolkodik a 2016 első félévében az EU soros elnökségét betöltő Hollandia is. Elképzelésük szerint 2020-tól ingyenesen elérhetővé tennék az EU összes tudományos kutatási eredményét és publikációját. Egyelőre úgy látszik, hogy sikeresen végigvihetik a döntéshozókon, hogy az EU maga alakítson ki egy olyan online rendszert, amelyben minden olyan publikáció elérhetővé váljon, melynek megírását közpénzből, illetve uniós forrásból finanszírozták. Terveik szerint minden állami egyetemnek – és a többi csatlakozónak – nem csak lehetősége, de kötelessége is lesz a szabad hozzáférhetőség jegyében feltölteni a tudományos munkáikat. A rendszerben nem tárolnák az összes tudományos dokumentumot, de az eredmények mellett az azt megalapozó adatokat is nyilvánossá kellene tenni, mely alól csak komoly szerzői jogi vagy biztonsági esetekben lehetne kivételt tenni. A holland kormány a lépéssel ráadásul egy sikeres nemzeti vállalkozásukat törheti le (a neve Elsevier), ami jól mutatja a közös ügyek elsőbbsége iránti elköteleződést. (Eduline, 2016) Az EU-tagállamok egyben azt is kérik a tudományos világtól, hogy más szempontok alapján ítéljék meg a tudományos munka minőségét. Véleményük szerint a kutatókat nem az alapján kéne rangsorolni, hogy mennyit publikáltak vagy hányan citálják őket, hanem nagyobb hangsúlyt kéne fektetni arra, milyen társadalmi hatása van a munkájuknak. (Horváth, 2016)

2. A felhőalapú szolgáltatások

Az informatika fejlődésének új korszakát teremtette meg az információk felhőben történő tárolásának lehetősége. Az így tárolt adatokhoz – a világhálón keresztül – okoseszközeivel (robot, számítógép, tablet, okostelefon, okosóra stb.) bármikor hozzáférhet az arra jogosultságot szerzett felhasználó, így a megszerzett információkat nem kell minden egyes eszközén tárolnia, hiszen mindig ugyanahhoz az információhalmazhoz fordul kérdésével. Ráadásul biztos lehet abban, hogy eszközeiről a mindenkori legaktuálisabb információkat érheti el, amennyiben az adatgazdák megfelelően karbantartják adatbázisukat. A felhasználónak módjában áll az is, hogy megadott eszközein szinkronizálja a dokumentumait, nincs redundancia, nincs aktualitási probléma, ráadásul ez a technológia ma már a valós idejű (real-time) csoportmunka végzését is lehetővé teszi.

Az OECD országainak többségéről elmondható, hogy a nagyvállalatokban dolgozók 95%-a, a középvállalatok alkalmazottainak 85%-a használja munkája során az internetet nap mint nap, ugyanez az arány a kisvállalatok esetében 65%. A gyors technológia-váltások miatt azonban a mobilitás, a felhőalapú szolgáltatások igénybevétele új készségeket kíván meg, hiszen pl. az Európai Unió digitális adatforgalmának háromnegyede okostelefonok és tabletek segítségével, Wi-Fi hálózatokon keresztül bonyolódik le. (Nemzeti Hírközlési és Informatikai Tanács, 2015)

Napjainkban a vállalatoknak nagyon sok kihívásnak és követelménynek kell megfelelniük annak érdekében, hogy lépést tarthassanak a technológiai fejlődéssel éppúgy, mint a növekvő adatmennyiséggel és ügyfélkörük változó igényeivel. Csak így érhetik el, hogy az üzleti feladataikat minél korszerűbb és gyorsabb megoldásokkal oldhassák meg. Nem hagyhatják figyelmen kívül ugyanakkor az egyre szűkülő költségvetést, az egyre rövidebb megtérülés követelményét, és egyensúlyt kell kialakítaniuk a beruházásokra fordított összegek és a működtetési költségek között is. „Óriási mennyiségű adat termelődik naponta világszerte. Percenként 204 millió e-mailt küldenek el, 3 millió Google keresést végeznek, 6 millió YouTube-videót néznek meg és 590 ezer tweet születik." (NetIQ Novell SUSE Magyarországi Képviselet, 2016) A vállalatoknak, illetve az adatközpontoknak lépést kell tartaniuk ezzel a rohamlép-

tékben növekvő adatáradattal, és ez rengeteg új kihívást eredményez számukra. Az adatközpontok üzemeltetői is számos területen változtatni kényszerülnek: új szintre kell emelni az automatizálást, több eszköz felügyeletét kell ellátniuk kevesebb erőforrással, optimalizálni szükséges a kihasználtságot és a működést is rugalmasabb formában kell biztosítaniuk.

A szakértők a megoldást – a helyi számítóközpontban üzemeltetett adatbázisok helyett – a felhőalapú szolgáltatások alkalmazásában látják. Álláspontjuk szerint ez a technológia nagyobb rugalmasságot és hatékonyságot nyújt, segíti az innovációk fejlesztését, jobb felügyeletet és biztonságot garantál, továbbá magas szintű szolgáltatások és önkiszolgáló funkciók nyújtását teszi lehetővé költséghatékony üzemeltetés mellett, így megfelel az új igényeknek. „Mielőtt azonban egy vállalat megkezdené útját a felhőbe, érdemes pontosan összesítenie az üzleti elvárásokat és kötelezettségeket, illetve a várt eredményeket. Ezután célszerű a szervezeten belüli elvárásokat és a teljesítéshez szükséges erőforrásokat is megvizsgálnia. Következő lépésként az üzleti folyamatok átalakítását kell megterveznie annak érdekében, hogy a legtöbbet tudják kihozni a privát felhőből, illetve döntsenek a telepítendő szolgáltatások köréről. Arra is figyelmet kell fordítani, hogy milyen háttérinfrastruktúra szükséges a szolgáltatások futtatásának támogatásához, illetve milyen önkiszolgáló funkciók támogatják a működést a szervezeten belül. Érdemes referencia-architektúrákat is tanulmányozni, hogy további hasznos ötleteket gyűjthessenek." (NetIQ Novell SUSE Magyarországi Képviselet, 2016) A felhőalapú technológia bevezetésével ugyanakkor jelentősen megváltozik egy vállalat infrastruktúrája. Az asztali PC-k elveszítik önálló számítógép-funkcióikat, terminálként működnek. A felhőben tárolt adatokat ugyanakkor megfelelő mértékben struktúrálni kell, ez a feltétele ugyanis annak, hogy minél könnyebben és gyorsabban lekérdezhetők legyenek. A vállalat informatikusai számára pedig ez újabb kihívásokat, továbbképzési kötelezettséget jelent, hiszen egy-egy üzleti területen működő gazdálkodó szervezet speciális szakmai ismereteit is figyelembe kell venni a fejlesztéseknél.

Az Európai Bizottság felhőalapú szolgáltatásokra és világszínvonalú infrastruktúrákra vonatkozó tervezetet készített, melynek célja, hogy a tudomány, a vállalkozások és a közszolgáltatások is kihasználják a nagy adathalmazokban rejlő lehetőségeket. A legtöbb tudományos adatot kontinensünk, Európa

állítja elő a világon. A széttagolt és nem elégséges infrastruktúra miatt azonban az EU nem tudja teljes mértékben kihasználni a nagy adathalmazokban rejlő lehetőségeket. A Bizottság ezért a jelenlegi kutatási infrastruktúra megerősítése és összekapcsolása révén létre kíván hozni egy új európai nyílt tudományosadat-felhőt, amelynek jóvoltából „az Európai Unióban 1,7 millió kutató és 70 millió, a tudomány és technológia területén dolgozó szakember tárolhatja, oszthatja meg vagy használhatja fel újra egy közös virtuális környezetben a nagy adathalmazok keretében létrejött információkat. A tervek szerint a világszínvonalú infrastruktúra lehetővé fogja tenni Európa számára, hogy gazdasági és tudáspotenciáljához mért eredményeket érhessen el a nagy teljesítményű számítástechnika terén folyó világszintű versenyben." (Computerworld, 2016) A technológia kidolgozása a feltétele annak, hogy az európai kutatási eredményeket és dokumentumokat (ingyenes lekérdezéssel) közzé tehessék.

A digitális gazdaságért és társadalomért felelős európai biztos így fogalmazott: „Az európai számításifelhő-kezdeményezés és ezen belül is a szuperszámítógépes kapacitás, a nagy sebességű összeköttetés, a csúcstechnológiás adat- és szoftverszolgáltatások jóvoltából végre megmutatkozhatnak a nagy adathalmazokban rejlő értékek a tudomány, az ipar és a közszféra számára. E kezdeményezéssel nem titkolt célunk az, hogy az Európai Unió 2020-ra a nagy teljesítményű számítástechnika területén a világ három legmeghatározóbb szereplője között legyen. Emellett a kvantumtechnológiában rejlő lehetőségeket is vizsgáljuk, amelyek azzal kecsegtetnek, hogy a jelenlegi szuperszámítógépek által nem megoldható számítási problémákra is megoldásokat kínálnak."

Az európai számításifelhő-kezdeményezés megkönnyíti a kutatók és innovátorok számára az adatokhoz való hozzáférést és azok további felhasználását, továbbá mérsékli az adattárolás és a nagyteljesítményű elemzések költségeit. Az adathalmazok elemzésén alapuló innováció segíthet lendületbe hozni az európai versenyképességet – többek között az orvostudomány és a közegészségügy területén –, de akár új iparágaknak is lökést adhat. (Computerworld, 2016)

„Az EB számításai szerint a kivitelezéshez 6,7 milliárd euróra lenne szükség, amit különböző EU-s fejlesztési programokból, tagállami forrásokból

és magánbefektetésekből kellene finanszírozni. A Bizottság tervei között szerepel egy olyan útmutató létrehozása is, melynek alapján az oktatási intézmények és a (jövőbeli) munkavállalók talán könnyebben tudnak majd eligazodni a „digitalizálódott" világban." (Voith, 2016)

3. A kibertérben tárolt információk hasznosításának új módszere, a Big Data

A tudományban jött el először a Big Data korszaka, és egyre több tudományágban lesz meghatározó. (Szalay, 2016) Vámos akadémikus (2016) sysbook könyvében így ír: „A rendezetlen, vagy átláthatatlannak tűnő adattömegekből különböző matematikai eszközökkel emeljük ki a számunkra fontos jeleket, jelkapcsolatokat (Big Data). Így kezelik például a kereskedő vállalatok az egyének és csoportok vásárlási szokásait, az egészség szakértői a megbetegedéseket, azok okait, terjedését, a fizikusok a nagy ütköztető berendezések képadataiból az egyes részecskék hatásait. Ezzel foglalkozik az adatbányászat. A dolgok internetesedése, közeli és távoli jelkapcsolata, továbbá a viselhető érzékelők terjedése egyre általánosabbá teszi a mintavételezés technikáját és a felhasználást támogató számítási és techikai módszereket, az így keletkező tömeges adatok feldolgozását."

Az M2M Rendszerház Kft. is kitért a Big Data jelentőségére: „Bár nincs pontos és mindenki által elfogadott definíciója, azt azért ki lehet jelenteni, hogy a Big Data – nevének megfelelően – azt az óriási és laikusként nehezen elképzelhető adatmennyiséget, illetve annak feldolgozását jelenti, amit a hálózatokon lévő gépek és emberek előállítanak." (M2M Zóna, 2014)

A „Nagy Adat" egyre nagyobb mértékben nyer teret a gazdaság szereplői, különösen a gazdálkodó szervezetek tevékenységében, fejlődésében. A világhálón nyilvános adatként tárolt és hozzáférhető óriási adatmennyiség feldolgozása a korábbiaktól eltérő hardveres és szoftveres környezetet igényel. Az egyes témakörökben elismert – és programozási ismeretekkel is rendelkező – szakértők célorientált adatbányászati módszertanokat dolgoztak ki, melyek felhasználásával a gigantikus adatmennyiségből a megrendelő felhasználó számára releváns információkat lehet kinyerni. Ezek alapján már

megfelelő elemzéseket végezhetnek a kutatók vagy a döntéshozók, ugyanakkor korábban nem ismert információkra, megoldásokra is fény derülhet, pl. a fogyasztók szokásainak vizsgálatára, egész piacok felmérésére is lehetőség nyílik. Az adatfeldolgozásnak ugyanakkor nem képezik részét pl. a videók, hiába foglalnak elképzelhetetlenül sok tárterületet. A Big Data nemcsak a mennyiséget, hanem azt a feldolgozási módot is jelenti tehát, ami egyértelművé teszi, hogy csak feldolgozható (strukturált) adatok esetében beszélhetünk erről az alkalmazásról.

A módszertan eredményességét jelzi pl. az Economist magazin, ami szerint „a DataminR nevű New York-i startup cég Twitter-üzenetek adatelemzésével jellemzően öt-tíz perccel az előtt tud értesítéseket küldeni ügyfeleiknek, mielőtt egy esemény (pl. földrengés) bekövetkezik, tehát gyakorlatilag real-time adatelemzésről van szó. Oszama bin Laden likvidálását is 23 perccel korábban tudták előre jelezni, mint bármely más médium. A prognózist a gyilkosságról és Obama rendkívüli sajtótájékoztatójáról szóló tweetek adatelemzésével tették." (DataMiner, 2014) Magyar példaként említhetjük az Országos Meteorológiai Szolgálatot is, ahol – egy adott célból – az előrejelzések elkészítéséhez rövid idő alatt rengeteg adatot kell feldolgozni. Számukra mellékes, hogy szuperszámítógépük van-e, mivel az adatfeldolgozás lényegét a hardveren futó algoritmusok együttese, a szellemiség adja. (Sepp, 2016)

Szalay (2016) szerint a Big Data korszaka rövidesen hatalmas változásokat hoz a mindennapi életben is. Japánban pl. olyan, kifejezetten az időseknek kialakított lakóterületeket terveznek, ahol önműködő kerekesszékeken közlekednek, automaták vásárolnak helyettük, adagolják a gyógyszereiket, de akár meg is fürdetik a nehezen mozgókat. A sofőr nélküli autók megjelenése is drámaian csökkenteni fogja a városok közúti forgalmát. A sofőr nélküli autók technológiája már készen van, bevezetésük csupán a piac függvénye.

4. Az informatika mint a digitális gazdaság alapja

Ma már alig akad olyan munka, amit el lehetne végezni minimális informatikai tudás nélkül, a jövőben pedig szinte minden szektorban egyre nagyobb szerepet kapnak a gépek és a robotok. Általánosan elfogadott tény, hogy

a világ a kognitív[1] üzlet és számítógépek korába lépett. Az utóbbi pár év fejlődésének eredményeként beértek a kognitív számítógépek, amelyek a szöveges és képi, a hang- és videóalapú információkat is fel tudják dolgozni, azokat értelmezik, összefüggéseket tárnak fel bennük, melyekből tanulnak, következtetéseket vonnak le, így értékes betekintéssel, tanácsokkal segítik a vállalatokat és az embereket. (Kis, 2016) Tokióban 2016 januárjában bemutatták a világ első olyan robotját, amely képes az emberek érzelmi reakcióinak és a testbeszéd olvasására. Az elsajátított információkat feltölti egy felhőalapú tárhelyre, ahonnan a többi robot elsajátíthatja azokat.

Sepp (2016) szerint öt lépés vezet egy vállalat kognitívvá válásához. Stratégiaalkotást követően el kell dönteni, hogy milyen adatokat fog gyűjteni a vállalat és azokat hogyan készíti elő, majd kapcsolódnia kell a kognitív felhőhöz, ki kell építenie kognitív infrastruktúráját és gondoskodnia kell annak megfelelő védelméről. A jelen vállalatai tehát már nem térhetnek ki az egyre gyorsuló digitalizáció elől. Eredményeik növeléséhez nem elég a termelékenység és a költséghatékonyság növelése, kognitív vállalattá kell fejlődniük. Meg kell ismerniük innovációs szükségleteiket, ki kell dolgozniuk a szervezeti tanulás módszertanát, és fel kell tárniuk a vállalaton belüli emberi kapcsolatok sajátosságait.

A digitalizáció tartalma és üteme jelentős mértékben befolyásolja egy vállalat szervezeti egységeinek intézményen belüli súlyát, a döntési és végrehajtási hierarchiában elfoglalt helyét is. Míg napjainkban az üzleti és az informatikai szervezeti egységek konvergálása figyelhető meg (az informatika döntéselőkészítő súlya csökken), addig az új technológiák, különösen a felhőben történő adattárolás és a Big Data technológia kidolgozása és alkalmazása, az informatika újbóli erősödését, a hierarchiában magasabb szintre emelését jelentheti. Ezt az igényüket az informatikusok azzal magyarázzák, hogy az adatok elemzése során mindig azonos módszertant alkalmaznak, ezzel objektív képet mutatnak a vállalat döntéshozóinak még a döntés meghozatala előtt, elkerülve ezzel az esetleges jövőbeni üzletági kudarcokat. Az üzletági szakemberek ugyanakkor hajlamosak arra, hogy egy-egy döntés helyességét támasszák alá az általuk tetszőlegesen alkalmazott módszertan alapján készített jelentéseikben, ezzel is munkakörük stabilitását kívánják biztosítani.

1 Jelentése: megismerő, a megismerésre vonatkozó; a gondolkodáson alapuló.

5. A negyedik ipari forradalom (Ipar 4.0)

A PwC (PricewaterhouseCoopers) kutatói a negyedik ipari forradalomról (az Ipar 4.0-ról) és főképp a digitális vállalat megvalósításáról szóló nagyszabású kutatása során kilenc jelentős iparágból több mint kétezer vállalat képviselőit kérdezték meg huszonhat országban. A felmérés célja annak a jelenleg zajló folyamatnak a bemutatása volt, melynek keretében napjaink vezető ipari vállalatai digitalizálják belső vertikális üzemi folyamataikat és a horizontális partnereikkel folytatott együttműködésüket. Ezzel egyidejűleg digitális funkciókkal és innovatív, adatalapú szolgáltatások bevezetésével tökéletesítik termékportfóliójukat. Az Ipar 4.0 megvalósulásához hozzájáruló digitális technológiák között megtalálható a számítási felhő, a kiterjesztett valóság és a viselhető eszközök, a dolgok internete (IoT)-platformok, a helymeghatározó módszerek, a fejlett ember-gép interfészek, a hitelesítés és a csalásfelismerő technológiák, a 3D nyomtatás, az intelligens szenzorok, a nagy adattömegek elemzése, valamint a mobileszközök.

A negyedik ipari forradalomról közzétett PwC-tanulmány szerint a digitális vállalati alkalmazások sikeres bevezetésének előfeltétele a hatékony adatelemzés. A megkérdezett vállalatok fele hozott létre dedikált adatelemzési funkciókat céges vagy üzletiegység-szinten. A PcW kutatása szerint az Ipar 4.0 továbbgyorsítja a globalizációt is, mivel olyan digitális hálózatokat hoz létre, amelyek behálózzák a Földet. Ennek köszönhetően mind a fejlett, mind a fejlődő országok jelentősen profitálhatnak a negyedik ipari forradalomból. A legmesszebbre a német és japán vállalatok jutottak belső folyamataik és a partnereikkel folytatott tevékenységek digitalizálásában. A korszerű technológiákba és az alkalmazottak képzésébe való komoly befektetések eredményeképpen jelentősen nőtt a működési hatékonyság, javult a minőség és csökkentek a költségek. Az amerikai vállalatok is egyre többet kívánnak invesztálni a digitális üzleti modellek kifejlesztésébe, egyre gyorsuló ütemben digitalizálják termékeiket és szolgáltatásaikat. A kínai iparvállalatok kiemelkedően teljesítenek a digitalizáció minden területén, mivel kivételesen rugalmasak és rendkívül nyitottak a digitális átalakulásra. „Kína az egyik olyan ország, amely sokat nyerhet a munkaigényes gyártási folyamatok automatizálásával és digitalizálásával, ugyanakkor megoldást kell találnia a fizetések emelésére." (Mészáros, 2016)

6. A dolgok internete, az IoT

A vállalati innováció és a jelen informatikusai számára egyre nagyobb kihívást jelent a dolgok internete (IoT – Internet of Things). „A McKinsey tanulmánya szerint a dolgok internete rohamos terjedés előtt áll. Elképesztő ütemben nő a hálózatba kapcsolt érzékelők, készülékek és egyéb berendezések száma. Immár több mint egy évtizede barátkozunk a dolgok internete (IoT) fogalmával, mégis eltartott egy ideig, amíg megjelent a mindennapjainkban. Ma világszerte több mint 12 milliárd eszköz kapcsolódik a világhálóra. A következő évtizedben azonban meredeken nő majd ez a szám, a becslések 50 milliárdtól 1 billióig szórnak." (Tóth, 2016)

Szerinte a dolgok internetének korában a behálózott világ számtalan készüléke lesz képes egyidejűleg és észrevétlenül kommunikálni egymással; a létrejövő digitális vállalatok megerősítik a gazdaságot és új üzleti modelleket hoznak létre. Azokban az országokban, ahol előrelátó a kormányzat és megfelelő szabályozási rendszert alakítanak ki, ahol teljesen kiépítik a hálózatokat és erős gazdasági környezet alakul ki, fel fog gyorsulni az IoT terjedése. Akárcsak az ipari forradalom, a dolgok internete is több lépésben valósul meg. Azt mondják, az IoT végül a múlt minden műszaki csodáját, a nyomdagépet, a gőzgépet, a villamosságot is elhomályosítja. Az IoT tehát az internet evolúciója.

Az IoT-megoldások közül a magánszemély felhasználók az intelligens otthoni riasztó, az intelligens parkolórendszer, az okosautó, az okosotthon és az okosmérés alkalmazásokat tartják a leginkább rokonszenvesnek. Az okosriasztó a felhasználó távollétében figyeli az otthonát, rendellenesség esetén sms-értesítést küld. Az intelligens parkolórendszer parkolóhelyet keres az autós számára, míg az okosautó a környező járművek és gyalogosok helyzetét érzékeli, csökkentve ezzel a balesetveszélyt. Az okosmérő segítségével a szolgáltató valós idejű információkat kap pl. a gáz- és melegvíz-felhasználásról, a felhasználó pedig az aktuális költségeiről. Az okosotthonban pedig a háztartási eszközöket és berendezéseket távolról, okostelefonnal is irányíthatjuk. (eNet, 2015)

Az IoT-vel kapcsolatban pesszimista nézetekkel is találkozhatunk, ugyanis a tanulni képes robotok beláthatatlan és előre nem tervezhető, az emberre

veszélyes helyzeteket is okozhatnak. A fejlődés elől azonban nem térhetünk ki, megfelelő előrelátással, szabályozással és a szabályok betartatásával el kell érni a megfelelő fejlesztési, fejlődési eredményeket. A mesterséges intelligencia létrehozása nem minden aspektusból megnyugtató, de „ez még sosem állította meg az emberiséget abban, hogy megcsináljon valamit." (Szalay, 2016)

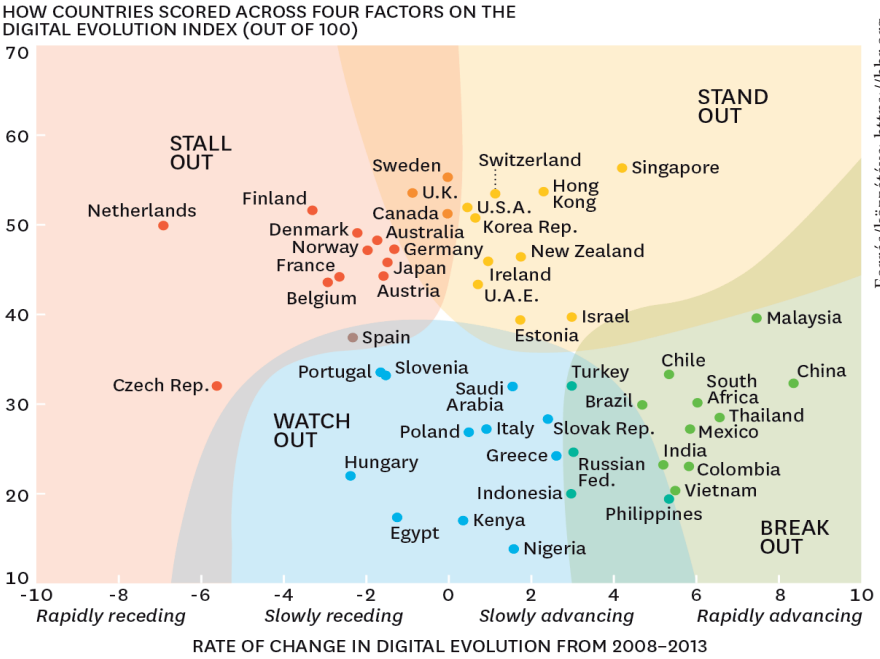
7. A digitális gazdaság fejlődésének várható üteme

Chakravorti, Tunnard és Chaturvedi (2014) Hol fejlődik a digitális gazdaság a leggyorsabban? című tanulmányukban egy új index-számítási módszertant dolgoztak ki és tették közzé. 50 ország 2008 és 2013 közötti digitális gazdasági mutatóit vizsgálták, és kidolgozták az egyes országok digitális fejlődési indexét. Meghatározták, hogy egy 100-as skálán az egyes országok milyen index-pontszámot mutatnak, és bemutatták az országok indexhez viszonyított digitális fejlődésének változását is. Az eredmények alapján az országokat 4 kategóriába sorolták: gyors ütemben lemaradó, lassan lemaradó, lassan fejlődő és gyorsan fejlődő országok.

- Kiemelkedő (Stand Out) országok, melyek a digitális fejlődés magas szintjét mutatták a múltban és egy felfelé irányuló röppályán maradnak.
- Helybenjáró (Stall Out) országok, melyek a fejlődés magas fokát érték el a múltban, de jelenleg veszteségesek, és nem fontos számukra a kockázatvállalás.
- Kitörésre alkalmas (Break Out) országok: potenciális lehetőségük van a digitális gazdaságuk fejlesztésére. Globális pontszámuk még mindig alacsony, de felfelé haladnak, és az egyensúlyra ügyelve később a *Kiemelkedő országok* közé tartozhatnak.
- Bizonytalan fejlődésű (Watch Out) országok: jelentős lehetőségekkel és kihívásokkal néznek szembe, alacsony a pontszámuk úgy az aktuális szintjük, mint a felemelkedési lehetőségeik tekintetében. Okos innovációkkal és átmeneti intézkedésekkel néhányan leküzdhetik a korlátjaikat, míg mások megrekednek.

Digitális kapacitásukat egyenetlen mértékben építő országok

A group of 50 countries reveals four main areas of digital readiness.



Forrás/közzétéve: https://hbr.org

SOURCE DIGITAL EVOLUTION INDEX, THE FLETCHER SCHOOL AT TUFTS UNIVERSITY HBR.ORG

A *Kitörésre alkalmas* (Break Out) országok, mint India, Kína, Brazília, Vietnam és a Fülöp-szigetek, meglehetősen gyorsan továbbfejlesztik digitális gazdaságukat. A növekedés következő szintjét azonban elég nehezen tudják majd elérni.

A *Bizonytalan fejlődésű* (Watch Out) országok, mint Indonézia, Oroszország, Nigéria, Egyiptom és Kenya, jelentős közös vonásokat és alacsony szintű elkötelezettséget mutatnak a reformok iránt, intézményes a bizonytalanság.

A legtöbb nyugat- és kelet-európai ország, továbbá Ausztrália és Japán helybenjárnak (Stall Out). Egyetlen módon tudják visszaszerezni fejlődésük korábbi ütemét, ha egy nagy ugrással elérik, amit a Kiemelkedő országok (Stand Out) a legjobban tesznek: meg kell duplázniuk a (szellemi és technológiai) innovációjukat, és a belső határokon túli piacokat kell keresniük.

8. Az informatikai iparág munkaerőigénye

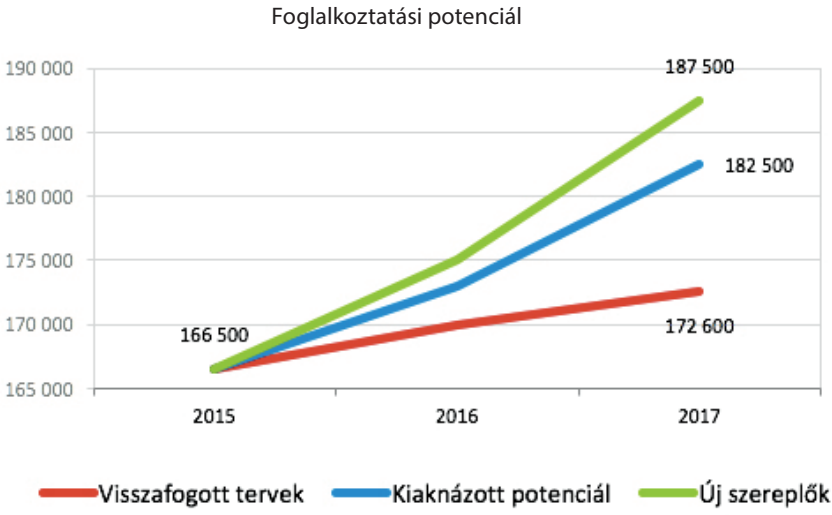
A gazdálkodó szervezeteknél – közöttük a szolgáltatások körében is – már ma is alig akad olyan munka, amit el lehetne végezni informatikai tudás nélkül, a jövőben pedig – a tudományág rohamos fejlődése következtében – szinte minden munkahelyen egyre nagyobb szerepet kapnak a gépek és a robotok. Elengedhetetlen tehát, hogy a munkavállalók – szaktudásuk mellett – megfelelő informatikai ismeretekkel is rendelkezzenek.

Az informatikai iparág szereplői ugyanakkor egyre inkább speciális tudással rendelkező szakembereket keresnek, akiknek a megítélésénél az egyik legfontosabb szempont, hogy képesek-e végrehajtani az általuk igényelt speciális tevékenységeket, megbízható tudással és tapasztalatokkal rendelkeznek-e egy adott szakterületen.

Stubnya (2016) szerint informatikusból azonban itthon és Európában hatalmas hiány van. Különböző becslések szerint 20-22 ezer informatikust tudnának felvenni a hazai cégek, és az IT-iparág fejlődése miatt ez a szám csak nőni fog. A Kormányzati Informatikai Fejlesztési Ügynökség és az NFM megbízásából készített BellResearch-tanulmány következtetései alapján ráadásul ez a helyzet csak egyre rosszabb lesz, hiszen az informatikusok iránti kereslet bőven az átlag felett fog nőni a következő években nemcsak Magyarországon, de a világban is. Ma Európában 600-700 ezer fős hiány van szoftverfejlesztőből, és ez a hiány 2020-ra különböző uniós kutatások alapján 825-900 ezer lesz. A hazai informatikai munkaerőpiacon betölthető 22 000 új állás – az előrejelzések szerint – összesen 72 000 embernek adhat munkát a nemzetgazdaságban. Ennek elsődleges és fő feltétele a szakember-kibocsátás mennyiségi és minőségi növelése, fejlesztése.

Amikor munkaerőhiányról beszélünk az IT-szektorban, akkor nem pusztán arról van szó, hogy kevés a fejlesztő. Mivel az informatikai munkaerőpiac eléggé rétegzett, a különböző szintű képesítéssel rendelkező munkák esetében eltérő, hogy mekkora a hiány. A tanulmány megállapítása szerint jelenleg Magyarországon:

- rengeteg OKJ-s képzettségű fejlesztőre és rendszergazdára lenne szükség, belőlük van a legnagyobb hiány, de a piaci szereplők az OKJ-s képzések minőségét, piaci értékét alacsonyra becsülik,



Forrás/közzétéve: ivsz.hu/projektek, ivsz.hu/wp-content

- felsőfokú szakképzettségű és Bsc-diplomás informatikusból is nagy hiány van,
- mesterdiplomás és PHD-s informatikus kéne a legkevesebb, de ők is mindannyian gyorsan munkát találnának mostanában a magyar munkaerőpiacon.

Magyarországon az ICT (Információs és Kommunikációs Technológia) szektor 122 ezer főt alkalmaz, további több mint 40 ezren dolgoznak az ágazaton kívül informatikai munkakörben. A nemzetközi és hazai informatikai munkaerőpiacon mégis nagymértékű a munkaerőhiány, amely exponenciálisan nő. A hiány gátolja a növekedést, veszélyezteti a versenyképességet.

„A helyzet mégis az, hogy hosszabb távon a képzettebb informatikusokra lehet nagyobb szüksége az országnak. Ha most nem növeljük exponenciálisan a magyar oktatási rendszerből kilépő informatikusok számát, akkor pár éven belül már nem arról fogunk beszélni, hogy hogyan fejlesszük a hazai IT-szolgáltatásokat, hanem arról, hogy hogyan akadályozzuk meg a hazai IT-iparág leépülését. Az egyetlen lehetőség, hogy a jobb minőségű munkaerőből csinálunk versenyelőnyt. Ehhez szakember kell, és nem lesz elég az OKJ-s programozó, hanem a mester- és a doktori képzésre is rá kell erősíteni, miközben az alsóbb szinteken is több emberre lesz szükségünk." (Horváth, 2016)

Az IT-szektor rohamos fejlődése miatt a vállalatok maguk sem tudják, milyen szakemberre lesz szükségük egy hét vagy egy hónap múlva, azt pedig, hogy néhány év múlva kikre, végképp nem. Mindenesetre az elmúlt évek tapasztalatai alapján az egyértelműnek tűnik, hogy a munkáltatóknál az egyes szakterületekre specializált tudás iránti igényt fokozatosan felváltja az alapkompetenciákra építő toborzás. (Fremda, 2016)

Jelenleg közel 24 milliónyian keresnek állást az 500 millió lakossággal rendelkező Európai Unióban, ennek ellenére a vállalkozásoknak komoly nehézségekbe ütközik szakképzett informatikusok felvétele. A legnagyobb az informatikushiány Németországban, de Unió szerte – különösen pedig Olaszországban és az Egyesült Királyságban – egyre komolyabb lesz a helyzet, ha nem végez az igényeknek megfelelő számú szakember. (Mészáros, 2015)

A helyzetet súlyosbítja, hogy az európai munkaerő mintegy harmada – sajnálatos módon – hiányos informatikai ismeretekkel rendelkezik, vagy teljesen híján van ezeknek, és 15%-uk még sohasem használta az internetet.

A munkaerő kiválasztásakor a vállalatok azért sem építhetnek a speciális tudás kikötésére, mert a tudomány nagyon gyorsan változik, ezért egyre többféle, egyre szerteágazóbb tudásra lenne szüksége egy modern munkavállalónak. A természettudományok korábban egyre speciálisabb területekre szakosodtak, de ma már újra valamiféle konvergencia figyelhető meg közöttük. Az informatikai feladatok elvégzésére is korábban matematikusokat, majd alkalmazott matematikusokat, fizikusokat kerestek és alkalmaztak a munkáltatók. Ma már az egyetemeken is gazdaságinformatikus, műszaki informatikus és programtervező informatikus szakokon képzik a jövő információtechnológiai (IT) szakembereit. Az informatikai ismeretek mellett tehát komoly pénzügyi-gazdasági, műszaki, statisztikai ismeretekkel is fel kell vértezniük magukat a hallgatóknak.

A CIO Insight magazin (CIO Insight/HWSW, 2006) szerint „már 2007-ben az egyik legfontosabb trendként jelentkezik az informatika és az üzleti élet közötti határvonalak elmosódása", vagyis az informatikus és nem informatikus szakemberek ismereteinek, tevékenységének a keveredését figyelték meg. Ez igaz volt mind a vezetők, döntéshozók, mind a beosztottak szintjén. Az amerikai magazin által akkor megkérdezett fiatal, 40 év alatti IT-vezetők több mint harmada vallotta például hogy kiegyenlített módon rendelkezik már

informatikai és üzleti ismerettel, háttérrel egyaránt. Az üzleti ismeretek iránti elvárás annál jellemzőbb, minél nagyobb vállalatról volt szó. Előléptetéskor ez a szempont még ennél is sokkal fontosabbá vált. (Bizó, 2016)

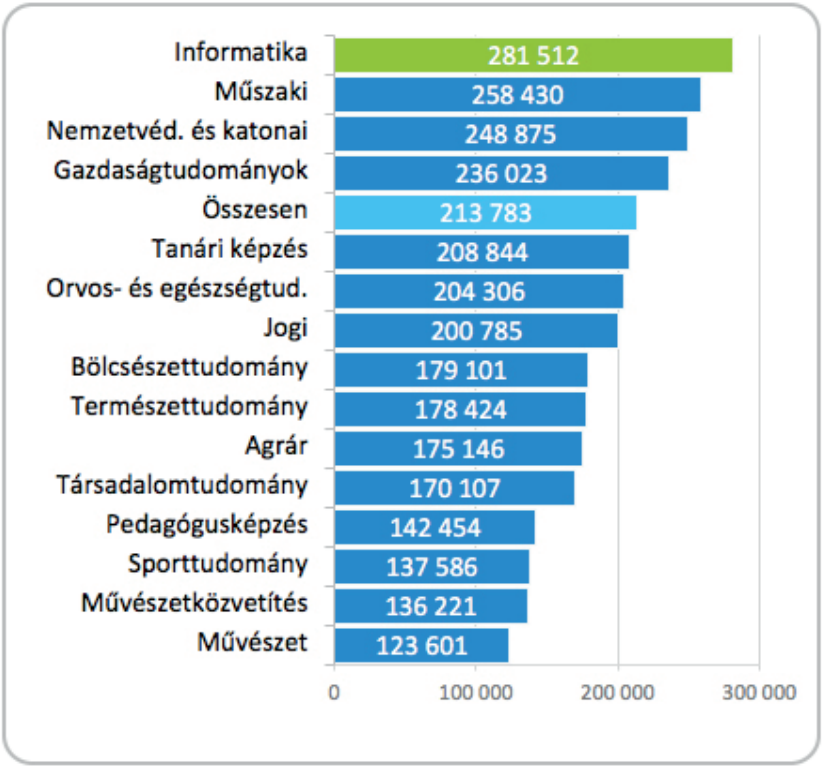
A CompTIA IT-iparági szervezet összeállította azokat az informatikai szaktudásokat, amelyek iránt 2016-ban a legnagyobb igény mutatkozik a munkaadók részéről. A vállalatok jelenleg a dolgok internetével és a nagy adatmennyiségek feldolgozásával, elemzésével kapcsolatos fejlesztésekre koncentrálnak. Örök problémájuk ugyanis, hogy – az informatika területén – folyamatosan jelennek meg az új technológiák, az ezek bevezetéséhez és üzemeltetéséhez értő szakemberekből azonban állandó hiány mutatkozik. (Mészáros, 2016) Azok az informatikusok tehát, akik a CompTIA által felsorolt szaktudások valamelyikével (vagy akár egyidőben többel is) rendelkeznek, bizonyosan kimagasló jövedelemre számíthatnak. A kiemelt szakterületek a következők:

- IT-támogatás
- információbiztonság
- programozás, fejlesztés, mérnöki ismeretek
- szoftvertesztelés és minőségbiztosítás
- infrastruktúra-adminisztráció
- stratégiai tervezés
- üzleti menedzsment
- információmenedzsment és adatelemzés

A Targetjobs dolgozata ugyanakkor a különféle IT-állásokra pályázókkal szemben szokásos elvárásokat foglalja össze. Bemutatja a leggyakrabban keresett 10 IT-állást, elmagyarázza azok lényegét, az elvárt diploma típusát és azt is, milyen képességekkel ajánlatos rendelkezni az állás betöltéséhez. Ezek az IT-állások az alábbiak:

1. Szoftvermérnök (alkalmazásfejlesztő, szoftverarchitekt, rendszerprogramozó/ rendszermérnök): elemzői képességekkel bír, logikus gondolkodású, képes csapatban dolgozni, figyel a részletekre.
2. Rendszerelemző (termékszakértő, rendszermérnök, megoldásszakértő, technikai tervező): képes információk kinyerésére és elemzésére, jól kommunikál, rámenős, érzékeny.

A frissdiplomások havi bruttó összjövedelmének átlaga
Magyarországon a képzési területek szerint



Forrás/közzétéve: ivsz.hu/projektek, ivsz.hu/wp-content

A frissdiplomások bruttó havi összjövedelmének átlaga a vizsgált képzés képzési területe szerint (Ft/hó)

Adminisztratív adatbázisok integrációja 2013, Educatio

3. Üzleti elemző (üzleti architektúra-, vállalati szintű információspecialista): jól kommunikál, jól prezentál, jártas a projektmenedzsmentben, jó problémamegoldó.
4. Technikai támogató (helpdeskes, működéselemző, problémamenedzser): széleskörű technikai ismeretekkel rendelkezik, jó problémamegoldó, jól kommunikál és képes meghallgatni másokat, türelmes, diplomáciai érzékkel rendelkezik.

5. Hálózati mérnök (hardvermérnök, hálózattervező): hálózatspecifikus ismeretekkel rendelkezik, jól kommunikál, tud tervezni, elemzői képességekkel bír, jó problémamegoldó.
6. Technikai tanácsadó (IT-tanácsadó, alkalmazásszakértő, vállalati szintű információspecialista): jól kommunikál, jól prezentál, érti a technológiát és az üzletet, jártas a projektmenedzsmentben, képes csapatban dolgozni.
7. Technikai értékesítő (értékesítési menedzser, ügyfélmenedzser, értékesítési vezető): termékismerettel rendelkezik, rámenős, interperszonális képességekkel rendelkezik, energikus, mobil, üzleti ismeretekkel rendelkezik.
8. Projektmenedzser (terméktervező, projektvezető, projekttervező): jó szervező, jó problémamegoldó, jól kommunikál, világosan gondolkodik, nyomás alatt is nyugodt marad.
9. Webfejlesztő (webtervező, webproducer, multimédia-architekt, internetmérnök): alapszinten érti a webtechnológiákat (kliens-, szerver- és adatbázisoldalon), elemző gondolkodású, jó problémamegoldó, kreatív.
10. Szoftvertesztelő (tesztelemző, minőségbiztosító szoftvertesztelő): képes figyelni a részletekre, kreatív, jó szervező, képes elemzően és kutató módon, feltáróan gondolkodni.

Mindössze két állás esetében (szoftvermérnök, hálózati mérnök) állítja a cikk szerzője, hogy feltétlenül szükséges informatikai szakirányú diploma, a többi esetben vagy előnyös, vagy nem szükséges. Egyetlen esetben mondja, hogy alapos programozói tudás javallt (webfejlesztő). Az említett képességek túlnyomó többsége vagy úgynevezett „soft skill", vagy elsajátítható ismeret, vagy adottság. (Mester, 2016) Megállapíthatjuk, hogy az egyes IT-állások esetében is elvárás a több szakma ismerete, és már elképzelhetetlen a vállalati tudás gyarapodása a különböző szakterületek konvergálása nélkül.

Az amerikai Munkaügyi Statisztikai Hivatal egy friss elemzése szerint ugyanakkor az Államokban egyre kevesebb programozóra lesz szükség az elkövetkező években. Véleményük szerint „az elkövetkező 10 év során mintegy 8%-kal fog csökkeni a szoftverfejlesztői állások száma annak ellenére, hogy a számítógépes (tehát felhasználói) munkahelyek száma 12%-kal bővül majd. A programozói állások visszaesése nem fog minden területet azonosan érinteni. Web-programozókból például a prognózis szerint 27%-kal többre

lesz szükség, mint jelenleg. Az asztali technológiákkal dolgozók ugyanakkor cserébe még az említett 8%-osnál is durvább csökkenésre számíthatnak a készségeik és ismereteik iránt mutatkozó keresletben." (Sting, 2016) Ez az elemzés is mutatja, hogy a jövő informatikus-szakemberek iránti igénye elsősorban a technikai fejlődés irányától és ütemétől függ. A magas informatikus-igény számát a becslések az informatikai fejlődés jelenlegi helyzete és üteme szerint határozzák meg, míg mások (pl. az amerikai kutatók) már a fejlesztések tartalmi irányváltozását is figyelembe veszik.

Talán nincs még egy olyan szakma, amelyben a folyamatos, élethosszig tartó tanulás annyira fontos, mint az informatikai-programozói területen, mert a technológiai ismeretek gyorsan elavulnak. A vállalatoknak hatalmas kihívást jelent az alkalmazottak képzése, ha nem akarnak versenyhátrányba kerülni. Mindenképpen gondoskodniuk kell arról, hogy a náluk dolgozó informatikusok folyamatosan képben legyenek a vállalati működés, a gyártott termékek, a nyújtott szolgáltatások terén jelentkező technológiai és informatikai újdonságokkal.

A programozói munkaerőigény átalakulása nagymértékben függ tehát a vállalati digitalizáció szintjétől, illetve a vállalat működési területétől, mert azt a digitalizáltságuk színvonala határozza meg. A globális nagyvállalatok elsősorban magas színvonalon képzett – mester- vagy doktori diplomával rendelkező – munkatársakat keresnek. A piacvezető globális kereskedelmi vállalatok az informatika területén vásárlóközpontú szemléletre tértek át, és az informatikai vezetőiktől azt várják el, hogy korszerű, felhasználói igények alapján kialakított alkalmazásokat szállítsanak a mindennapi funkciók támogatására is. Emellett az elkövetkező egy-másfél évben fejlesztendő új alkalmazások mintegy 90%-át a mobilhasználók igényeihez is igazítaniuk kell. Legfontosabb üzleti igényeik között szerepel a termelékenység növelése, az üzleti folyamatok automatizálása, de az adatok láthatóságának biztosítása, a felhőbe való migráció, valamint a kiberbiztonságra való törekvés, az incidensek elhárítási képességének javítása is.

A „saját (belső) hálózatot" üzemeltető és fejlesztő vállalatok többsége megelégedhet a középfokú végzettségű, de jó képességű informatikai munkaerővel, aminek az asztali technológiák fejlesztése-karbantartása és a relatíve alacsonyabb bérigény az oka. A modern technológiák alkalmazásába is

befektető (felhőalapú alkalmazásokat, illetve külső adattárakat is igénybe vevő) vállalatok számára azonban fontos, hogy legyen magas szinten képzett programozó az alkalmazottjuk.

Magyarországon is nagy a kereslet a képzett mérnökök és informatikusok iránt, akik a legjobban keresők között vannak, ugyanis havonta akár több százezres fizetést is kaphatnak. Állásváltoztatás szándékával nem kell hirdetéseket böngészniük, hiszen már nem a cégek válogatnak a jelentkezők közül, hanem a munkavállalók válogathatnak az ajánlatok közül. Egy jelenleg munkában álló szoftverfejlesztő pl. hetente átlagosan négy új állásajánlatot is kap. (Csányi, 2016) A HR-munkatársak feladata ma már inkább az új munkaerő „levadászása és átcsábítása", mintsem álláshirdetések megfogalmazása. Ehhez természetesen jól kell ismerniük a jelen és jövő vállalati igényeit, a további működésre kidolgozott vállalati stratégiákat is.

A statisztikák szerint Amerikában a fizetési lista első tizenöt helyén infokommunikációs állások találhatók. Magyarországon viszont – bár jelenleg számos betöltetlen álláshely van ebben az ágazatban – még azok közül sem mindenki ebben az irányban tanul tovább, akik informatikai középiskolába jártak.

Fremda (2016) szerint a Morgan Stanley Budapesten több mint 1200 embert foglalkoztató pénzügyi szolgáltató cégének csapatához évente 70-80 friss diplomás csatlakozik – elsősorban a matematikai és informatikai végzettséget nyújtó egyetemekről, főiskolákról –, mivel a tudományterületek között egyre inkább elmosódnak a határok. Míg tíz éve még klasszikus matematikusokat kerestek, ma már olyan szakemberekre van szükségük, akik emellett programozni is tudnak. Analitikus gondolkodásra, jó kommunikációs és prezentációs, valamint problémamegoldó képességre, nyelvtudásra és nemzetközi csapatmunkára van szükség az érvényesüléshez, a digitális írástudás pedig alapkövetelmény. A szükséges pénzügyi tudást a pályakezdők jellemzően a cégnél tanulják meg. Az elmúlt évek tapasztalatai alapján az egyértelműnek tűnik, hogy a területekre specializált tudás iránti igényt fokozatosan felváltja az alapkompetenciákra építő toborzás.

Mészáros (2016) összefoglalójában „A Salesforce Research kutatási jelentése szerint ahhoz, hogy valamely vállalat élen járjon a digitális átalakulásban és az innovációkat a lehető leggyorsabban meg tudja valósítani, új szakértel-

mekre lesz szüksége. Az új típusú appok kifejlesztéséhez nem áll rendelkezésre a munkaerőpiacon kellő számú hozzáértő szakember. Az informatikai vezetők több mint a fele nehezen talál megfelelő szakértelemmel rendelkező munkatársakat az adatmérnöki, az IT-biztonsági és az alkalmazásfejlesztési területen. A felhő alkalmazásával csökkenthető az alkalmazotti létszám, gyorsítható az innováció, és az alkalmazások és adatbázisok migrációja is egyszerűbbé és gyorsabbá válik."

Strausz (2016) szerint az informatikai vezetőkkel szembeni elvárások jelentősen módosultak. Korábban az IT-vezetők önállóan dönthettek az eszközberuházásokról és az alkalmazás-fejlesztésekről. Ma azonban továbbra is csak olyan beruházásokhoz lehet forrásokat kapni, amelyek elősegítik az üzleti célok megvalósulását, és amelyek megtérülését a CIO precízen ki tudja mutatni, de át kell értékelni az eddigi megvalósítási módszertanokat. Az üzlet egyre kevésbé tolerálja a hosszú, akár több éves projekteket, amelyek nagyszabású célokat tűznek ki és több dolgot akarnak egyszerre megváltoztatni, miközben az eredmény (vagy éppen eredménytelenség) is csak évek múltán jelentkezik. Ilyeneket már csak azért sem lehet csinálni, mert olyan gyorsan változnak az üzleti elvárások, hogy még a legpontosabban megfogalmazott igények mellett sem lesznek érvényesek az évekkel korábbi célkitűzések.

„Az informatika célja mindig is az volt, hogy elősegítse az üzleti célok megvalósulását, ám ennek eszközeit és módszereit hosszú időn keresztül az informatikai szervezet és annak vezetője határozta meg. Manapság viszont nem engedhetik meg maguknak a befelé fordulást, hanem az üzlet fejével gondolkodva kell a fejlesztéseken gondolkodniuk. Sőt, ahhoz is hozzá kell szokniuk – igaz, Magyarországon még csak kisebb mértékben –, hogy az informatikai döntések egy része az üzleti területeken születik." (Strausz, 2016)

9. Magyarországi kivándorlási helyzetkép

9.1. Kivándorlás a teljes népesség körében

A külföldi munkaadók a jól fizetett szenior pozíciókban kétszeres-háromszoros bérrel viszik külföldre a tapasztalt szakembereket, illetve azok tudását, munkaerejét. A külföldi munkaadók jóval rugalmasabbak, a magyar munka-

vállaló távmunkával azt is meg tudja oldani, hogy nem kell kitelepülnie (esetleg a hónap egy kisebb részét tölti kinn), így a magyar társadalom hagyományosan alacsony mobilitási hajlandósága nem akadály. A most középiskolás és egyetemista fiatalok nagy többsége már jól beszél angolul, külföldi tanulmányi ösztöndíjon jobban megszokja az idegen környezetet, így mobilabb, az agyelszívás sokkal jobban fogja veszélyeztetni. A tanulmányaikat külföldön folytató diákok pedig – a diploma megszerzése után – már jó eséllyel maradnak és vállalnak munkát külföldön.

A munkaerő-felmérés adatai szerint (KSH, 2014) külföldre túlnyomó részt a fiatal korosztályok tagjai költöznek. A migráns magyarok 25%-a 30 év alatti, 63%-a még nem érte el a 40 éves kort. További 18% tartozik a negyvenes korosztályba, 11% az ötvenesek közé, míg a 60 felettiek aránya mindössze 5%-os.

„A migráció munkaerőpiacra gyakorolt hatása szempontjából alapvető fontosságú a kivándorlók iskolai végzettség szerinti összetétele. Az adatok

A munkaerő-felmérés szerint külföldi telephelyen dolgozók létszáma a fontosabb ismérvek és országok szerint, 2013

Megnevezés	Ausztria	Németország	Egyesült Királyság	Egyéb EU tagország	Egyéb ország	Összesen
Nem						
Férfi	31 126	22 743	5536	8552	2901	70 858
Nő	11 634	6 545	3330	2934	2680	27 123
Életkor						
15-29	10 033	6836	4280	3062	2347	26 558
30-49	27 012	17448	4116	7021	2390	57 987
50-	5 715	5004	470	1403	844	13 436
Legmagasabb iskolai végzettség						
Egyetem, főiskola	4 365	4591	3292	1998	2402	16 648
Mióta dolgozik jelenlegi munkahelyén						
Kevesebb, mint 1 éve	12 249	11575	4649	4136	1893	34 502
Több, mint 1 éve	30 511	17713	4217	7350	3688	63 479
Összesen	42 760	29 288	8 866	11 486	5 581	97 981

Forrás: http://www.ksh.hu/docs/szolgaltatasok/sajtoszoba

egyértelműen jelzik a kivándorlók átlag feletti iskolai végzettségét és a diplomások koncentrációját körükben. Míg az itthon élő lakosság körében a 8 általánost vagy annál kevesebbet végzettek aránya 24%, addig a kivándoroltak között ez az érték 6% csupán. A többlet kisebb mértékben az érettségizettek, nagy arányban viszont a diplomások körében jelentkezik: a diplomások aránya az összlakossághoz képest a kivándoroltak között jelentősen magasabb (18% vs. 32%).

A kivándorlók közül a Nagy-Britanniába települők sajátos demográfiai összetételű csoportot képeznek. Az ide költöző magyarok különösen fiatalok: az adatfelvételkor átlagéletkoruk mindössze 33 év volt, kiköltözésük idején pedig mindössze 29 évesek voltak. Túlnyomó részük nőtlen vagy hajadon. Eltérően a németországi és az ausztriai bevándorlóktól, körükben meglehetősen kevés a szakmunkás (15%), viszont sok az érettségizett (43%) és a diplomás (36%). Lényegében azonos arányban találunk közöttük férfiakat és nőket." (KSH, 2014)

9.2. Frissdiplomások munkavállalása külföldön

Az Educatio Nonprofit Kft. 2015-ben a diplomás pályakövetési rendszer adatai alapján végzett kutatása a 2009-ben, 2011-ben és 2013-ban abszolutóriumot szerzettek teljes körére kiterjedt. A 3 évben összesen 21100 hallgató abszolválta felsőfokú tanulmányait, közöttük 1101-an (5,2%) informatikai szakterületen. Az adatokat azonban nem hasonlíthatjuk össze az azonos években felvett hallgatók számával, mert az abszolutórium megszerzésének éve – több félév ismétlése, évhalasztás, az oktatási rendszerből történő kilépés miatt – sok hallgató esetében kitolódik. A kutatást lezáró Educatio zárótanulmány – többek között – az alábbiakat tartalmazza:

A felsőfokú tanulmányokat követő években a frissdiplomások 7%-a dolgozott már külföldön és további 6%-uk a megkeresés időpontjában is külföldi munkavégzésről jelzett vissza. A külföldi munkavégzés leggyakoribb országa Németország, Ausztria és az Egyesült Királyság. A külföldi munkát végzők/végzettek aránya a sporttudományi, informatikai, természettudományi és műszaki képzési területek diplomásai között haladja meg az átlagot, és igen csekély a jogi, közigazgatási és pedagógiai frissdiplomások között. A külföldön dolgozók 39%-a felsőfokú végzettségéhez nem kapcsolódó munkát vállalt

külföldön a diplomázás utáni időszakban. Az itthoni frissdiplomások 28%-a tervez külföldi munkát az elkövetkező öt évben, további kb. egyharmaduk nem látja előre ilyen irányú terveit. A (további) külföldi munkát tervezők a legnagyobb arányban a műszaki és informatikai képzési terület frissdiplomái között vannak jelen.

A pályakövetési rendszer a munkaerőpiaci bekapcsolódást a felsőfokú tanulmányok idejére vonatkozóan is vizsgálja. „A frissdiplomások 45%-a már az abszolutórium megszerzésekor is főállásban dolgozott. A válaszadók megközelítőleg 60%-a végzett tanulmányai alatt szakterületéhez kapcsolódó munkát, s közel ugyanennyien kapcsolódtak be valamilyen nem szakmai munkatevékenységbe. A szakmai munkavégzésre leginkább az informatikai, pedagógusképzési és sporttudományi képzési területek hallgatóinak nyílt lehetősége a felsőfokú tanulmányok során.

Erősen szakmai vonatkozásúak az orvos- és egészségtudományi, jogi, pedagógiai, műszaki és informatikai diplomákkal betölthető munkakörök. A frissdiplomás foglalkoztatottak 17%-a azonban úgy érzi, hogy munkája nem igényel felsőfokú végzettséget. A felsőfokú végzettséget nem igénylő munkát végzők aránya az átlagosnál magasabb a bölcsész, agrár- és sporttudományi területek végzettjei között." (Veroszta, 2015)

A pályakezdőket ma már nem csupán a fizetés motiválja. Döntő többségük számára fontos például az, hogy a munkájuk pozitív és fenntartható változást hozzon a társadalom számára. Azt is lényegesnek tartják, hogy a szervezet, amelynél dolgoznak, hozzájáruljon egy jobb világ kialakulásához. A KPMG több mint 300, a világ vezető egyetemein és főiskoláin tanuló, üzleti szakirányra specializálódott egyetemistát kérdezett meg karrierterveikkel, elvárásaikkal és motivációikkal kapcsolatban.

„Szinte az összes diák úgy gondolja, a jó karrier építéséhez fontos, hogy kiterjedt nemzetközi kapcsolatokkal rendelkezzen. A válaszadók 89%-a felkészült arra is, hogy akár többször is más országba költözzön a megfelelő munka érdekében." (Balla, 2015)

„A magyar piacon azt tapasztaljuk, hogy a pályakezdők a szakmai fejlődési lehetőséget, a fiatalos, dinamikus környezetet és a jó társaságot keresik egy munkahelyen" – mondta a kutatással kapcsolatban a KPMG Magyarország HR-igazgatója. A szakember szerint fontos számukra a versenyképes kompen-

zációs csomag, a hosszabb távon is vonzó, kiszámítható karrier, valamint a munka és a magánélet egyensúlya is.

A diákok nem csak egy szerepben és egy országban gondolkodnak, hanem gyakran akár 2-3 különböző karriert is elindítanak. A munkavállalói preferenciák változásaihoz természetesen a munkaadóknak is alkalmazkodniuk kell. A KPMG globális HR-vezetője úgy véli, hogy „azoknak a szervezeteknek van lehetősége kitűnni a munkaadók közül, amelyek többféle karrierutat tudnak kínálni, különböző országokban." (Balla, 2015)

10. A munkaerőpiac jövője

A globalizáció és a feltörekvő országok gyors gazdasági növekedése komoly hatással van a munkahelyekre, ami már a közelmúltban is jelentős kulturális sokszínűséget eredményezett. A vállalatok gyorsan kiterjesztették üzleti tevékenységüket más országokra és a helyi környezetükün kívülről toboroznak alkalmazottakat. A munkatársak így több kontinensen és időzónában dolgoznak. Ennek a folyamatnak az is következménye, hogy a jövő munkahelyei lényegesen változatosabbak és fejlettebbek lesznek, amelyekre a nyelvi, kulturális és munkamódszerbeli sokszínűség lesz jellemző. Emiatt az üzleti vezetőknek olyan multikulturális munkakörnyezetet kell kialakítaniuk, amely elfogadja és támogatja a sokszínűséget. (Mészáros, 2016)

A jövő munkaerőpiacát jelentősen befolyásolja, megváltoztatja majd a napjainkban is zajló ipari forradalom, és ennek következtében egy vállalat digitalizációs szintje is. A Pew Research Center kutatóintézet 2014-ben megkérdezte a szerintük leginkább hozzáértő 1896 embert, mit gondolnak, inkább jó vagy inkább rossz lesz a dolgozó népnek a következő tíz évben az automatizáció és a robotok térhódítása. „A szakértők meglepően megosztottnak bizonyultak a kérdésben: 52%-uk optimista, 48%-uk viszont úgy gondolja, a társadalom nem fogja tudni megfelelően kezelni az új kihívásokat, így azoknak több lesz a vesztese, mint a nyertese. Akik nem félnek a jövőtől, azzal érveltek, hogy a történelem során már rengeteg technológiai innováció lezajlott anélkül, hogy negatív hatásai lettek volna a foglalkoztatásra, sőt általában inkább új munkahelyek jöttek létre miattuk. Szerintük hiába veszélyeztet

egy csomó munkahelyet a robotika terjedése, ezt bőven kompenzálni fogják a fejlődés során keletkező újak. A technológia megszabadít majd a kellemetlen munkáktól, ráadásul a folyamat arra is lehetőséget teremt az emberiségnek, hogy újragondolja a munka fogalmát kreatívabb, közösségibb, társadalmilag hasznosabb irányba.

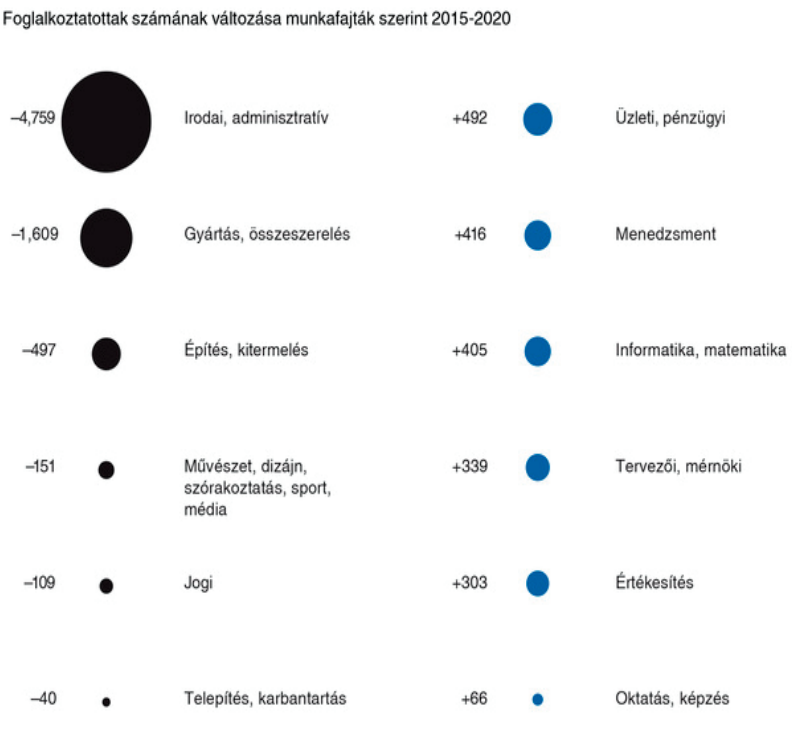
Ezzel szemben a majdnem ugyanennyien levő kételkedők úgy gondolják, hogy a negyedik ipari forradalom lényegileg különbözik a korábbiaktól, ezért sokkal nagyobb kihívást jelent majd a munkaerőpiacnak, mint elődei. Szerintük az átalakulás túl gyors lesz ahhoz, hogy a szabályozók és a gazdasági szereplők értelmesen tudjanak rá reagálni, ezért egy sor kellemetlen mellékhatás várható. Ilyen a fehérgallérosokat is érintő tömeges munkanélküliség, vagy a mélyülő szakadék a társadalmi rétegek között." (Előd, 2016)

A Világgazdasági Fórum (World Economic Forum, WEF) The Future of Jobs című jelentése szerint is komoly hatással lesznek az üzleti modellekben bekövetkező átfogó változások a munkaerőpiacra az elkövetkezendő években. (Mészáros/WEF, 2016) A kutatásban a legnagyobb munkáltatók HR-vezetői, továbbá akadémiai és nemzetközi szervezetek, professzionális szolgáltatócégek vezető szakértői vettek részt. 371 szervezet 13 millió alkalmazottját képviselték kilenc szektorban, tizenöt fejlett és feltörekvő gazdaságban (USA, Japán, Kína, India, Brazília, Mexikó, Németország, Franciaország, Spanyolország, Olaszország, Egyesült Királyság, Törökország, Dél-Afrika, Öböl-menti Együttműködési Tanács, Ausztrália, Délkelet-Ázsiai Nemzetek Szövetsége). A szakértők véleménye szerint a technológiai változásokkal egyidejűleg jelentős társadalmi-gazdasági, geopolitikai és demográfiai változások mennek végbe, amelyek hatása megközelíti a technológiai forradalomét. A válaszadók a változás demográfiai és társadalmi-gazdasági hajtóerői közül a legfontosabbnak a munka természetének megváltozását, rugalmassá válását tartják.

A technológiai jellegű ösztönző erők közül a legtöbben ugyanakkor a mobilinternet és a számítási felhő technológiáinak elterjedését jelölték meg a legfontosabbként. Ezt követte a számítási teljesítmény növekedése és a nagy adattömegek feldolgozása, valamint a dolgok internetének térhódítása. A jövő munkaerőpiacát nem egyedül a technológiai változások határozzák meg. Az idei World Economic Forumra is készült egy jelentés, amely meg-

próbálja számba venni a munkaerőpiaci változás összes lehetséges dimenzióját. Elődi (2016) bemutatja ezek közül a legérdekesebbeket:

- „A WEF-riport legijesztőbb állítása, hogy a munkaerőpiaci trendek alapján a világ 15 legnagyobb gazdaságában 7,1 millió munkahely fog megszűnni a következő 5 évben. Ezt szinte teljes egészében a mesterséges intelligencia és az automatizáció számlájára írható. A gépek eddig csak a kékgalléros pozíciókat veszélyeztették, de a jövőben már irodai dolgozók munkáját is feleslegessé tehetik.
- A veszteséget kompenzálni fogja, hogy a 7,1 millió munkahely megszűnésével párhuzamosan létrejön 2 millió új is, persze más ágazatokban, inkább a magasan képzett munkaerőt igénylő, kevéssé automatizálható feladatok elvégzésére. A pozitív és a negatív hatások összege mínusz 5,1 millió munkahely 5 év alatt. Ez inkább a változás sebessége miatt érdekes adat, az összes munkahely számához viszonyítva nem sok, a vizsgált országokban összesen 1,86 milliárdan dolgoznak ma, vagyis a világ összes dolgozójának 65%-a.
- A munkahelyek megszűnése nem egyformán érinti az egyes ágazatokat, lesznek olyanok, amelyek kifejezetten felvirágoznak majd a közeljövőben, másokban viszont jelentős mennyiségű dolgozót fognak leépíteni. A kutatók számításai szerint a megszűnő munkahelyek kétharmada az irodai adminisztratív munkakörökre koncentrálódik, de nem fognak jól járni a gyártásban, építésben, összeszerelésben dolgozók sem, sőt a szórakoztatóiparban is csökkenő emberi munkaerőigényre lehet számítani.
- A munkahelyek számának csökkenésén túl lesznek más lényeges változások is a foglalkoztatásban. Terjedni fognak az atipikus, rugalmas foglalkoztatási formák, amelyek a jól képzettek számára új lehetőségeket teremthetnek, de összességében növelik a foglalkoztatási bizonytalanságot és magasabb fokú tudatosságot igényelnek a munkavállalók részéről. Egyre több mérnökre és IT-szakemberre lesz szükség. Az elöregedő társadalmakban növekedni fog az egészségügyi szektor súlya, míg a fiatalabb populációval rendelkező feltörekvő gazdaságokban az oktatásban lesz szükség sok munkaerőre. Arányaiban nőni fog a női foglalkoztatottság, és valószínűleg több nő lesz vezető pozícióban, mint ma. Szinte biztos, hogy már a közeljövőben egy csomó új típusú állás jön létre. Ezek az új munkafajták részben



Forrás/közzétéve: index.hu/gazdasag/2016/03/18

talán olyasmik lesznek, amikről most nem tudjuk elképzelni, hogy piaci alapon működőképesek lennének, de később már lesznek, akik fizetnek értük. Természetesen az IT-szektorban is egy csomó új igényt hozhatnak a következő évek.

- A jelentés szerint már 2020-ra kicserélődik a munkáltatók által elvárt legfontosabb tulajdonságok egyharmada olyan képességekre, amelyek ma még nem szerepelnek a topligában. Ez is különbözően érinti az egyes iparágakat, a legkevésbé a média és szórakoztatóipar változik majd ebből a szempontból, a legjobban pedig a pénzügyi, befektetési ágazat.
- Kérdés persze, hogy fog mindezzel lépést tartani az oktatás. A pesszimisták szerint leginkább sehogy, és ebben a kérdésben még a pozitívabb jövőképpel rendelkezők is elismerik, hogy komoly gondok vannak. Már ma is az a hely-

zet a gyorsan változó ágazatokban, hogy mire a diákok eljutnak az egyetem utolsó évéig, az elsőévesként megtanult anyagnak nagyjából a fele már elavultnak számít. Ráadásul sok ország (köztük Magyarország) még egyáltalán nem eszmélt rá, hogy az általános iskolától kezdve olyan dolgokkal tömik tele a diákok fejét, amelyek abszolút nem számítanak hasznos tudásnak az internet világában.

- Éppen ezért a jövőben meg kell, hogy változzon a munkáltatók szerepe. Az átalakulásban nagy rész jut majd a multiknak, amelyek hiába csak a kisebb részét foglalkoztatják a világ 3 milliárd dolgozójának, helyben rengeteg kisebb vállalkozást is életben tartanak. Ezért sok múlik majd azon, a nagy cégek hogyan kezelik a problémákat és mennyire tudnak gyorsan alkalmazkodni a megváltozott követelményekhez.
- Lassan, de biztosan beköszönthet a nők kora. Több iparágban ők lehetnek a változás motorja, most viszont úgy tűnik, hogy a megszűnő munkahelyek nagyobb része esik majd azokra a területekre, ahol több nő dolgozik. Tipikusan ilyenek az egyszerűbb, adminisztratív irodai munkák, amelyeket a legjobban megritkítanak a mostani folyamatok. Ezt súlyosbíthatja, hogy az új állások többsége olyan iparágakban jön majd létre, amelyekben a nők hagyományosan alacsonyabb arányban vannak jelen."

Az ITBehaviour (2016) szerint – mint oly sok más területen – az informatikában is kötelező érvényű és azonnal kamatoztatható tudást jelent az érzékenység, a kreativitás és az empátia, vagyis amit a férfiak női tulajdonságnak vélnek (ma divat már az EQ mérése a HR-es embervadászatban). Az idén 5. alkalommal megrendezett Lányok Napja[2] nem titkolt célja, hogy 2020-ra az ICT-cégek munkatársainak 30%-a nő legyen. A színesség, a különbözőség, a más álláspontok és ötletek ütköztetése kiemelt jelentőségű, sőt ma már kötelező a folyamatos innovációban. A program kiváló lehetőséget nyújt arra, hogy már fiatal kortól arra ösztönözzék a lányokat, bátran válasszák az informatikai/programozói pályát, hiszen minden eddiginél több informatikusra lesz szükség, és nem csak az Európai Unióban. A Big Data korában hatalmas szükség lesz olyan szakemberekre, akik biztonságosan tárolják és dolgozzák fel az adatgyűjtő eszközök által megszerzett információkat.

2 A nap, amikor sok vállalat, kutatási intézmény, egyetemi laboratórium nyitja meg kapuit a középiskolás lányok előtt a tudomány és a technológia, a kutatás és az informatika területén.

11. A kibertér hátterét biztosító oktatás

11.1. Az oktatási rendszerek

„Hiába tűnik jónak egy ország oktatási rendszere, azt nem lehet lemásolni úgy, mint mondjuk egy gazdasági rendszer egy központilag tervezett gazdaságból piacgazdaságra való átállása során. Az oktatásnál sokkal jobban jelen van az ország kultúrája és hagyományai, mint egy gazdasági berendezkedésnél. Természetesen egyetlen ország sem tökéletes, és mindenhol van lehetőség fejlesztésre, tehát a beiskolázottság, az írni-olvasni tudás és a diplomások és kutatók számának növelésére." (Vörös, 2014)

A felsőoktatás intézményrendszerét szerte a világon két fő típus, az egyetem vagy a főiskola teszi ki, a képzés általában 3 szintű: alapszak, mesterszak és doktori képzés. Az intézmények lehetnek állami vagy magánintézmények. Az állami egyetemeket és főiskolákat a kormány finanszírozza, a magánegyetemeket és főiskolákat magánúton működtetik. A főiskolák általában kisebbek, mint az egyetemek és csak alapképzést nyújtanak. A felsőoktatási intézményekben – legyen az akár állami, akár magán – a hallgatók különböző címeken ösztöndíjat szerezhetnek, ami vagy teljesen ingyenessé teszi a diplomaszerzést számukra, vagy valamilyen részben csökkenti tandíjukat. A tandíj azonban igen tetemes összeget tesz ki, amire a hallgatók „diákhitelt" vehetnek igénybe, tehetős családból érkező hallgatók esetében a szülők térítik meg azt. A hitel összege általában olyan magas, hogy annak összege akár egy helyben vásárolható ház értékét is kiteszi, és a hitelt igénybe vevő diáknak akár élete végéig kell fizetnie. Az ösztöndíjat nyújtó egyetem ugyanakkor abban érdekelt, hogy az oktatási területe szempontjából legtehetségesebb diákokat támogassa, és ennek megfelelő toborzási eljárást alkalmaz.

A magánegyetemek esetében nem kizárt, hogy adományok formájában támogassák azokat, pl. oktatási alapítványok (pl. a Bill és Melinda Gates Alapítvány) rendszeres támogatásban részesítsék az általuk kiválasztott egyetemet. Ennek fejében természetesen célzott kutatási megrendeléseket is adhatnak az intézménynek.

Az egyetemek oktatáson kívüli fontos célkitűzése a kutatási tevékenység is. Már az egyetemi oktatás megkezdésekor is a középiskolában megfelelően képzett hallgatókra építenének, akikből – a doktori képzést követően – akár

a jövő tudósai válhatnak. A tudomány azonban – ide értve elsősorban az informatika területét – olyan gyorsan változik, hogy oktatásával, művelésével még ezek az intézmények is nehezen birkóznak meg. Szalay professzor (2016) szerint „még az amerikai egyetemek is nehezen küzdenek meg azzal, hogy a tudomány nagyon gyorsan változik, egyre többféle, egyre szerteágazóbb tudásra van szüksége egy modern tudósnak."

Berács-Temesi (2016) álláspontja szerint „Európának meg kell újulnia ahhoz, hogy felzárkózzon az észak-amerikai kontinens egyetemeihez, illetve ahhoz, hogy az Ázsiában megfigyelhető gazdasági növekedés hamarosan a felsőoktatásban is éreztetni fogja hatását. A világon jelenleg 100 millió felett van az egyetemi hallgatók száma. Közülük több mint 2 millió hallgató külföldi állampolgárként vesz részt a felsőoktatásban, tehát nem a hazájában tanul. A fogadó országok listáját az USA, Anglia, Franciaország, Németország, Ausztrália után már Kína és Japán követi. A küldő országok listáját Kína, India, Japán és Korea vezeti, de a 10. helyen már az USA is megjelent ebben a rangsorban. A külföldi szemeszterek befejezése után azonban a diákok általában visszatérnek hazájukba, otthon kamatoztatják külhonban megszerzett ismereteiket.

Az ázsiai országok arra törekszenek, hogy kiaknázzák a magán- és a közszféra együttes jelenlétéből származó lehetőségeket. Az állami és magánegyetemek egyaránt fejlődnek, a piaci mechanizmusok beengedése a felsőoktatás rendszerébe pedig nem szorítja háttérbe a kormányzatok aktív részvételét az oktatás finanszírozásában, a tudást ösztönző tevékenységébe. Az ázsiai állampolgárok értékelik a tudást, tudják, hogy pénzbe kerül, hogy megszerzéséhez stresszes évek szükségesek, de költenek rá mind egyénileg, mind társadalmi szinten. Az elmúlt évtizedekben a fiatalok többsége az amerikai, európai elitegyetemekre áramlott. Most, a második hullámban, Amerika és Európa, mellett, dinamikusan növekszik az ázsiai országok egymás közti mobilitása is." (Berács-Temesi, 2008)

A japán kormányzat is támogatja Japán, mint fogadó ország státusának erősítését. A japán felsőoktatásban tanuló külföldi hallgatók száma 25 évvel ezelőtt alig haladta meg a tízezer főt. Mintegy húsz évet vett igénybe, hogy ma már 118 000 külföldi hallgató tanul Japánban. 92%-uk Ázsiából érkezik; Európa 3%-kal, Észak-Amerika 1,8%-kal részesedik a külföldi hallgatók össz-

arányából. A hallgatók 73%-a magánegyetemen tanul. Viszonylag alacsony a tandíj, és egyre több egyetem vesz részt a nemzetközi képzésben. Az ázsiai országok még nem rendelkeznek az Erasmushoz hasonló központi programmal, de a nemzeti stratégiák ennél lényegesen nagyobb diákáramlást fognak kiváltani. Magyarország és a hozzánk hasonló kis országok számára érdemes felkészülni az 5-10 éven belül kibontakozó harmadik hullámra, amikor már Ázsia is az európai hallgatók fontos külföldi úti célja lesz. (Berács-Temesi, 2008)

„Míg az ázsiai országokban kevésbé adnak teret a kreativitásnak, addig a nyugati országok inkább az egyéni ötleteket támogató tanítást választják. Az arany középút természetesen a kettő ötvözése lenne, azonban ezt kevés országban tudják sikeresen megvalósítani." (Vörös, 2014) Más megfogalmazás szerint vannak „önmegvalósító" és „teljesítménykényszeres" oktatási rendszerek. Ezek jellemzőit az alábbi példák mutatják be.

Dél-Korea az oktatásban világelső, és abban is első a világon, hogy a 25-34 éves korosztály kétharmadának van egyetemi végzettsége. Az ország abban is világelső, hogy az egyetemen tanulók 13%-a tanul külföldi, elsősorban amerikai egyetemeken. Dél-Koreában kijelöltek az évben egy napot, amikor az érettségit tett diákok képességét felmérik. Ekkor nem az iskola minősít, hanem a diákokat nem ismerő szakbizottság. Csak ennek a felmérésnek az eredményei alapján nyílik lehetőség az egyetemre jutásra. Hogy melyik egyetemen folytathatja a diák a tanulmányait, attól függ, hogy ki hogyan végzett ezen a minősítésen. Az egyetemre jutás lehetőségét a szülők is támogatják, nagy gondot, időt és költségeket fordítanak gyermekeik tanulmányaira, Szöulban pl. a családi jövedelem 16%-át a gyerekek iskolán kívüli oktatására költik. Az egyetemen szerzett diploma életre szóló karriert garantál. (Kopátsy, 2013)

Az Eduline (2009) szerint jó tudni, hogy az amerikai iskolákban néhány kötelező tárgyon kívül a diákok szabadon választanak tantárgyakat, az ottani iskolákban nem jellemző, hogy nagy nyomás alatt kellene gyakorolni a tanulmányaikat. A tantárgyak gyakorlatorientáltak és nagy számban lehet válogatni az érdekesebbnél-érdekesebb tanórai lehetőségek közül. Az oktatás célja, hogy önbizalmat nyerjen a diák az iskolai foglalkozások során. A számonkérés tesztek formájában történik, amiket előre bejelentenek. Ha valami előnyként jelentkezik egy amerikai középiskolai tanév során, akkor az, hogy

a gyerekek önbizalma és önállóságra való törekvése hatalmas ütemben fejlődik. Az iskolaév pontos tartamát Amerikában minden iskola maga határozza meg. Nagy figyelmet szentelnek az egyes diákok érdeklődési körére, és annak megfelelő pályaorientációs fejlesztésére.

A Kínai Népköztársaság 1979-es gazdasági fordulata után felgyorsult a tudásalapú társadalom kiépülése. A Népköztársaság prioritásként fogalmazta meg, hogy minden polgára befejezze az iskolai tanulmányokat. Az iskolakötelezettség időtartamát kilenc évben határozták meg, ami 15 éves korig tart Az ezt követő 3 éves időszakban a diákok részt vehetnek egy egyetemre felkészítő középiskolai oktatásban. A diákokból hiányzik a kreativitás, az iskolában inkább „magolni" tanítják őket. A kínai egyetemekre való bekerülés nagyon költséges, ezért a 20 évesek mindössze 22%-a tanul a felsőoktatásban. Az állam mellett a családok is jelentős összegeket invesztálnak az oktatásba, a gazdasági, politikai elit számára külön egyetemek nyíltak. Az egyetemeken, főiskolákon tanulók száma folyamatosan növekszik. Kínában csak az számít, ki a legjobb tanuló. A szülők ezért különösen szigorú elvárásokat támasztanak gyermekükkel szemben, ugyanakkor jelentős összegeket áldoznak a taníttatására. A kínai családokban leginkább a „Tigrisanya" határozza meg a családi elvárásokat, és folyamatosan ellenőrzi gyermeke teljesítményét, (a szabályozásból eredően egyke) gyermeke eredményes tanulmányi eredményeiért pedig minden szigort és fenyítést bevet. (Vörös, 2014)

India szövetségi államként megosztja az oktatási jogköröket a szövetségi kormány és a tagállamok között, de a gyakorlatban a szövetségi kormánynak van döntő szerepe, mivel az jelöli ki az oktatáspolitika irányát, és a finanszírozás is a központi kormánytól függ. A brit mintájú indiai iskolarendszerben az általános iskolai tanulmányokat egy négyéves oktatási kurzus követi, ami 14 éves korig tart, és egy közbülső szint az általános és a tulajdonképpeni középiskola között. A felsőoktatásban három különböző intézménytípust találhatunk: műszaki főiskolákat, főiskolákat és egyetemeket. India a kiváló minőségű oktatási rendszer és az oktatásra alapozott fegyelmezett, képzett munkaerő nélkül soha nem érte volna utol egykori gyarmattartóját, Nagy-Britanniát. Korábban az iskolázottság olyan alacsony szintű volt, hogy az 1986-os oktatáspolitikai ötéves terv célul tűzte ki: 1990-ig az összes 11. életévét betöltött gyermek öt évet töltsön az általános iskolában. Ezt az időszakot

követően az állam jelentős erőforrásokat fordít az oktatási rendszer hatékonyságára. (Figyelő, 2012)

Kínában és Indiában az oktatást kezdettől fogva a prioritások közé sorolták. Mindkét országban a legmagasabb szinteken vállalták az oktatási minőségbiztosítást. Az állami oktatásnak, valamint a tanulás megbecsülésének évezredes hagyományai vannak.

Az Egyesült Királyságban a diákok számára 16 éves korban esedékes az érettségi vagy GCSE (General Certificate of Secondary Education) vizsga. Ezután a tanulók eldönthetik, hogy akarnak-e továbbtanulni, vagy munkába állnak. Miután a diák megszerezte a GCSE-képesítést és úgy dönt, hogy főiskolára vagy egyetemre szeretne jelentkezni, vagy szakmát szeretne tanulni, úgy 2 éves képzésen továbbtanulhat és megszerezheti az A-Level (emelt szintű) érettségit, vagy GNVQ- vagy BTEC-képesítések egyikét. Ez az oklevél az alapja annak, hogy főiskolára vagy egyetemre jelentkezhessen a diák. Az állami oktatás a tankötelezettség lejárta után is ingyenes 19 éves korig, illetve 25 éves korig azok számára, akik korábban nem vettek részt ilyen jellegű oktatásban, illetve nem szereztek bizonyítványt. Ezen a 2 éves képzésen már nincsenek kötelező tárgyak. Minden tanuló érdeklődésének megfelelően, illetve további terveinek fényében választhat az adott iskola által kínált tantárgyakból. A felsőoktatási intézmények közé tartoznak az egyetemek (universities) a főiskolák (higher education colleges) és az ún. „university college"-ok. A 2004-es felsőoktatási törvény tette lehetővé, hogy a főiskolák és egyetemek tandíjat kérjenek hallgatóiktól. (London Aid Specialist Ltd., 2015)

Vörös (2014) jellemzése szerint „Törökország oktatási rendszere – strukturáltsága tekintetében – többé-kevésbé megegyezik Magyarországéval. Az intézmények többsége állami tulajdonban van és a diákok 95%-a ilyenekben tanul. Magyarországhoz hasonlóan Törökország is részt vesz az Erasmus programban."

Oroszország oktatási rendszere a világ 15 legjobbja között szerepel. Az oktatás jellegzetessége, hogy szinte teljesen ingyenes. Ez egyrészt a Szovjetunió hagyatékának is köszönhető, másrészt pedig annak, hogy a tanulók több mint 99%-a állami intézményekben tanul (a felsőoktatásban ez az arány valamennyivel kisebb). Oroszországban kötelező egy 11 éves iskolai időszak, ami az általános iskolát, a középiskolát és az egyetemi felkészítő képzést tartalmazza. A programot a legtöbb intézmény egy egységben, ugyanazon intézményen

belül kínálja. A diákoknak lehetősége van arra is, hogy az utolsó két évet szakképzésben töltsék el. Ezt követően egy sztenderdizált tesztet kell elvégezniük, ez alapján nyerhetnek felvételt az egyetemekre. Az állam csak egy bizonyos számú helyet biztosít ingyenesen (akárcsak Magyarországon), a többi hely tandíjköteles. 2007-től Oroszország is a bolognai rendszerű oktatást biztosítja, tehát a 3-4 éves alapképzést és a 2 éves mesterképzést. Ösztöndíjakat és ingyenes lakhatást biztosít az állam az egyetemre az ország távoli pontjairól érkezőknek. Az orosz lakosság több mint 60%-a iratkozik be felsőoktatásra, ami magas aránynak mondható. Az orosz oktatásban az orvosi és matematikai képzés világhírű. (Vörös, 2014)

Charlotte (2015) összefoglalója alapján a finn rendszer összeolvasztja az általános iskolát és a középiskolát egy kilencéves alapiskolába, amiben minden diáknak tanulnia kell. Minden iskola jó, és mindenhol lehetséges az átjárás az iskolák között. Az alapoktatásban a tanárok odafigyelnek a diákokra; ha problémát látnak, mert egy gyerek tanulási nehézségekkel küzd, azt orvosolniuk kell. Minden diáknak, 18 éves koráig részt kell vennie pályaorientációs és tanácsadói beszélgetéseken, hogy a későbbiekben helyes döntéseket tudjanak hozni. A középfokú oktatás felépítése moduláris elven működik, nem pedig egy tanterv szerint, nincsenek évfolyamok sem. A diákok az iskolák által ajánlott kurzusokból maguk építhetik fel a tantervüket. Finnország oktatási rendszerére a kevés tanítási óra jellemző, ami átlagban napi négy óra. A teszttek helyett a diákokat az órai aktivitás figyelembevételével értékelik, ezért nincsenek jegyek sem. A rendszer hátránya, hogy az iskolák bizonyítványai nem összehasonlíthatók. A finneknél az érettségi három szakaszban zajlik, összesen 18 hónapon keresztül. A finn tanárok szakmájukban igen nagy szabadságot és szabad kezet kapnak. Sokan vannak, akik nem a fizetésért dolgoznak, hanem a szakma adta lehetőségek, szabadság és kreativitás miatt. Csupán ahhoz, hogy valaki alapfokú oktató legyen, mesterképzés kell.

„Szingapúr három egyeteme közül kettő benn van a top 50-ben." (Cseke, 2016) Szingapúrban a gyermekeknek már az általános iskola befejezésekor vizsgázniuk kell, később pedig mindig tesztet kell írniuk, mielőtt felsőbb intézménybe lépnének. Az egyik sorsdöntő írásbeli vizsgára 12 évesen kerül sor, ekkor dől el, hogy gimnáziumban, technikumban vagy valamilyen szakképzőben, esetleg felzárkóztató intézetben tanulhat tovább egy gyermek. Szigorú

ponthatárok vannak, ha valaki nem felel meg, akkor egy „váltó" más irányba tereli. A szingapúri iskolarendszer egy valódi versenyistálló. Cseke (2016) szerint a magas színvonalú oktatás záloga, hogy csak a legkiválóbbak kerülnek a pedagóguspályára. Szingapúr oktatási rendszerének egyik pillére a tanárképzés minőségének magas színvonala, emellett az idősebb tanárok is mentorálják fiatalabb kollégáikat. Egyetemre kizárólag a legjobban érettségiző diákok 30%-a jelentkezhet. Közülük választják ki a jövő tanárait is. Képzésükre különös gondot fordít az állam, kiemelt ösztöndíjat kapnak, fizetésük már pályakezdőként meghaladja a szingapúri átlagjövedelmet. Az oktatási minisztérium osztályterem-laboratóriumokat tart fenn, ahol a jó gyakorlatokat kísérletezik ki és adják tovább egymásnak a tanárok, akik emellett évi 100 óra szakmai továbbképzésen is részt vesznek, hogy naprakész ismeretekkel rendelkezzenek szakterületük legújabb tudományos-technológiai eredményeiről. A szingapúri oktatás filozófiája, hogy minden gyermek képes a tanulásra, ám differenciáltan kell fejleszteni őket, hogy a maximumot hozzák ki belőlük. Már a kezdetekkor a képességeiknek megfelelő képzési programokban vesznek részt, s nem hagyják, hogy lemaradjanak a gyengébb képességűek. Akiknek nehezen mennek a tudományos tantárgyak, szakmai tárgyakat választhatnak, illetve a művészeteket vagy sportot. Már az alapfokú intézményben tanítják a matematika, a nyelvtan és a természettudományos tantárgyak mellett a kritikai gondolkodást és azt, hogy a diákok merjenek kezdeményezni. (Cseke, 2016) A magyar közoktatási rendszert a szingapúri minta alapján kívánják átalakítani.

11.2. Magyarország közoktatási rendszere

Tóth (2015) megállapítása szerint idehaza tévedésben élnek az emberek az informatikusi munkával kapcsolatban, a magyar szülők 20-25 évvel le vannak maradva. A többség most is úgy hiszi, hogy jogászként, orvosként vagy mérnökként könnyebb érvényesülni. Talán az e hitben élő családi háttér is oka lehet annak, hogy hazánkban a középiskolás diákok többsége nem is érdeklődik az informatikai szakma iránt, bármennyire is jól kezeli okostelefonját, táblagépét vagy laptopját.

Ezek működésének elvére, a működtető technológiára már sokan nem kíváncsiak. A pályaorientáció segítése érdekében fontos a szülők megszólítása,

mivel egyrészt nekik sincs kialakult képük az informatikus szakmáról, és nem ismerik az elhelyezkedési-jövedelmi lehetőségeket, másfelől pedig a gyerekek leginkább őket tekintik az elsődleges információforrásnak. Szintén fontos információs „csatorna" lehet az informatikatanár. (BellResearch, 2015)

Azt sem hagyhatjuk figyelmen kívül, hogy az informatikai szakterület művelése elképzelhetetlen magas színvonalú angol nyelvtudás nélkül. Ennek általános hiányára pedig a nyelvvizsga hiánya miatt ki nem adott egyetemi diplomák sokasága mutat rá. A tárgyalóképes nyelvtudás mellett ugyanakkor magas szintű kommunikációs készséggel is kell rendelkeznie egy informatikusnak, hogy egy jó fejlesztési eredmény érdekében szűkebb szakmai területén jó kapcsolatokat építhessen ki az üzletági szakemberekkel.

A szakértők alig győzik hangsúlyozni, hogy az informatikai ismeretek alapját, a kódolást már a középiskolákban, és nem az informatika tantárgy keretében kellene oktatni. Az Európai Unió 28 tagországából 14-ben a programozás már külön tantárgy. A digitális írástudást minden egyéb tantárgy keretében fejlesztik. 2013-ban az oktatási szektorban a magyar kormány több mint negyven rendszerszintű változtatást indított el. Az ilyen nagyságrendű reformot végrehajtó országok példája azonban azt mutatja, hogy legalább egy évtizedre van szükség ahhoz, mire a bevezetett intézkedések hatása mérhetővé válik.

A magyar közoktatási rendszer kritikáját oktatók, oktatáskutatók és munkaadók egyaránt megfogalmazták. Nahalka (2016) szerint „A különböző kormányok leginkább azért hibáztathatók, mert nem sokat tettek a mélyben zajló folyamatok jobb megismeréséért, és egy hosszú távú, valódi változásokat hozó gyakorlat kialakításáért. A sikeres országok példája mutatja, hogy nem a gyerekeknek kell alkalmazkodni az iskolához, hanem fordítva. Magyarországon ez nem így van. Olyan oktatási rendszert kell kialakítani, amelyben minden tanuló azt kapja az iskolától, amire az optimális fejlődéséhez speciálisan neki szüksége van." Balla (2015) szerint „Az nem állapot, hogy van egy intézményünk, az úgynevezett iskola, amit elvileg azért tart a társadalom, hogy fiatal tagjait felkészítse az életre, munkavállalásra, de erre már képtelen, mivel a digitális tudás szinte mindenhova kell már a munkahelyeken, az oktatás viszont lemaradt a forradalom mögött, ezért a tanulóknak más nem hivatalos utakon kell megszerezniük a szükséges tudást."

Kiderült, hogy az iskolaiszámítógép-használat nem fejleszti a digitális készségeket, az otthoni viszont igen. Sőt, az iskolai számítógépezés nemhogy nem fejleszti, egyenesen negatív hatása van a tanulókra. Az informatikaórák tananyaga elavult, a kilencvenes évek kihívásaira készít fel, néha szó szerint a kilencvenes évek válaszaival, grafikáival. Ma már nem tudnak ezzel mit kezdeni a gyerekek. Ezen kívül az okoseszközök a legtöbb intézményben tiltottak, ahelyett, hogy kihasználnák a modern eszközöket és biztosítanának azoknak, akiknek nincs rá pénzük. (Lannert, 2015)

Részben megoldást jelentenek a technológiakövetés égető problémájára az online informatikai képzések, amelyek nagy választékban érhetők el az interneten, akár teljesen ingyen is. Az angol rövidítésük alapján MOOC-nak (massive open online course, tömeges nyitott online kurzus) nevezett távoktatási képzések kiváló lehetőséget kínálnak a fejlődésre, nemcsak az informatika területén, hanem a legkülönfélébb más szakmákban is. A MOOC-ok a képzésekkel kapcsolatos három nagy gondon enyhítenek: pénzkímélők, lépést tartanak a fejlődéssel (folyamatosan jelennek meg új kurzusok) és internetkapcsolat birtokában bárhonnan elérhetők. Gyakorlatilag korlátlan számú jelentkezőt tudnak fogadni és bárki részt vehet a képzésen a weben keresztül, ha ismeri a nyelvet, amelyen azt tartják. Az online oktatási programok gazdag választéka lehetővé teszi továbbá, hogy olyan kurzusokon is részt vehetnek az érdeklődők, amelyek közvetlen környékükön vagy az országukban nem elérhetők, illetve a hagyományos oktatási formában túlságosan sokba kerülnek. Távoktatással mód nyílik neves külföldi egyetemek online elérhető képzéseit is látogatni. (Mészáros, 2016)

Az online kurzusok létjogosultságát és népszerűségét jelzi például, hogy egy harvardi diák két év után megszakította egyetemi tanulmányait, mert elavultnak tartotta az ott oktatott informatikai tananyagot. Saját szoftverfejlesztési módszertant és programozási anyagot dolgozott ki, majd online iskolát indított, ahol a diákoknak a tandíjat csak az után kell megfizetni, amikor már állást kaptak. Ilyen típusú kurzusokat Magyarországon is indítottak. „A felnőttek a Green Fox Academy 4 hónapos képzésén, egymillió forintos tandíjért szerezhetnek programozói szaktudást. A Codecool azt ígéri, hogy másfél év alatt képzi profi programozóvá a jelentkezőket, és Budapesten 390 ezerbe, Miskolcon 300 ezer forintba kerül egy félév, ám ezt csak akkor kell

kifizetni, ha sikerült is munkát találni. Ma már ki sem kell mozdulni otthonról, ha tanulni akarunk. A Codecademy oldalán ingyen végig lehet venni az alapokat számos programozási nyelven. A Courserán külföldi egyetemek kurzusaira lehet befizetni, és 2015-ben a Miskolci Egyetem is elindította a nyílt képzési portálját, ahol az adatbázis-kezeléstől a szerverüzemeltetésig több tucat különböző informatikai kurzusra lehet jelentkezni." (Tóth, 2015)

A BellResearch (2015) kutatása alapján megállapítható, hogy a piacon igény mutatkozik rövidebb, gyakorlatorientált képzésben részesülő szakemberekre is; Magyarországon ezen OKJ-s képzésekkel próbálnak segíteni. Az OKJ-s képzéseknek az értékét azonban nem ismerik el. Sokan már tizenéves korukban önállóan megtanulnak programozni, és az informatikusokra általában is jellemző, hogy maguktól utána járnak olyan dolgoknak, amik érdeklik őket, folyamatosan fejlesztik a tudásukat. Ők még az OKJ-s képzésekben sem vesznek részt.

Hazánkban valódi informatikaoktatás (az informatikai szakközépiskolák kivételével) nincs, a programozás elenyésző hányadban része a tananyagnak. A középiskolai oktatás összességében nem támogatja az informatika szempontjából rendkívül fontosnak ítélt gondolkodás-központúságot, minden esetben az érettségi követelményrendszer által egyébként forszírozott lexikális tudás kerül előtérbe. (BellResearch, 2015)

A fejlett ipari országokat tömörítő szervezet, az OECD 2000-ben felmérést indított a középiskolai tanulók tudásának megismerésére. A PISA (Program for International Student Assessment) háromévente lebonyolított vizsgálatsorozat keretében a 15 éves tanulók tudását vizsgálják meg, mert ők azok, akik még iskolaköteles korban vannak, de már közelednek a felsőoktatásba való belépés és a munkavállalás felé. A tesztek alapján a diákok képességpontokat kapnak, és ezek összesítésével számítják ki az egyes országok eredményeit. (Götz, 2014)

Az alábbi táblázat azt mutatja, hogy a digitális gazdaság fejlődésének üteme várhatóan azokban az országokban lesz a leggyorsabb, ahol a középiskolai oktatás által jól megalapozott ismeretekre építhetnek az egyetemi oktatók és a majdani munkavállalók. Az OECD 2012-es felmérése alapján készített PISA-jelentés matematikai eredményei bemutatják az egyes országoknak az OECD-átlagtól való eltérés irányát, amit a Tufts Egyetem professzorai által közzétett,

az általuk vizsgált országok digitális fejlődésének indexével vetettem össze. Egyértelműen megállapítható, hogy az egyes országok digitális fejlődési indexe szoros korrelációt mutat a 15 éves diákok matematika-ismereteinek szintjével. A „Bizonytalan fejlődésű" kategóriába sorolt országok diákjainak eredményei rendre az OECD-átlag alá esnek. Kivételt csak Lengyelország és Szlovénia jelent.

A PISA (2012) jelentésében közzétett matematikai sorrend és az OECD-átlagtól való eltérés iránya, valamint a Tufts Egyetem Fletcher Iskolájának kutatói által közzétett tanulmányban felsorolt országok a digitális kapacitásuk egyenetlen mértéke szerint:

PISA felmérés alapján sorrend matematikából (2012)			Kiemelkedő	Helybenjáró	Kitörésre alkalmas	Bizonytalan fejlődésű
			ország			
1	Sanghaj-Kína	↑			X	
2	Szingapúr	↑	X			
3	Hongkong-Kína	↑	X			
4	Tajvan	↑			X	
5	Korea	↑	X			
6	Makaó-Kína	↑				
7	Japán	↑		X		
8	Liechtenstein	↑				
9	Svájc	↑	X			
10	Hollandia	↑		X		
11	Észtország	↑	X			
12	Finnország	↑		X		
13	Kanada	↑		X		
14	Lengyelország	↑				X
15	Belgium	↑		X		
16	Németország	↑		X		
17	Vietnam	↑			X	
18	Ausztria	↑		X		
19	Ausztrália	↑		X		
20	Írország	↑	X			
21	Szlovénia	↑				X
22	Dánia	↑		X		

PISA felmérés alapján sorrend matematikából (2012)			Kiemelkedő	Helybenjáró	Kitörésre alkalmas	Bizonytalan fejlődésű
			ország			
23	Új-Zéland	↑	X			
24	Csehország	~		X		
25	Franciaország	~		X		
26	Egyesült Királyság	~		X		
27	Izland	~				
28	Lettország	~				
29	Luxemburg					
30	Norvégia	~		X		
31	Portugália	~				X
32	Olaszország	↓				X
33	°Spanyolország	↓		X		
34	°Oroszország	↓			X	
35	°Szlovákia	↓				**X**
36	°Egyesült Államok	↓	X			
37	°Litvánia	↓				
38	°Svédország	↓		X		
39	Magyarország	↓				X
40	°Horvátország	↓				
41	°Izrael	↓	X			
42	Görögország	↓				X
43	Szerbia	↓				
44	Törökország	↓			X	
45	Románia	↓				
46	Ciprus	↓				
47	Bulgária	↓				
48	Arab Emírségek	↓	X			
49	Kazahsztán	↓				
50	Thaiföld	↓			X	
51	Chile	↓			X	
52	Malajzia	↓			X	
53	Mexikó	↓			X	
54	Montenegró	↓				
55	Uruguay	↓				
56	Kosztarika	↓				
57	Albánia	↓				

PISA felmérés alapján sorrend matematikából (2012)			Kiemelkedő	Helybenjáró	Kitörésre alkalmas	Bizonytalan fejlődésű
			ország			
58	Brazília	↓			X	
59	Argentína	↓				
60	Tunézia	↓				
61	Jordánia	↓				
62	Kolumbia	↓			X	
63	Katar	↓				
64	Indonézia	↓			X	
65	Peru	↓				
	Fülöp-Szigetek				X	
	India				X	
	Dél-Afrika				X	
	Szaud-Arábia					X
	Egyiptom					X
	Kenya					X
	Nigéria					X

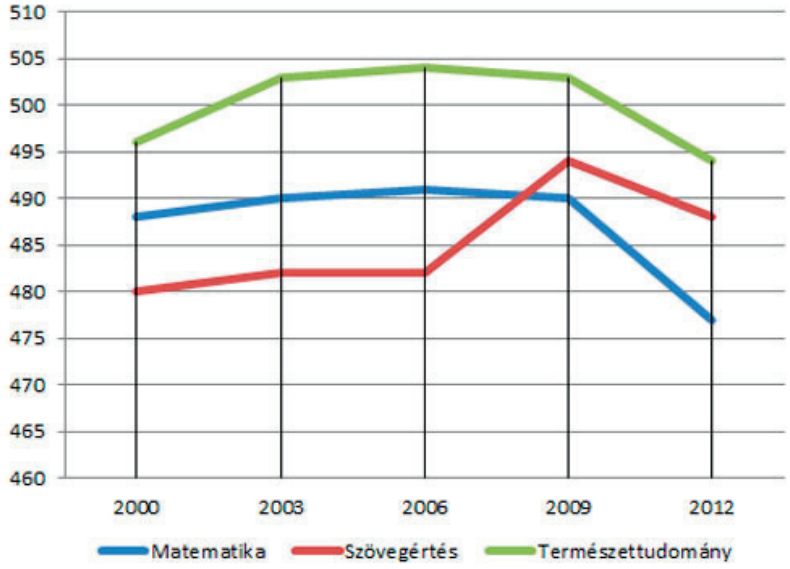
Forrás: oktatas.hu, továbbá hbr.org

Jelmagyarázat:
↑ Statisztikailag szignifikánsan magasabb az OECD-átlagnál.
~ Szignifikánsan nem különbözik az OECD-átlagtól.
↓ Statisztikailag szignifikánsan alacsonyabb az OECD-átlagnál.
° Szignifikánsan nem különbözik Magyarország eredményétől.

A 2012-es PISA-mérésen Lengyelország kiugróan jó eredményeket ért el, többször feltűnik lehetséges követendő példaként itthon és külföldön is. Az elmúlt másfél évtizedben szinte folyamatosan javuló lengyel eredményeket az 1999-es oktatási reformhoz lehet kötni, mely teljesen felforgatta az addig megszokott oktatási rendszert.

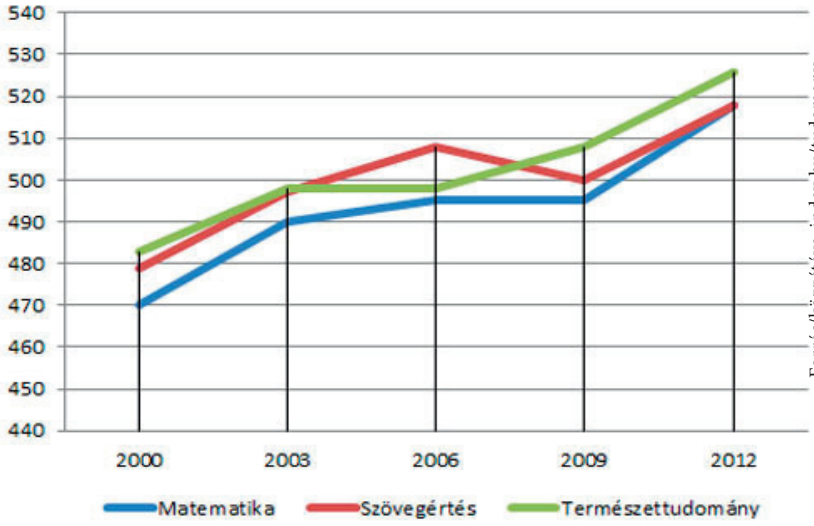
A lengyelek először a gyengébb képességű diákok körében tudtak fejlődést felmutatni, ennek legfőbb oka az új szisztéma és az egy évvel meghosszabbított általános képzés volt. A reform során fontos szerepet kapott az intézményi autonómia, a tanári munka megbecsülése és a kompetenciafejlesztésre alapozott alaptanterv is. (Velkey, 2015)

Magyarország PISA-eredményeinek alakulása



Forrás/közzétéve: index.hu/tudomany

Az ezredfordulón nagyszabású oktatási reformot végrehajtó Lengyelország PISA-eredményei



Forrás/közzétéve: index.hu/tudomany

11.3. A 2012-es PISA-felmérés

Az első PISA-felmérésen Magyarország a középmezőnyben helyezkedett el. A kutatás fő mérési területein a magyar tanulók később is rendre a nemzetközi átlag körül teljesítettek. Ezt a tulajdonképpeni stagnálást törte meg a 2012-es eredmények alapján tapasztalható drasztikus visszaesés, melynek során a diákok matematikából, szövegértésből és természettudományos ismeretekből sem érték el az OECD-országok átlagát. A 2012-es felmérés kiegészítő vizsgálata szerint a kreatív problémamegoldás is komoly kihívás elé állította a diákokat. E tekintetben a kutatásban részt vevő országok 44-es listáján hazánk a 33. helyet foglalja el, és ezzel a helyezéssel a régióban csak Bulgáriát és Montenegrót utasítja maga mögé. (Götz, 2014)

A 2012-es felmérésben 65 ország mintegy félmillió tanulója vett részt, köztük közel 4600 magyar diák. A főbb vizsgálati területek minden eredményét 2015 őszén hozták nyilvánosságra, részeredményeket azonban 2014-től már folyamatosan publikáltak. A kétezer oldalas jelentés sokkoló adatokat tartalmazott tanulóink teljesítményéről. Hazánk a korábbi, középmezőnyben elfoglalt pozíciójához képest a szövegértés és a természettudományok terén már csak a fejlett ipari országok egyharmadát tudta megelőzni, míg matematikából ennél is kevesebbet, csupán egyhatodukat. A gyengén teljesítő diákjaink aránya mindhárom területen nőtt, míg a legmagasabb szinten teljesítők aránya csökkent. Ez utóbbi matematikából már csak alig 2%, míg például Sanghajban ez az érték 30% felett van. A magyar diákoknak gyakran nehézkes volt az információk megtalálása, rossz helyekre kattintottak és sokáig tartott megtalálniuk a válaszokat. A szövegértésteszteken folyamatosan romlik a magyar diákok teljesítménye, egy 2014-es felmérés alapján már a diákok 20%-a tekinthető funkcionális analfabétának.

A magyaroknál már csak a brazil, az egyesült arab emirátusokbeli és a kolumbiai diákok teljesítettek rosszabbul. A digitális feladatokat a leggyorsabban az ausztrál, kanadai, francia és amerikai diákok oldották meg, azonban ők viszonylag gyakran hibáztak. A magyar diákokra kevésbé volt jellemző, hogy sokat vesződtek egyes nehezebb feladatokkal, és sokan voltak, akik bele sem kezdtek azokba. A teszt legnehezebb feladatát a szingapúri tanulók 70%-a oldotta meg helyesen. A magyar diákok között különösen sokan voltak, akik bele sem kezdtek a digitális feladatba. Az OECD-országok-

ban átlagosan 9% volt ezen tanulók aránya, míg Magyarországon 20%. (Götz, 2014)

„A PISA-felmérések alapján a magyar gyerekek harmada annyira rossz teljesítményt nyújtott, hogy ezzel gyakorlatilag kizárják magukat a munkaerőpiacról, mert nem rendelkeznek azokkal a minimális képességekkel sem, amelyek alkalmassá tennék őket bármilyen, a betanított segédmunkánál bonyolultabb feladat elvégzésére" – értékelte az adatokat Csapó. Különösen elszomorító a helyzet, ha az élbolytól való lemaradásunkat vizsgáljuk. Az első helyeket hosszú idő óta kibérlő ázsiai országok fényévekre vannak tőlünk, de az európai listavezetőktől számított távolságunk is egyre növekszik. (Csapó-Götz, 2014)

„Kimutatták, hogy ha egy évvel megnöveljük a teljes népesség iskolázottságát, az nagyjából 2%-ot ad hozzá a gazdasági növekedés üteméhez." (Götz, 2014) Ehhez azonban a középfokú oktatási rendszert szükséges megreformálni, mert az egyetemek egyre elégtelenebbnek tartják azt a tudást, amivel hallgatóik érkeznek. A múlt században Magyarország több Nobel-díjas tudóst adott a világnak. Legtöbbjüket olyan tanárok tanították, akik „nagy tanáregyéniségek voltak, imádtak tanítani, és rendkívül sikeresen motiválták a diákokat a tanulásra. Elkötelezett hivatástudatuk és tényszerű tudásuk volt, és a tudás tiszteletét és szeretetét is átadták diákjaiknak"– mondta Wigner Jenő. Aki vitázni akart, megtehette, sőt igényelték, hogy a diákok újszerű megoldásokat találjanak a problémákra. Az „elit" iskolák azonban az átlagnál jóval magasabb követelményeket is támasztottak, amit sok diák nem bírt, és máshová ment át tanulni. (Monsooninfo, 2016) A tanároktól tudományos tevékenységet is elvártak, így azok egyetemeken is oktattak, mégis középiskolás tanárok maradtak.

Ma azonban már nem ilyen a helyzet. Nahalka (2016) egy fontos tényezőre is felhívta a figyelmet: „Sajnos ki kell mondani, hogy a magyar pedagógustársadalom nagyobbik része nem a kor színvonalán teljesít. Ezért persze nem őket kell hibáztatni. A pedagóguspályán nagyon erős a kontraszelekció. A jelenlegi köznevelési informatikaoktatás céljaiban, mennyiségében, tartalmában és eszközeiben nem alkalmas a felsőfokú képzés által igényelt bemeneti tudásszint átadására, a képzési rendszer tartalma elavult. Az iskolában egyentananyagot kell tanítani. Ráadásul a nemrég lezajlott béremelés sem

tette sokkal kívánatosabbá a szakmát, ezért az utánpótlás is veszélybe került." (Götz, 2014)

11.4. Felsőoktatási helyzetkép

A rohamos léptékben haladó társadalmi-technológiai (és ezen belül az informatikai) forradalom hozta változásokat, fejlesztéseket eredményező alkalmazások kidolgozását, azok használatbavételét, továbbá a folyamatos vállalati üzemeltetést biztosító szakembergárda oktatásának legfőbb intézményei az egyetemek. Szalay professzor a világban akármerre tart előadást, mindenütt találkozik egy-egy magyar névvel. „Egyre több a magyar név az MIT-n (Massachusetts Institute of Technology, a világ legrangosabb egyeteme Cambridge-ben), ahol van egy fiatal magyar tudósgeneráció, akik már Amerikában vannak otthon." A professzor szerint „a magyar egyetemek egyre inkább lemaradnak a rangsorokban a jobb amerikaiakhoz képest. Egyre több gyerek jön rá, hogy ki lehet menni, és ha igazán jók, akkor nem kell évi 40 ezer dolláros tandíjat fizetni, hanem gyakorlatilag ingyen tanulhatnak. Nem lehet figyelmen kívül hagyni azt a tényt, hogy az egyetemi tanulmányokat a középiskolában nyert ismeretek alapozzák meg, egy-egy diák jövője szinte kivétel nélkül itt dől el. A tendencia ugyanis egyértelmű, a legtehetségesebb diákok már középiskolában külföldi egyetemre készülnek, és aki már kint jár egyetemre, jó eséllyel kint is marad."

A növekvő szakemberigényt az informatikai felsőoktatás kibocsátása nem követi. A felsőoktatási intézményekbe jelentkezők és felvettek száma csökken, amit az alábbi táblázat mutat be.

Felsőoktatási intézménybe jelentkezők és felvettek száma

Év	Jelentkezők		Informatika aránya	Felvettek		Informatika aránya
	Összesen	ebből: informatikára		Összesen	ebből: informatikára	
2016/P	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
2016/Á	111162	10363	9,3%	n.a.	n.a.	n.a.
2016/K	5457	563	10,3%	4404	353	8,0%
2016 össz.						
2015/P	8191	553	6,8%	5961	445	7,5%
2015/Á	105646	10104	9,6%	72260	5389	7,5%
2015/K	5877	494	8,4%	4676	316	6,8%
2015 össz.	***119714***	***11151***	**9,3%**	***82897***	***6150***	**7,4%**

Év	Jelentkezők		Informatika aránya	Felvettek		Informatika aránya
	Összesen	ebből: informatikára		Összesen	ebből: informatikára	
2014/P	9535	581	6,1%	7338	476	6,5%
2014/Á	106175	9627	9,1%	74182	5234	7,1%
2014/K	5736	578	10,1%	4512	390	8,6%
2014 össz.	***121446***	***10786***	***8,9%***	***86032***	***6100***	***7,1%***
2013/P	8139	450	5,5%	6190	356	5,8%
2013/Á	95447	8703	9,1%	72679	5022	6,9%
2013/K	5685	486	8,5%	4485	323	7,2%
2013 össz.	***109271***	***9639***	***8,8%***	***83354***	***5701***	***6,8%***
2012/P	9540	358	3,8%	7709	276	3,6%
2012/Á	110616	9865	8,9%	80136	5297	6,6%
2012/K	6418	522	8,1%	4630	369	8,0%
2012 össz.	***126574***	***10745***	***8,5%***	***92475***	***5942***	***6,4%***
2011/P	13294	409	3,1%	11602	320	2,8%
2011/Á	140954	11312	8,0%	98144	6170	6,3%
2011/K	7483	482	6,4%	6095	358	5,9%
2011 össz.	***161731***	***12203***	***7,5%***	***115841***	***6848***	***5,9%***
2010/P	13789	381	2,8%	11275	284	2,5%
2010/Á	140308	10412	7,4%	98246	5768	5,9%
2010/K	5936	375	6,3%	4585	256	5,6%
2010 össz.	***160033***	***11168***	***7,0%***	***114106***	***6308***	***5,5%***
2009/P	13885	414	3,0%	12393	359	2,9%
2009/Á	127306	10324	8,1%	94724	5589	5,9%
2009/K	2715	198	7,3%	2219	143	6,4%
2009 össz.	***143906***	***10936***	***7,6%***	***109336***	***6091***	***5,6%***
2008/P	14832	486	3,3%	13417	427	3,2%
2008/Á	96991	7741	8,0%	81108	4922	6,1%
2008/K	2073	85	4,1%	1805	80	4,4%
2008 össz.	***113896***	***8312***	***7,3%***	***96330***	***5429***	***5,6%***
2007/Á	108928	9577	8,8%	81637	5801	7,1%
2006/Á	132771	9587	7,2%	94142	6170	6,6%
2005/Á	150232	10675	7,1%	103364	6592	6,4%
2004/Á	167371	10827	6,5%	109851	6142	5,6%
2003/Á	160217	12206	7,6%	106376	7263	6,8%
2002/Á	164703	14889	9,0%	109470	8838	8,1%
2001/Á	148880	15347	10,3%	98031	8583	8,8%

Forrás: www.felvi.hu

Jelmagyarázat:

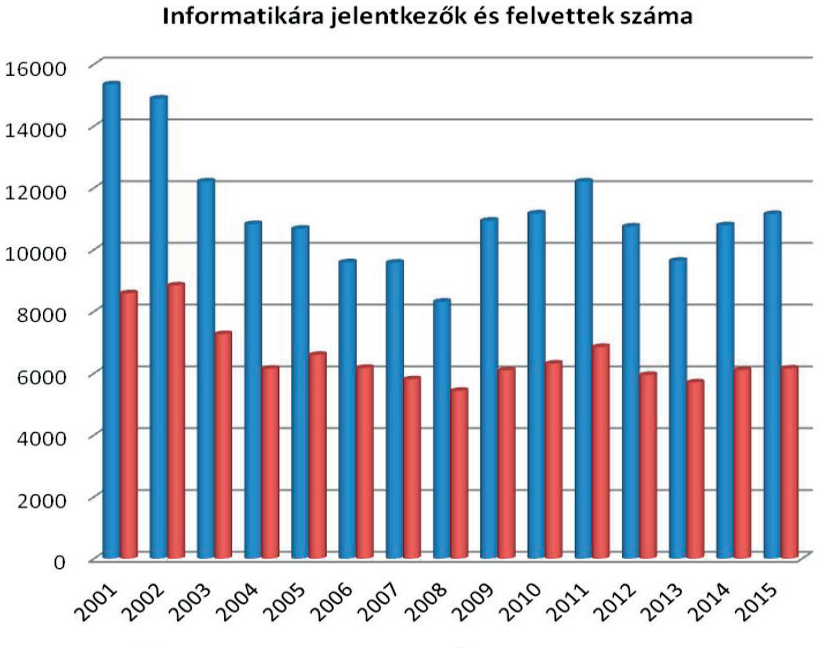
…év/K: …év februárjában induló képzések felvételi eljárása

…év/Á: …év szeptemberében induló képzések felvételi eljárása

…év/P: …év szeptemberében induló képzések felvételi eljárása (pótfelvételi)

A középiskolai diákok körében végzett felmérések azt jelzik, hogy az érettségi után átlagosan 10-20%-uk (az elit iskolákban pedig a diákok 30-50%-a)

gondolt arra, hogy külföldön végezné felsőfokú tanulmányait. A felsőoktatási intézmények informatikai tanulmányaira ezért is alacsony a túljelentkezés aránya, pedig az államilag támogatott hallgatói létszám relatíve magas. Nincs tehát valódi verseny a bekerülésért, alacsony pontszámmal is be lehet jutni felsőoktatási intézménybe, és ez már az oktatás nívóját gyengíti.



Forrás: felvi.hu

Az sem bátorítja a középiskolásokat, hogy az terjed az informatikus szakokról, hogy az első félévben az évfolyam felét rendre megbuktatják matematikából. Ez az informatikai pályaorientáció Horváth (2016) szerint abból az időszakból maradt meg, amikor egy informatikusnak a gép működésétől kezdve, a fizika és a matematika elméleti részletein keresztül a programokig mindenhez kellett értenie. És régen ez a buktatási arány lehet, hogy indokolt is volt, mivel korábban tényleg csak a legkiválóbb matekosok lehettek jó szakemberek, de mára már annyira leegyszerűsödtek az egyes részfeladatok, hogy nem kell mindenkinek a legjobbnak lennie minden területen.

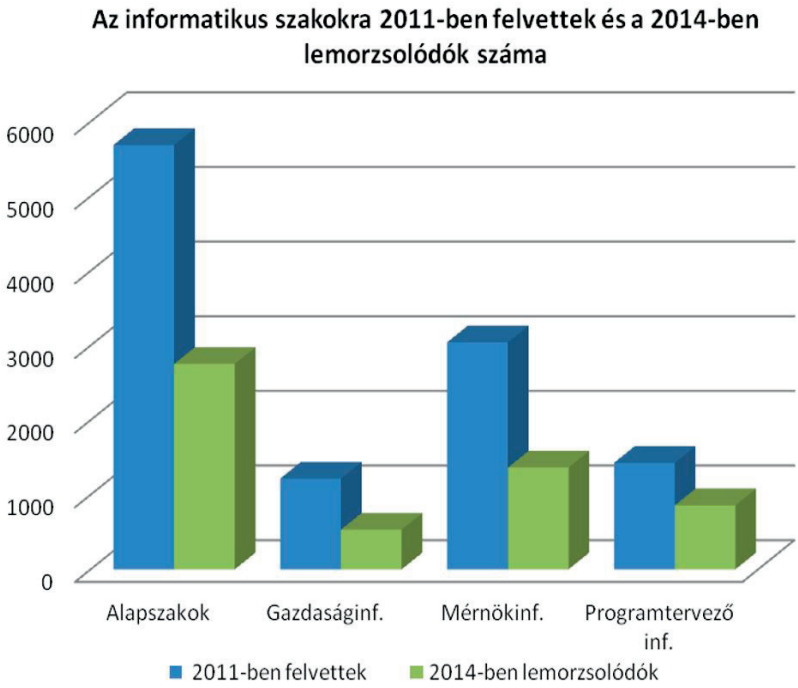
A felsőoktatás problémáinak, és főleg a munkaerőhiánynak az informatikai képességek átadása szempontjából iszonyatosan gyenge magyar közoktatásban vannak a gyökerei. Ennek az az oka, hogy amit a középiskolában ma informatikaként tanulnak, az még arra sem elég, hogy felkeltse a diákok érdeklődését az informatika iránt, nemhogy ahhoz, hogy felkészítse őket a felsőoktatásra.(Stubnya, 2016)

Bár a kormány relatíve magas létszámban határozta meg az államilag támogatott informatikus hallgatói létszámot, mégsem elégséges az évente kiadott diplomák száma. A felvett hallgatók már a képzés első két-három évében is olyan ajánlatokat kapnak különböző cégektől, hogy a magas jövedelem és az informatikai területen „biztos jövő" érdekében abbahagyják tanulmányaikat, ezért rendkívül magas arányú a lemorzsolódás. A lemorzsolódást az is elősegíti, hogy a mesterszakok nem nyújtanak annyival több előnyt, ami miatt megérné a többlet két év, továbbá az, hogy nagy az átfedés az alapszakok és a mesterszakok tananyaga között.

A BellResearch (2015) kutatása szerint a lemorzsolódás további oka, hogy a középiskolai oktatásban jellemzően a lexikális tudás megszerzése a cél, ami pedig elavult, ma már más készségekre van szükség. Az informatikai szakokon gondolkodásra és csapatmunkára is szükség van, ami teljesen más rendszerű és szellemű tanulást kíván meg. „Informatikai szakon 20 hazai felsőoktatási intézmény nyújt képzést az ország 13 városában, összesen mintegy 25000 főnek. Az informatikai képzési területen gazdaságinformatikus szakot indít a legtöbb intézmény (15). Mérnökinformatikus szakon tanul az informatikushallgatók mintegy fele (11500 fő 12 intézményben). A programtervező informatikus alapszak oktatása a leginkább koncentrált (9 intézmény). Az informatikai területtel rokon szakok képzésében is hangsúlyos az informatikaoktatás (legjelentősebb rokon szak a villamosmérnöki), így a végzettek a munkaerőpiacon el tudnak helyezkedni informatikai munkakörökben is.

2015-ben már 52% volt a felsőoktatásban a lemorzsolódás, nagyon sokan otthagyják a képzést. A hallgató sok esetben így is ugyanolyan jó állásokra pályázhat attól függetlenül, hogy kettő vagy négy év egyetem van a háta mögött. (BellResearch, 2015)

Horváth (2016) viszont inkább úgy látja, hogy a középfokú szakképzettséggel és az alapszakos diplomával rendelkezők körében a legnagyobb a hiány



Forrás: ivsz.hu/projektek, ivsz.hu/wp-content

a munkaerőpiacon. Szerinte nálunk a felsőoktatás mindenkit megpróbál felkészíteni a mesterszintre. Ezzel szemben úgy kéne funkcionálnia, mint egy tehetségkutató műhelynek.

2015 elején kormányzati szinten elfogadták a duális képzés rendszerét, melynek lényege, hogy az egyetemi hallgatók – miközben egyetemre járnak – tanulmányi munkaszerződés keretében egy szakmailag minősített vállalkozásnál fél évig gyakornokoskodnak. Amellett, hogy gyakorlatra tesznek szert, a hallgatók a vállalkozástól fizetést is kapnak. A hallgató számára így megnő a munkaidőalap. Ez az ára annak, hogy „élőben" ismerjék meg a vállalkozás működését. A munkavégzés jellemzően a vizsgaidőszakok alatt történik, mert az egyetemek ragaszkodnak a megszokott gyakorlatukhoz, és nem engedélyezik, hogy a szorgalmi időszak alatt a hallgatók a vállalkozásnál is teljesítsék kötelezettségüket. Arra azonban nincs garancia, hogy a mentorált hallgató a diplomaszerzés után is a vállalkozásnál marad, ott kamatoztatja

tudását. A vállalatok egyre inkább arra kényszerülnek, hogy maguk szervezzék meg alkalmazottaik képzését, illetve továbbképzését.

A felsőoktatásban arra is van lehetőség, hogy a hallgatók labortípusú képzésben vegyenek részt, ahol tanulmányaik részeként már korán bekapcsolódhatnak a valódi kutatási feladatok megoldásába, felkészülhetnek az élvonalbeli fejlesztői munkára és együtt dolgozhatnak tanáraikkal. Az ELTE vezetésével működik az Innovációs és Technológiai Intézet (EIT) Digital budapesti társult csomópontja, ahol az EIT Digital mesterképzésének keretében a hallgatók a képzés során felkészülhetnek a világpiacon folyó versenyre, továbbá húsz vezető európai egyetem kettős diplomáját és európai oklevelét is kézhez vehetik. A programban különös hangsúllyal szerepel az innovációs, kreatív, problémamegoldó készségek fejlesztése. Ezt az a nyelvtudás teszi lehetővé, ami ma már korosztályi sajátosság, mert a mai hallgatók többsége már úgy érkezik az egyetemre, hogy megfelelő nyelvtudással rendelkezik. (Horváth, 2016)

Bojár (2016) szerint az információtechnológia világában a tehetségekért folytatott verseny még annál is ádázabb, mint a vevőkért folytatott verseny. Az általa alapított intézetben ő azt tanítja, hogy milyen típusú üzleti tudásra van szüksége egy sikeres szoftvercégnél dolgozó informatikusnak. Tapasztalata szerint a hallgatók általában igen jó színvonalú technikai tudást szereznek az egyetemeken, Magyarországon is, de az üzleti világ értése és tisztelete hiányzik a műszaki-tudományos oktatásból. Ez okozza azt, hogy a kivételes műszaki eredményekből ritkán lesz üzleti siker. Intézetében arra tanítják meg a hallgatókat, hogy hogyan kell a vevő fejével gondolkodni. A világ legjobb egyetemei küldik hozzájuk egy-egy szemeszterre a diákjaikat, és az itt szerzett tudást beépítik saját tantervükbe. Az azonban nagyon sajnálatos, hogy kevés magyar diák jelentkezik a Budapesten tartott kurzusokra, pedig ők tandíjmentesen kapják azt, amiért az amerikaiak tizenötezer dollárt fizetnek félévente.

Az informatikusoknak „egy életen át" kell tudásukat karbantartani, fejleszteni. A speciális szakmai ismereteiket – a saját vállalatuk által szervezett továbbképzéseken túl – olyan képzőközpontokban is fejleszthetik, amit globális informatikai cégek szerveznek, mint pl. az Apple 2016-ban Olaszországban megnyitott Fejlesztői Képzőközpontja, az Oracle Egyetem, vagy a kilencezer magyar hallgatót képző Cisco Hálózati Akadémia.

Összegzésként megállapítható, hogy a negyedik ipari forradalom korát élve a kibertér társadalmi-technológiai hatása alapvetően változtatja meg életünket. Olyan technológiák születnek – számítási, illetve hibrid felhő, az adatelemzést támogató „Nagy Adat" (Big Data), a „dolgok internete" (IoT) –, amelyek embertársaink mindennapi életének színvonalát befolyásolják. Amennyiben befogadják és alkalmazzák azokat, életminőségük egyre inkább javulni fog, de ha – ismerethiányuk miatt – érzéketlenek maradnak a fejlődéssel szemben, akkor azoknak a társadalmi rétegeknek az életnívója hatványozottan lemarad.

A jövőben jelentős mértékben átalakul a vállalatok munkaerő-igénye. Új szakmák keletkeznek, míg mások eltűnnek. Az informatikusok iránti igény várhatóan jelentős mértékben megnövekszik, míg az irodai adminisztratív dolgozók körében számottevő leépítés következik be.

A minőségi informatikai tudást a felsőoktatási intézményekben szerte a világon általában 3 szintű képzés (alapszak, mesterszak, PhD képzés) keretében lehet megszerezni. A magyar egyetemekről azonban egyre magasabb létszámban morzsolódnak le a hallgatók, 2-3 éves tanulás után sokukat „elszívnak" a munkáltatók. A mesterszakok nem nyújtanak lényegesen több és tartalmában más ismeretanyagot az alapszakoknál. A doktori képzés befejezéséig csak azok a hallgatók jutnak el, akik valódi elhivatottságot éreznek az informatika-tudomány iránt, és a tudás fontosabb számukra, mint a minél korábbi életkorban megszerezhető magas jövedelem. Hazánk informatikus mérnökei közül már többen is világsikereket értek el úgy a tudományban, mint üzleti (vállalkozási) területen. Az egyetemek azonban csak azokra a tudás-alapokra építhetnek, amit a középfokú oktatás keretében szereznek meg a hallgatók. Az oktatási módszertan országonként változó és nem sztenderdizálható. Megállapítható, hogy az oktatás eredményessége a középiskolai tanárok és az egyetemi oktatók társadalmi és anyagi megbecsülésétől jelentős mértékben függ. Az amerikai és a finn gazdasági eredmények bizonyítják, hogy a társadalmi és gazdasági fejlődés üteme nem feltétlenül a teljesítménykényszeres oktatásszervezési módszerekkel függ össze. Sokkal inkább a kreativitás, a kritikus problémamegoldási képesség kifejlesztése a megoldás kulcsa.

A digitális gazdaság fejlődésének üteme jelentős mértékben függ a középiskolás diákok informatikaismereteinek szintjétől. A magyar diákok 2009-ig az OECD-országok között a középmezőnyben foglaltak helyet. A 2012-es fel-

mérés azonban már drasztikus visszaesést mutatott, a diákok sem matematikából, sem szövegértésből, sem természettudományos ismeretekből nem érték el az OECD-országok átlagát, ráadásul a kreatív problémamegoldás is komoly kihívás elé állította őket. A középiskolások, továbbá az egyetemi hallgatók digitális tudásának huszonegyedik századi szintre emelése hazánk egyik legfontosabb feladata, meg kell szüntetni a diákokra ma jellemző „digitális analfabétizmust". Csak így van esélyünk arra, hogy gazdaságunk és életszínvonalunk ne maradjon le véglegesen, mert aki lemarad, az kimarad.

Irodalomjegyzék

Elektronikus tartalmak

BALLA Zsolt (2015) Külföldre mennek a pályakezdők az ideális munkáért. Letöltve: http://www.uzletresz.hu/vallalkozas/20150420-kulfoldre-mennek-a-palyakezdok-az-idealis-munkaert.html (Utolsó letöltés: 26/06/2016)

BELLRESEARCH (2015) A hazai informatikus- és IT-mérnökképzés helyzetének, problémáinak, gátló tényezőinek vizsgálata. Letöltve: http://ivsz.hu/wp-content/uploads/2016/03/a-hazai-informatikus-es-it-mernokkepzes-helyzetenek-problemainak-gatlo-tenyezoinek-vizsgalata.pdf (Utolsó letöltés: 27/05/2016)

BERÁCS József – TEMESI József (2016) Új hullám az ázsiai csendes-óceáni felsőoktatási régióban. Letöltve: https://www.felvi.hu/pub_bin/dload/FeMu/2008_02/oldal67_70_beracs_temesi.pdf (Utolsó letöltés: 06/04/2016

BIZÓ Dániel (2006) Az üzleti ismeretek előnyt jelentenek az informatikusok számára. Letöltve: http://www.hwsw.hu/hirek/32467/cio-insight_top_trends_2007_informatikus_kriterium_elony_uzleti_ismeret.html (Utolsó letöltés: 25/03/2016)

BUDAPESTI ICT NETWORK (2016) Rólunk mondták. Letöltve: http://budapestictnetwork.elte.hu/rolunk-mondtak/ (Utolsó letöltés: 25/03/2016)

CHAKRAVORTI, Bhaskar; TUNNARD, Christopher; CHATURVEDI, Ravi Shankar (2015) Where the Digital Economy Is Moving the Fastest. Letöltve: https://hbr.org/2015/02/where-the-digital-economy-is-moving-the-fastest#b03g06t20w15 (Utolsó letöltés: 25/03/2016)

CHARLOTTE (2015) A finn oktatási rendszer sikerének titka. Letöltve: http://www.kulfoldremennek.hu/tanulas/224-a-finn-oktatasi-rendszer-sikerenek-titka (Utolsó letöltés: 26/03/2016)

COMPUTERWORLD (2016). A dolgok biztonsága. Letöltve: http://computerworld.hu/computerworld/a-dolgok-biztonsaga.html (Utolsó letöltés: 25/03/2016)

COMPUTERWORLD (2016) Világelső lehet Európa az adatközpontú gazdaság területén. Letöltve: http://computerworld.hu/computerworld/vilagelso-lehet-europa-az-adatkozpontu-gazdasag-teruleten.html (Utolsó letöltés: 27/04/2016)

COURSERA (2016) Take the world's best courses, online. Unlock Value in Massive Datasets. Learn fundamental big data methods in six straightforward courses. Letöltve: https://www.coursera.org/specializations/big-data (Utolsó letöltés: 25/03/2016)

CSÁNYI Klaudia (2016) Itt a hiányszakmák toplistája: ezekben bárki könnyedén találhat állást. Letöltve: http://faktor.hu/faktor-ezek-a-hianyszakmak-magyarorszagon (Utolsó letöltés: 14/06/2016)

DATAMINER (2014) Real-time adatelemzés Twitterből. Letöltve: http://adattudomany.blog.hu/2014/06/11/real-time_adatelemzes_twitterbol (Utolsó letöltés: 25/03/2016)

DIGITALHUNGARY (2015) Mi is az az IoT? Letöltve: http://www.digitalhungary.hu/e-volution/Mi-is-az-az-IoT/2202/ is nagyon jó: mi is az az IoT? (Utolsó letöltés: 26/03/2016)

EDUCATIO NONPROFIT KFT./VEROSZTA Zsuzsanna (2015) Frissdiplomások 2014, Kutatási zárótanulmány. Letöltve: https://www.felvi.hu/pub_bin/dload/DPR_tanulmanyok/ frissdiplomasok_2014_zarotanulmany.pdf (Utolsó letöltés: 25/06/2016)

EDULINE (2016) A világhírű MIT minden tudományos tananyagát ingyen elérhetővé tette. Letöltve: http://eduline.hu/felsooktatas/2016/6/18/A_vilaghiru_MIT_minden_ tudomanyos_tananyaga_FXO106 (Utolsó letöltés: 26/06/2016)

EDULINE (2009) Középiskola külföldön: így néz ki egy tanév az USA-ban. Letöltve: http://eduline.hu/felsooktatas/2009/9/4/20090902_kozepiskola_kulfoldon_usa (Utolsó Letöltés: 26/04/2016)

ELŐD Fruzsina (2016) Teljesen felbolydul a munka világa a következő évtizedben (a World Economic Forum kutatása alapján). Letöltve: http://index.hu/gazdasag/2016/03/18/a_jovo_munkaja/ (Utolsó letöltés: 29/03/2016)

FIGYELŐ (2012) Ez a titka a leggyorsabban fejlődő országoknak. Letöltve: http://figyelo.hu/cikk_print.php?cid=381617_ez_a_titka_a_leggyorsabban_fejlodo_orszagoknak (Utolsó letöltés: 30/05/2016)

GÖTZ Attila – NAHALKA István – CSAPÓ Benő (2014) Csapnivaló a magyar PISA-bizonyítvány. Letöltve: http://index.hu/tudomany/2014/04/23/csapnivalo_a_magyar_pisa-bizonyitvany/ (Utolsó letöltés: 25/03/2016)

HORVÁTH Bence (2016) Minden tudományos dolgozat egy rendszerbe kerülhet 2020-tól az EU-ban. Letöltve: http://eduline.hu/felsooktatas/2016/5/31/Minden_tudomanyos_dolgozat_egy_rendszerbe_k_6A0LSG (Utolsó letöltés: 26/06/2016) ÉS http://444.hu/2016/05/27/minden-eu-ban-keszult-tudomanyos-publikacio-szabadon-hozzaferheto-lehet-2020-tol

HORVÁTH Zoltán (2016) Programtervező informatikus képzés az ELTE-n. Letöltve: http://computerworld.hu/computerworld/programtervezo-informatikus-kepzes-az-elte-n.html?hirlev (Utolsó letöltés: 25/03/2016)

KIS Endre – SEPP Norbert (2016) A kognitív vállalatok kora. Letöltve: http://computerworld.hu/computerworld/a-kognitiv-vallalatok-kora.html (Utolsó letöltés: 25/03/2016

KOPÁTSY Sándor (2013) A dél-koreai iskolarendszer. Letöltve: http://kopatsys-andorgondolatai.blogspot.hu/2013/01/a-del-koreai-iskolarendszer.html (Utolsó letöltés: 30/05/2016)

KÖZPONTI STATISZTIKAI HIVATAL (2014) „Helyzetkép a magyarországi elvándorlásról". Letöltve: http://www.ksh.hu/docs/szolgaltatasok/sajtoszoba/seemig_sajto_reszletes.pdf (Utolsó letöltés: 17/05/2016)

LAKY Zoltán (2016) A mutató, amiben a britekkel együtt mi állunk Európa élén. Letöltve: http://valasz.hu/kultura/a-mutato-amiben-a-britekkel-egyutt-mi-allunk-europa-elen-117694 (Utolsó letöltés: 25/03/2016)

LAUFER Tamás (2015) A digitális gazdaság alapja az informatika. Letöltve: http://ivsz.hu/hirek/laufer-tamas-a-digitalis-gazdasag-alapja-az-informatika (Utolsó letöltés: 25/03/2016)

LAZA Bálint – LANNERT Judit (2015) Nyugi, a gyereke biztosan digitális analfabéta lesz. Letöltve: http://index.hu/tech/2015/06/24/digitalis_tanterv_digitalis_keszsegek_ ivsz_magyarorszag/ (Utolsó letöltés: 25/03/2016)

LONDON AID SPECIALIST LTD. (2015) Angol oktatási rendszer. Letöltve: http://londonspecialista.hu/hu/hasznos-infok/angol-oktatasi-rendszer (Utolsó letöltés: 27/05/2016)

M2M ZÓNA (2014) Big Data: felfoghatatlan, hogy mennyi adat létezik. Letöltve: http://m2mzona.hu/mi-az-m2m/big-data-felfoghatatlan-hogy-mennyi-adat-letezik (Utolsó letöltés: 25/03/2016)

MALLÁSZ Judit (2016) Fontos a vállalat együttműködése a felsőoktatással. Letöltve: http://computerworld.hu/computerworld/fontos-a-vallalat-egyuttmukodese-a-felsooktatassal.html (Utolsó letöltés: 25/03/2016)

MALLÁSZ Judit (2016) Mérnökképzés mesterfokon. Letöltve: http://computerworld.hu/computerworld/mernokkepzes-mesterfokon.html (Utolsó letöltés: 25/03/2016)

MCPHERSON, David (2016) Big Data and the Internet of Things. Letöltve: http://blog.edx.org/big-data-and-the-internet-of-things?track=blog (Utolsó letöltés: 25/03/2016)

MESTER Sándor (2016) Karrier az informatikus diplomán innen (a Targetjobs felmérése alapján). Letöltve: http://computerworld.hu/computerworld/karrier-az-informatikus-diploman-innen.html?hirlev ÉS https://targetjobs.co.uk/career-sectors/it-and-technology/286189-ten-typical-jobs-graduates-can-do-in-it (Utolsó letöltés: 23/03/2016)

MÉSZÁROS Csaba (2016) A munkaerőpiac jövője (a Világgazdasági Fórum TheFuture of Jobs című 2016. évi jelentése alapján). Letöltve: http://computerworld.hu/computerworld/a-munkaeropiac-jovoje.html?hirlev és www3.weforum.org/docs/Media/WEF_Future-of-Jobs_embargoed.pdf (Utolsó letöltés: 14/06/2016)

MÉSZÁROS Csaba (2016) Az informatika napjainkban (a Salesforce Research 2016. évi kutatási jelentése alapján). Letöltve: http://computerworld.hu/computerworld/az-informatika-napjainkban.html (Utolsó letöltés: 17/06/2016)

MÉSZÁROS Csaba (2016) Ezek a legkeresettebb informatikus szaktudások (a CompTIA IT-iparági szervezet összeállítása alapján). Letöltve: http://computerworld.hu/computerworld/ezek-a-legkeresettebb-informatikus-szaktudasok.html?hirlev ÉS https://www.comptia.org/resources/common-it-employability-skills (Utolsó letöltés: 25/06/2016)

MÉSZÁROS Csaba (2015) Hatalmas informatikushiány várható Európában. Letöltve: http://computerworld.hu/cio/hatalmas-informatikushiany-varhato-europaban.html (Utolsó letöltés: 25/03/2016)

MÉSZÁROS Csaba (2016) Így változtatják meg az alkalmazottak a munkahelyeket (az OpenText tanulmánya alapján). Letöltve: http://computerworld.hu/computerworld/igy-valtoztatjak-meg-az-alkalmazottak-a-munkahelyeket.html?hirlev (Utolsó letöltés: 01/04/2016)

MÉSZÁROS Csaba (2016) Ingyenes online informatikai kurzusok. Letöltve: http://computerworld.hu/computerworld/ingyenes-online-informatikai-kurzusok.html (Utolsó letöltés: 25/03/2016)

MÉSZÁROS Csaba (2016) Ipar 4.0: így modernizálódnak a vállalatok (a PricewaterhouseCoopers, (PwC) globális felmérése alapján). Letöltve: http://computerworld.hu/computerworld/ipar-4.0-igy-modernizalodnak-a-vallalatok.html ÉS https://www.pwc.com/gx/en/metals/pdf/industry-4.0-metals-key-findings.pdf (Utolsó letöltés: 06/06/2016)

MOLNÁR Csaba (2016) Nincsenek politikai ambícióim. Letöltve: http://mno.hu/nagyinterju_magazinban/bojar-gabor-nincsenek-politikai-ambicioim-1336632 (Utolsó letöltés: 27/05/2016)

MONSOONINFO (2016) A 20. századi világszínvonalú oktatásunk titka. Letöltve: http://monsooninfo.blog.hu/2016/05/28/a_20_szazadi_vilagszinvonalu_oktatasunk_titka (Utolsó letöltés: 28/05/2016)

NEMZETI HÍRKÖZLÉSI ÉS INFORMATIKAI TANÁCS (2015) Versenyképes oktatás, versenyképes munkaerőpiac (2015). Letöltve: http://nhit.hu/dokumentum/80/_Oktatasinformatika_NHIT_0723.pdf (Utolsó letöltés: 26/03/2016)

NETIQ NOVELL SUSE MAGYARORSZÁGI KÉPVISELET (2016) OpenStack: kulcs a felhőhöz. Letöltve: http://ceginfo.computerworld.hu/netiq-novell-suse-magyarorszagi-kepviselet/openstack-kulcs-a-felhohoz.html?hirlev (Utolsó letöltés: 25/06/2016)

SCHOPP Attila – STRAUSZ György (2016) Informatikai székfoglaló. Letöltve: http://www.itbusiness.hu/Fooldal/hirek/Technology/Informatikai_szekfoglalo.html (Utolsó letöltés: 17/05/2016)

STAISZTIKAI TÜKÖR (2015) Munkaerő-piaci helyzetkép, 2014. Letöltve: https://www.ksh.hu/docs/hun/xftp/stattukor/munkaeropiac14.pdf (Utolsó letöltés: 17/05/2016)

STING (2016) Egyre kevesebb programozóra lesz szükség a következő években (a US Bureau of Labor Statistics (BLS) alapján). Letöltve: http://prog.hu/hirek/4149/egyre-kevesebb-programozora-lesz-szukseg-a-kovetkezo-evekben ÉS http://www.i-programmer.info/news/99-professional/9303-programming-jobs-to-decline.html (Utolsó letöltés: 25/03/2016)

STUBNYA Bence (2016) Nem tüntetnek érte, de a jövő múlik rajta. Letöltve: http://index.hu/gazdasag/2016/03/04/informatikushiany_munkaeropiac_oktatas_informatika/ (Utolsó letöltés: 25/03/2016)

SZALAY Sándor (2016) A tudomány most válik nagykorúvá, manufaktúrából az ipari forradalom korába lép. Letöltve: http://tldr.444.hu/2016/01/06/szalay-sandor-a-tudomany-most-valik-nagykoruva-manufakturabol-az-ipari-forradalom-koraba-lep (Utolsó letöltés: 25/03/2016)

TÓTH Balázs (2015) Havonta 5,5 milliárd forintot elbukunk. Letöltve: http://index.hu/tech/2015/12/28/havonta_5_5_milliard_forintot_elbukunk/ (Utolsó letöltés: 25/03/2016)

VARGA G. Gábor – WILLIN-TÓTH Kornélia – FREMDA Balázs (2016) Szakembervadászatra ítélve. Letöltve: http://nol.hu/gazdasag/szakembervadaszatra-itelve-1602479 (Utolsó letöltés: 26/06/2016)

VÁMOS Tibor (2016) SYSBOOK Rendszerekről mindenkinek, egyetemi hallgatóknak és a rendszertanulmányok művelőinek, sokfelületű e-könyv. Letöltve: http://sysbook.sztaki.hu/, (Utolsó letöltés: 14/06/2016)

VELKEY Kristóf (2015) A lengyel oktatási reform a PISA vizsgálatok tükrében. Letöltve: http://www.iskolakultura.hu/ikultura-folyoirat/documents/2015/04/07.pdf (Utolsó letöltés:27/05/2016)

VOITH Hunor (2016) Digitalizálná az ipart az Európai Bizottság. Letöltve: http://www.hwsw.hu/hirek/55489/eu-eb-digitalis-ipar-europai-tudomanyos-felho.html (Utolsó letöltés: 27/04/2016)

VÖRÖS Gábor (2014) Oktatás és kutatás a „sikerországokban". Letöltve: http://mandiner.hu/cikk/20141121_voros_gabor_oktatas_es_kutatas_a_sikerorszagokban (Utolsó letöltés: 30/06/2016)

WIKIPEDIA (2011) Internet. Letöltve: https://hu.wikipedia.org/wiki/Internet (Utolsó letöltés: 04/04/2016)

Folyóiratcikkek

TÖLGYES László (2016) A nők jobb kódot írnak, mint a férfiak?
ITBehaviour XIV. évfolyam, 10. szám 2016. május 17. 32-35. oldal ISSN 1589-3464

SCHOPP Attila (2016) A CIO-k feje a szerepük változása miatt fáj leginkább
IT Business XIV. évfolyam 5. szám 2016. március 1. 44-46. oldal ISSN 1589-3464

CSEKE Hajnalka: A szingapúri csoda; Írástudatlanokból világelsők
Figyelő 2016/21. szám, 2016. május 26. 34-36. oldal ISSN 0015-086X

Berki Gábor
(berkigabor@uni-nke.hu)

Kiberháborúk, kiberkonfliktusok

Lektorálta: Dr. Botz László PhD.

Absztrakt

Az utóbbi néhány évben egyre több hírt hallunk számítógéphálózati támadásokról. A célpontok között szerepelnek nemzetközi nagyvállalatok, kormányzati szervek, pénzügyi vállalatok és kritikus infrastruktúrák is. Az ártó szándékú támadók, kihasználva a sebezhetőségeket, a saját – legyen az ideológiai, vallási, pénzszerzési vagy akár katonai – céljaik elérése érdekében korlátozni, bénítani igyekeznek az információs társadalom részegységeinek működését. Jelen tanulmány célja, hogy bemutassa, milyen konfliktusok voltak az elmúlt időben a kibertérben, milyen fenyegetésekre kell számítani a kibertérből, és hogy milyen kiberhadviselési potenciállal rendelkeznek a világ vezető hatalmai.

Kulcsszavak: kibertér, kiberbűnözés, kiberhadviselés, kiberháború

Abstract

In recent years there have been growing reports of attacks on computer network. Targets include international corporations, government agencies, financial firms and critical infrastuctures. Through the exploitation of this vulnerability attackers directed by malice intend to restrain and paralyze components of information society in order to achieve their personal – either ideological, religious, financial or military – goals. The author would like to examine, what kind of conflicts were the last time in cyberspace, what kind of threats shall be counted in it and what extent cyber warfare potential of the world leaders have.

Keywords: cyberspace, cybercrime, cyber warfare, cyberwar

1. Bevezetés

Napjainkra az információtechnológia olyan mélyen átszőtte a társadalmakat, hogy számítógépek nélkül elképzelhetetlenné vált nemcsak az ipari, a pénzügyi vagy a kormányzati munka, hanem a polgárok mindennapi élete is. Ezt bizonyítja az az adat is, mely szerint 2015 novemberében a Föld lakosságának 46,4%-a, több, mint 3,3 milliárd ember használt internetet. (Internet World Stats, 2015) Bátran kijelenthetjük, hogy a modern kori ember komoly függőségbe került az informatikai rendszerekkel. A mindennapokat megkönnyítő informatikai eszközök és szolgáltatások azonban komoly biztonsági kockázatokat is rejtenek. Egyre-másra jelennek meg azok a hírek, melyek különböző kibertámadásokról, kiberbűnözésről és kiberhadviselésről szólnak. Ahhoz, hogy megérthessük, hogy milyen fenyegetések érhetik a kibertérből eszközeinket és adatainkat, meg kell ismerkednünk néhány alapvető fogalommal.

2. A kibertér fogalma

Első és legfontosabb, hogy tisztázzuk a kibertér mibenlétét. Magát a fogalmat William Gibson tudományos-fantasztikus szerző alkotta meg 1984-es *Neurománc* című regényében. Úgy írta le, mint egy számítógép-hálózatok által teremtett világot, tele mesterséges intelligens lényekkel és felhasználók milliárdjaival. A Enciklopédia Britannica megfogalmazása szerint *„a kibertér egy alaktalan, vélhetően „virtuális" világ, amely számítógépek, internetképes eszközök, szerverek, routerek és az internet-infrastruktúra egyéb elemeinek összekapcsolása révén jön létre."* (Bussell, 1995) Hétköznapi megfogalmazásban számítógépek, számítógép-hálózatok, az ezeket összekötő kommunikációs csatornák, az itt futó alkalmazások és az itt tárolt adatok alkotta virtuális világ összefoglaló neveként hivatkozhatunk rá. Nagyon sok kutató, szervezet próbálta már meghatározni a kiberteret, ennek megfelelően nagyon sok definíció is született rá. Az Egyesült Államok Védelmi Minisztériuma által kiadott és 2016 februárjában pontosított katonai terminológiai szótárban meghatározottak szerint a kibertér *„az információs környezet egy globális tartománya, amely tartalmazza az informatikai infrastruktúrák, a bennük tárolt adatok*

egymással összefüggő hálózatát, beleértve az internetet, a távközlési hálózatokat, a számítógép rendszereket, valamint a beágyazott feldolgozó és vezérlő elemeket". (JP 1-02, 2016)

Hazánkban a kibertér hivatalos megfogalmazására a 2013-ban megjelent, a Magyarország Nemzeti Kiberbiztonsági Stratégiája nevet viselő 1139/2013. számú kormányhatározatban került sor. Eszerint „a *kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.*"

A fenti meghatározásokból leszűrhető, hogy a kibertér az összekapcsolt elektronikus információs rendszerek és hálózatok összessége. Így a hálózatba nem kötött, önálló számítógépek nem részei a kibertérnek. Ha az összekapcsolás módját tekintjük, amely nemcsak vezetékes lehet, hanem vezeték nélküli is, a kibertér részének kell tekintenünk az elektromágneses spektrumot is, amelyen keresztül a kommunikáció történik. A vezeték nélküli kommunikáció legközismertebb formája a Wi-Fi, amely már szinte mindenhol elérhető, de ide kell sorolnunk a mobilhálózatokon keresztül igénybe vehető adatforgalmat is.

3. A kibertérből érkező fenyegetések

A következőkben vizsgáljuk meg, hogy milyen fenyegetések érkezhetnek a kibertérből. Alapvetően a támadások az informatikai rendszereken tárolt és kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, illetve a rendszerelemek rendelkezésre állása és funkcionalitása ellen irányulhatnak. Az adatok bizalmasságán azt értjük, hogy azt csak az arra jogosultak és csak a jogosultsági szintjüknek megfelelő mértékben ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról. A sértetlenség az

adat azon tulajdonsága, mely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyezik, nem történt benne illetéktelen változtatás. Ebbe beleértjük a hitelességét is, hogy a megfelelő forrásból származik-e. A rendelkezésre állás arra vonatkozik, hogy az adatot az arra jogosultak a szükséges helyen és időben elérhessék, használhassák. A rendszerelemek rendelkezésre állása pedig a rendeltetésszerű használat lehetőségét jelentik. (Muha, Krasznay, 2014 p10)

Ha megvizsgáljuk a támadások indítékait, csoportosíthatjuk a támadók körét, akiknek a szándékai, rendelkezésre álló erőforrásai és szaktudásuk eltérő lehet. A szakirodalmakban a fenyegetések többféle csoportosításával is találkozhatunk, de úgy gondolom, hogy jelen tanulmányban az általam legfontosabbnak tartott fenyegetéseket vizsgálom meg. Véleményem szerint ezek a

- kiberbűnözés,
- kiberkémkedés,
- hactivizmus,
- kiberterrorizmus,
- kiberhadviselés.

3.1. A kiberbűnözés

A kiberbűnözés tulajdonképpen számítógépek és számítógépes rendszerek segítségével, vagy számítógépek és hálózatok kárára elkövetett bűncselekmények gyűjtőfogalma. Motivációjáról az esetek többségében bátran kijelenthetjük, hogy az az anyagi haszonszerzés.

2001. november 23-án Budapesten 30 ország írta alá a Számítástechnikai Bűnözés Elleni Egyezményt, melyben részletesen leírták az ilyen típusú bűncselekményeket, az államok jogharmonizációjához szükséges lépéseket és az együttműködés kereteit. Három fő részre osztották a számítógépes bűncselekményeket.

1. *A számítástechnikai rendszer és a számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények*
   Idetartozik például a jogtalan belépés, az adatok vagy rendszerek sértetlensége elleni cselekmények vagy az eszközökkel történő visszaélés.
2. *Számítástechnikai bűncselekmények*
   Ez alatt a számítógépes hamisítás és a csalás fogalmának kifejtésére került sor.

3. *A számítástechnikai adatok tartalmával kapcsolatos bűncselekmények*
   Ez a passzus a gyermekpornográfiával szembeni eredményesebb fellépést lehetővé tévő intézkedéseket tartalmazza. (Számítástechnikai Bűnözés Elleni Egyezmény, 2001)

A szükséges intézkedéseket már minden ország megtette és beiktatta jogrendszerébe a megfelelő paragrafusokat, így könnyebbé vált a fellépés ezekkel a bűncselekményekkel szemben. A sikeres harc azonban így sem egyszerű, hisz ezen bűncselekmények jellemzői közé tartozik a gyorsaság és a nemzetköziség, amely nagyon megnehezíti a felderítést. Ahogy az internetpenetráció növekszik a világban, úgy nő a kiberbűncselekmények száma és az általa okozott anyagi kár is. A Norton Cybercrime Report már 2012-ben 114 milliárd dollárra becsülte a bűnözők okozta kárt, a járulékos költségeket (termeléskiesés, helyreállítás költségei), pedig 274 milliárd dollárra, amely így együtt már meghaladta a kábítószerek illegális forgalmából keletkezett 288 milliárd dollárt. (Norton, 2012) Nem csoda, hogy napjainkra már a szervezett bűnözés is jelen van a számítógépes bűncselekmények elkövetői között. Kis kockázattal nagy hasznot tudnak realizálni.

Népszerű elkövetési módszer az adathalászat, amellyel különféle személyes adatokat, bankszámla-, bankkártyaadatokat szereznek meg és ezekkel élnek vissza. Nagyon kezd elterjedni a különféle titkosítást végző rosszindulatú programok terjesztése, amelyek a fertőzött gépen tárolt anyagokat titkosítják és csak a kért váltságdíj kifizetése után kapják meg a felhasználók a feloldáshoz szükséges kódot. Idén februárban jelent meg a Locky elnevezésű ransomware[1], amely makrók segítségével fertőzte meg a számítógépeket. A csalók kéretlen elektronikus levelekbe Word dokumentumokat helyeztek el. Amikor ezt a felhasználó megnyitotta, akkor az elé táruló dokumentum csak értelmezhetetlen karaktersorozatokat tartalmazott. Egy üzenetben arra kérték, hogy engedélyezze a makrókat a fájl tartalmának megtekintéséhez. Ha ezt is megtette, akkor rögtön megfertőződött a számítógépe és elkezdődött a rombolás. A károkozó dokumentumokat, fotókat, videókat tesz használhatatlanná. Mindössze azokat a könyvtárakat hagyja érintetlenül, amelyek a Windows

1 Olyan rosszindulatú számítógépes program, amely valamilyen fenyegetéssel próbál pénzt kicsikarni a felhasználóból.

működéséhez feltétlenül szükségesek. Ez után üzenetben közli a váltságdíj összegét és a fizetési módot. Sok esetben a kért összeg átutalása után sem küldik el a titkosítás feloldására szolgáló kódot. A zsarolás másik formája, amikor vállalatokat, webáruházakat fenyegetnek meg, hogy amennyiben nem fizetnek, elérhetetlenné teszik az oldalaikat.

A kiberbűnözés elleni harc egyik fő fegyvere lehet a felhasználói tudatosság növelése, nem lehet eleget beszélni a körültekintő internethasználatról, hisz a megkárosított felhasználók jelentős része saját internetes tevékenysége folytán kerül a bűnözők csapdájába.

3.2. A kiberkémkedés

Azt tartják, hogy a kémkedés az egyik legősibb mesterség a földön. Nemcsak katonai titkok megszerzése jelent előnyt az ellenséggel szemben, hanem az ipari, pénzügyi, diplomáciai információk is az esetleges vetélytársakkal szemben. Az informatikai eszközök térnyerése és az internet elterjedése kifejezetten hasznos volt a kémek számára, hiszen egy jó felkészült támadó képes akár a világ másik végén lévő informatikai rendszerbe is behatolni és onnan adatokat letölteni. Az Egyesült Államok kiberbiztonsággal foglalkozó hatóságai 2002-től észleltek olyan informatikai behatolás sorozatokat, amelyek a katonai, a kormányzati és a vállalati szektor informatikai hálózatait érintette. A vizsgálatok szerint Kínához köthető hackerek hosszú időn keresztül precízen megtervezett és kivitelezett támadásokon keresztül 10-20 terrabájtnyi anyagot töltöttek le a megtámadott rendszerekről. Összehasonlításképpen, az amerikai Kongresszusi Könyvtár, amely a legnagyobb a világon, összes könyve kb. 10 terrabájt adatot tárol. Az akcióban, amely a Titan Rain nevet kapta, érintett volt a NASA, a Lockheed Martin és a Pentagon is. (Kovács, 2009)

2012 augusztusában tűnt fel egy új, kémkedésre kifejlesztett rosszindulatú program. A Gauss névre keresztelt vírus elsősorban banki és egyéb hozzáférési adatokat gyűjtött a fertőzött rendszerből, majd továbbította azokat a C&C[2] szerverek felé. Egy biztonsági cég szerint a Gauss elsősorban Libanonban, Izraelben és a Palesztin területeken volt aktív, de az Egyesült Államokból is jelentettek fertőzést. (CERT, 2012)

2 Command and Control – Irányító és vezérlő szerver

2013 januárjában a Kaspersky jelentette be, hogy leleplezett egy nagyarányú online kémkedési akciót. A vírusirtó cég által *Vörös októbe*rnek nevezett kártékony kód már 2007 óta volt aktív, főképp Kelet-Európában, a volt szovjet tagköztársaságokban, illetve Kelet-Ázsiában, de találtak fertőzött gépeket szerte a világon kormányszervezetekben, nagykövetségeken, kutatóközpontokban is. A vírus fő célja titkos dokumentumok megszerzése volt, de ezen kívül információkat gyűjtött a megfertőzött hálózatokról is. Ez a vírus is, akárcsak az előzőekben ismertetett kártevők, igen kifinomult volt és több, eddig ismeretlen metódust alkalmazott működése során. A terjedéséhez viszont régi, bevált módszereket, adathalász e-maileket, fertőzött weboldalakat, a Word- és Excel-sérülékenységeket használt. A program moduláris felépítésű, több mint ezer modult fejtettek vissza. Az egyik érdekes modul például a fertőzött számítógépre csatlakoztatott okostelefonokról, illetve a gépre dugott pendrive-okról le tudta menteni az érdekesnek tűnő tartalmat, még a törölt fájlokat is vissza tudta állítani ezekről. A forráskód, illetve az ahhoz fűzött megjegyzések orosz programozók munkájára engedtek következtetni. Persze az is elképzelhető, hogy ez csak az álcázás része volt és az orosz, illetve a programozói szlengben elterjedt kifejezésekkel csak félrevezetésből szórták meg az angol nyelvű megjegyzéseket a programsorok mellett. (Securelist, 2013)

Ezeknek az igen kifinomult kémprogramoknak a kifejlesztése nagyon nagy szakértelmet, anyagi és szellemi ráfordítást igényelt, minden ok megvan azt feltételezni, hogy kifejlesztésük mögött állami támogatás állhat.

3.3. A hacktivizmus

A következő fenyegetés, amelyet be kell mutatnom, a hacktivizmus. A szó a hacker és az aktivista szavakból alakult ki. Leghírhedtebb képviselőjük az Anonymous csoport. Ez a laza szerveződésű internetes közösség vélt vagy valós sérelmek megtorlásául vagy egyszerűen valamely ügyet felkarolva indít támadásokat internetes tartalmak, cégek, kormányzatok ellen.

Az Anonymous logója egy fej nélküli, babérkoszorúba foglalt öltönyös figura, tagjai pedig, ha utcára mennek vagy képet tesznek ki magukról a netre, akkor a *V mint vérbosszú* című filmből ismert mosolygó Guy Fawkes maszkot viselik, amelyet annak főhőse hordott.

Az Anonymous logója

(forrás: http://en.wikipedia.org/wiki/Anonymous_(group) letöltve: 2016. február 14.)

A közösség a 2003-ban alakult 4chan nevű képmegosztó oldal felhasználóiból verbuválódott. A kezdetben a japán képregények rajongóinak szóló oldal hamar nagy népszerűségre tett szert, tartalmában és stílusában azonban az internet sötét oldalához tartozik. A beszélgetések úgy általában a tizen-huszonéves internet, online pornó és videojáték-mániás amerikai fiatalok szellemi színvonalán zajlik, akik ebből ítélve az oldal törzsközönségét alkotják. Az obszcén tartalmairól és féktelen szabadosságáról ismert fórum, vagyis képes üzenő fala már kevesebb látogató számára érdekes és vállalható, de így is az internet egyik legnagyobb hatású oldala. Jellemző, hogy felhasználói a kortárs online popkultúra rengeteg fontos elemét termelték, termelik ki és dolgozzák fel újra folyamatosan. A 4chan mindezek ellenére, vagy talán épp ezért, az online tömegkultúra egyik termékeny alkotóműhelyévé vált, amelynek látogatói saját elvetemült humoruk és a Photoshop segítségével rengeteg internetes mémet, vagyis egy adott témára épülő, továbbküldés útján terjedő, folyamatosan remixelt műalkotást dobnak be a köztudatba. A 4chanról származnak például a lolmacskák, vagyis az internetes szlengben feliratozott vicces macskás képek. (Vámosi, 2010)

Ebből a közegből származik tehát az Anonymous, melynek fontos eszköze a weboldalakat automatikus lekérdezésekkel megbénító túlterheléses támadás, amire magasztos hangnemben megfogalmazott webes szórólapjain tobo-

rozza a résztvevőket, rendszerint nem csak a 4chanon, hanem más csevegő szobákban és fórumokon is. A szaknyelven dosolásnak[3] nevezett támadásokban való részvételhez nem is kell más, csak pár ingyenesen letölthető szoftver, amelyek beszerzéséhez, használatához a felhasználók rendszerint már a szórólapokon megkapják a szükséges instrukciókat. 2007-ben először így bénították meg a rasszista kijelentéseiről elhíresült amerikai rádiós, Hal Turner műsorát, noha a 4chanon mindennapos dolog a niggerezés vagy más népek, országok alpári stílusú pocskondiázása. A következő nagy támadás a szcientológiai egyház ellen indult 2008-ban. Tiltakozásul az egyház által véleményük szerint elkövetett csalások, illetve az egyház által állítólag végzett agymosások miatt, kiterjedt támadásba kezdtek ellenük. A szolgáltatásmegtagadásos támadásokon kívül, amellyel elérhetetlenné tették az egyház honlapját, nyilvánosságra hoztak több száz iratot és dokumentumot, amelyeket számítógépes betörések útján szereztek. (Nemes, 2008)

Saját meghatározásuk alapján tiltakoznak és fellépnek minden olyan jelenség ellen, amely a szólásszabadságot és az internet szabadságát veszélyeztetik.

Ebbe belefért a Sony ellen indított támadás is, mely során több millió felhasználó adatait, köztük bankkártyaszámait lopták el és tették nyilvánossá azért, mert a Sony perbe fogta azt a hackert, aki feltörte a PlayStation védelmét.

A legnagyobb port felvert támadássorozatuk a Wikileaks támogatását megakadályozó amerikai intézkedések miatt következett be. Mint az ismeretes, 2010-ben a Wikileaks több ezer titkos amerikai diplomáciai és katonai iratot jelentetett meg az interneten a szólásszabadság jegyében. Ez komoly diplomáciai feszültséget és még komolyabb biztonsági problémákat okozott, elsősorban az amerikai hadsereg műveleti területein. Az amerikai kormány erős politikai nyomást fejtett ki az oldal ellehetetlenítésére, többek között a finanszírozásával kapcsolatban. A PayPal, a Visa vagy a MasterCard e nyomás hatására nem engedélyezte a Wikileaks számláira történő utalásokat. Ennek hatására hirdette meg az Anonymous a fenti pénzintézetek elleni támadássorozatát, amelyben sikerült is kisebb fennakadásokat okozni. Ezekért a támadásokért 2013-ban 13 embert el is ítélt egy amerikai szövetségi bíróság. (Rawlings, 2013) 2015-ben a párizsi Charlie Hebdo szerkesztőségét ért táma-

3 DOS – Denial of Service – szolgáltatásmegtagadással járó támadás

dás, majd a novemberi 129 emberéletet követelő merénylet után háborút hirdettek az Iszlám Állam ellen. (Dubuis, 2015) Feltörték a terrorszervezet több szerverét, hozzájuk köthető Twitter és Facebook fiókokat és adataikat nyilvánosságra hozták.

Létezik az Anonymous csoportnak magyar szárnya is, Facebook oldaluk is van, ahol a hitvallásukat is közzétették:

> *„Anonymous vagyunk. Egy eszme vagyunk. A pénzügyi és politikai zsarnokság ellen küzdünk itthon és globális szinten, Egy emberibb világot akarunk, ahol nem a profit, a hatalom, az erőszak számít, hanem az igazság, a szabadság, az egyenlőség. Változást szeretnénk elérni: a tudás, az információ nyílt áramlását, a cenzúra eltörlését, a szúk, kapzsi elit uralmának a végét és a 99% valódi hatalmát. Közvetlen demokráciát, igazi beleszólást akarunk. A jelenlegi rendszer igazságtalan, embertelen és végpusztulás felé sodorja a civilizációt. Nincsenek vezetőink, nincsenek rendszabályaink, nincsenek bombáink, Sokan vagyunk, napról-napra egyre többen vagyunk. Légiót alkotunk. Nem felejtünk, nem bocsájtunk meg. Számolj velünk és számíts ránk! Csatlakozz hozzánk és legyél részese egy győztes forradalomnak!" (Anon, 2012)*

Magyarországi tevékenységük weboldalak feltörésével kezdődött; 2012. március 4-én feltörték az Alkotmánybíróság honlapját és átírták az Alaptörvény szövegét, április 8-án a Nemzeti Rehabilitációs és Szociális Hivatal következett. Augusztus 28-án túlterheléses támadást intéztek a Közgép Zrt. honlapja ellen, amelyet sikerült is egy rövid időre megbénítani. A magyar Anonymous saját csoportjának méretét 50-60 aktív főre tesz, akik állandóan akcióra készek, valamint további 150-200 fő elkötelezett követőre. Legutóbb 2016. február 23-án a Nemzeti Választási Irodánál történt incidens kopasz résztvevőit fenyegették meg személyes adataik nyilvánosságra hozatalával.

Hosszan sorolhatnánk a csoport által elkövetett támadásokat, a világ szerzői jogvédő hivatalaitól az arab tavasz támogatásán át a világméretű pedofilhálózat feltöréséig.

Céljaik néhány esetben támogathatók ugyan, de a módszereik veszélyesek és egyértelműen törvénytelenek. Nincsenek nevesített vezetőik, szervezetük

decentralizált és tagjaik a világ minden részén megtalálhatók. Az, hogy milyen célpontot támadnak sikeresen, attól is függ, hogy mennyi támogatót tudnak megnyerni maguknak.

Nagyon sok politikus, újságíró jelentette már ki, hogy az Anonymous csoport tagjai kiberterroristák. Én ezzel a véleménnyel nem értek egyet, szerintem a hacktivizmust nem lehet összemosni a terrorizmussal, mert nekik nem céljuk a pánikkeltés és az erőszak.

3.4. A kiberterrorizmus

Ma már közhelynek számító kifejezés, hogy a világ megváltozott 2001. szeptember 11-e óta, amikor is az Al Kaida terrorcsoport lerombolta New Yorkban a World Trade Center ikertornyait. Több milliárd ember nézte a Földön élőben, ahogy a füstölgő épületek összeomlanak. Kétségtelen, hogy ez volt a legnagyobb szabású terrortámadás, ami eddig történt. Oszama Bin Laden és társai örülhettek, hisz sikerült megleckéztetni az Egyesült Államokat, az amerikaiak mindennapjaiba becsempészni a rettegést. Végül is ez a terrorizmus célja, a fenyegetés, a félelemkeltés, a társadalombefolyásolás. A Hadtudományi Lexikonban található definíció szerint:

„Terror, megkülönböztetés nélküli támadás: minden olyan erőszakos cselekmény, vagy azzal való fenyegetés, amelynek elsődleges célja, hogy rettegést keltsen a polgári lakosság körében." (Hadtudományi Lexikon, 1995 p1324)

Míg a 70-es évek terrorcselekményei elszigetelt jelenségek voltak és csupán néhány országot érintettek, mára már világméretűvé vált a fenyegetettség, gondoljunk csak az Iszlám Állam vagy a Boko Haram rémtetteire.

A terroristacsoportok is kihasználják a korszerű technológiák adta lehetőségeket, melyek segítségével gyorsabban, hatékonyabban tudják a számukra fontos információt megszerezni, illetve célközönségük irányába eljuttatni.

Ha az információtechnológia terrorista célú alkalmazását vizsgáljuk, akkor több területet is kiemelhetünk, a teljesség igénye nélkül:

3.4.1. Kapcsolattartás

Mivel a hagyományos vezetékes és mobiltelefonok könnyedén lehallgathatók a hatóságok által, ezért az internet nyújtotta kommunikáció nagyon népszerű a terrorista szervezetekben. A sok helyről letölthető és könnyen kezelhető

titkosító programok segítségével kódolhatják az üzeneteiket, így nehezítve meg a felderítésüket. Az utóbbi időben előszeretettel használják a különböző játékkonzolok játékainak azon funkcióit is, amelyek segítségével a játékosok kommunikálhatnak egymással.

3.4.2. Információszerzés

Közhelynek hangzik, de valóban igaz, hogy amit nem lehet megtalálni az interneten, az nem is létezik. Tudják ezt a terrorista szervezetek is, és ki is használják az akcióik tervezéséhez. Ha beírjuk a Google keresőjébe a „How to make a bomb" mondatot, 153 000 000 találatot kapunk 0,66 másodperc alatt. Itt videók tömkelegét is megtaláljuk, amelyek lépésről lépésre mutatják be a bombakészítés módszereit. De a terrorakciók szervezéséhez jó szolgálatot tehet a Google Earth vagy a StreetWiev is, melyeken nagyszerűen fel lehet térképezni akár egy potenciális támadás környezetét is. Számos épület 3D-s látványképei és alaprajzai is megtalálhatók a neten. A lehetőségek széles tárházát támasztja alá egy al-Kaida kézikönyv, ami szerint nyilvános forrásokból, többnyire az internetről a szükséges információk 80%-a megszerezhető. (Timothy, 2003.) Nem véletlen, hogy 2003 januárjában Donald Rumsfeld akkori amerikai védelmi miniszter kiadott egy utasítást, mely szerint azonnal radikálisan csökkenteni kell az Amerikai Védelmi Minisztérium és egyéb USA-intézmények olyan weboldalainak a számát, illetve tartalmát, amelyeken keresztül különböző terrorszervezetek szenzitív információkra tehetnek szert, vagy a különböző honlapokon különkülön meglévő adatok felhasználásával juthatnak értékes – az USA számára pedig hihetetlenül veszélyes – következtetésekre. (Kovács, 2006.)

3.4.3. Propaganda

Az internet nagyon lényeges eszköz a terroristáknak az eszméik, szervezeteik, hőseik és tevékenységük bemutatására, hiszen a hagyományos médiákat nem használhatják propagandacélokra. Ezért saját weboldalakat üzemeltetnek itt számolva be tetteikről, céljaikról. Mindig hangsúlyozzák, hogy az ellenségeik hajthatatlansága miatt, céljaik elérésére nincs más lehetőségük, mint az erőszak. Saját magukat szabadságharcosnak állítják be, és így próbálnak szimpátiát ébreszteni maguk és az ügyük iránt. A könnyen befolyásolható embereket akár terrorcselekmények elkövetésére is ösztönözhetik az ilyen oldalak. Ez

a fajta propaganda sajnos nem hatástalan, az utóbbi idők magányos terroristái, mint például **Mohamed Merah, a toulouse-i merényletek elkövetője** 2012-ben **vagy a 2009-ben** az amerikai Fort Hood támaszponton 16 katona életét kioltó *Nidal Malik Hasszán* is lelkes olvasója volt ezeknek az oldalaknak. (Hess, 2009) Az Iszlám Állam is előszeretettel használja toborzásra, merényletek végrehajtására történő felbujtásra.

3.4.4. Adománygyűjtés

A terrorista szervezetek működésük finanszírozásához is felhasználják az internetet, weboldalaikon, fórumokon gyűjtenek adományokat. Az al-Kaida, függetlenül Oszama bin Laden jelentős magánvagyonától, mindig is függött a különböző adományoktól. Globális adománygyűjtő hálózatokat építettek ki, amelyek különböző alapítványokon, államoktól független szervezeteken és pénzintézeteken alapultak. Egy szunnita szélsőséges csoport, a Hizb al-Tahrir Európától Afrikáig terjedő internetes hálózatot használ erőfeszítései pénzbeli és elvi támogatására. Az IRA weboldalán pedig a látogatók hitelkártyával tudnak támogatást nyújtani. (Haig, 2007.)

Figyelemmel kísérik a közösségi oldalakat is, ahol azokat a felhasználókat, akik pozitívan nyilatkoznak hozzászólásaikban róluk, e-mailben keresik meg, hogy támogatást kérjenek tőlük. Az iszlám vallás öt alappillérének egyike a zakat, amely a muszlim vallású emberek számára kötelezővé teszi az anyagilag nehéz helyzetben lévő hittestvérek segélyezését. Ezt kihasználva számos olyan iszlám jótékonysági szervezet működik a világban, amely valójában terrorszervezetek finanszírozásában érdekelt. Természetesen nem terrorcselekmények támogatását kérik az olvasóktól, hanem árvaházak, gyermekek támogatását. Ez sok esetben hatásos érvelésnek bizonyul.

3.4.5. Pszichológiai hadviselés

Mint azt már említettem, a terrorizmus célja a fenyegetés, a félelemkeltés, a társadalombefolyásolás. Ennek nagyszerű eszköze az internet, ahol számos módja van a pszichológiai hadviselésnek, mint pl. félretájékoztatások, fenyegetések kézbesítése, félelem elültetése képek, videófelvételek bemutatásával stb. A legjobb példa erre az Iszlám Állam, amely professzionális szintre fejlesztette ezt a tevékenységet. Nap-nap után töltötték fel a különböző videó-

megosztó helyekre a hatásosan megvágott, HD minőségben felvett videóikat, elrabolt emberek lefejezéséről, elfogott katonák tömeges kivégzéséről. Ezekkel a felvételekkel nemcsak a keresztény világnak üzentek, hanem az ellenük harcoló muszlimoknak is. A módszer működött is, hisz katonai sikereiket nem egyszer az iraki vagy a szír hadsereg megfutamodásának köszönhették.

3.4.6. Kibertámadások

Ne legyenek illúzióink, mert ha egy terrorszervezetnek lenne lehetősége kritikus infrastruktúrák elleni kibertámadásra, amellyel emberéleteket is veszélyeztetne, habozás nélkül megtennék. Szerencsére azonban még nincsenek birtokában annak a tudásnak, mely ilyen támadás kivitelezéséhez szükséges. Már törtek be rendszerekbe, loptak el adatokat, cseréltek le honlapokat, de komolyabb támadást még nem sikerült véghezvinniük. Az nyilvánvaló, hogy ha egy hagyományos terrortámadást össze tudnának vonni egy kibertámadással, amely egymással összefügg, komoly károkat okoznának.

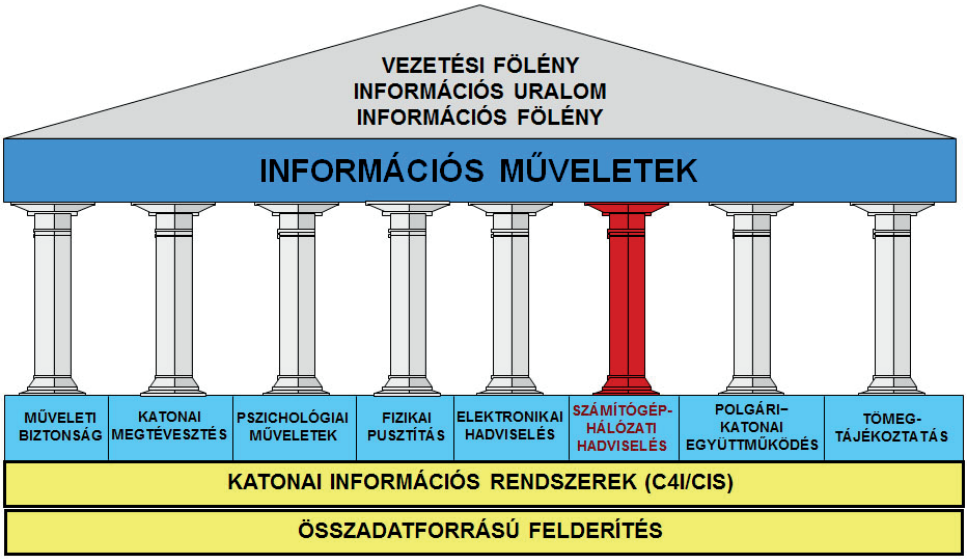
A hagyományos fegyverekkel végrehajtott támadások kibertámadásokkal való ötvözése már a kiberhadviselés témaköréhez tartozik.

4. Kiberhadviselés

A kiberhadviselés részletes ismertetése előtt meg kell ismerkednünk a katonai műveletekben elfoglalt helyével. A magyar terminológiában számítógéphálózati hadviselésként definiált tevékenység az információs műveletek szerves részét képezi. A NATO-ban az információs műveleteket az AJP 3.10-es doktrína taglalja, míg a Magyar Honvédségben a 2014-ben kiadott Információs Műveletek Doktrína foglalkozik vele. Az információs műveletek keretében egymással szorosan összefüggő tevékenységeket integrálunk annak érdekében, hogy a katonai műveletekben elérhessük az információs fölényt, ennek következtében kivívjuk az információs uralmat, majd a vezetési fölényt azáltal, hogy a saját oldali vezetési ciklus számára időcsökkentést, a szemben álló félnél pedig időnövekedést érünk el. Ez biztosíthatja, hogy elérjük a hadműveleti fölényt is. Ezen tevékenységek a fizikai, az információs és a tudati dimen-

ziókban fejtik ki hatásunkat. Részét képezi az elektronikai hadviselés, a pszichológiai műveletek, a műveleti biztonság, a katonai megtévesztés és a fizikai pusztítás is. (Haig, Várhegyi, 2005 p185) Az alábbi ábra mutatja be a számítógéphálózati hadviselés helyét az információs műveletekben.

2. ábra Számítógéphálózati műveletek helye az információs műveletekben



(forrás: Haig, Várhegyi, 2005 p198)

Az Egyesült Államokban egy kicsit másfajta megközelítést használnak a katonai szakértők. Egy új műveleti elgondolást dolgoztak ki, amelyet a 2014-ben elfogadott FM 3-38 Kiber-elektromágneses tevékenységek (Cyber Elecromagnetic Activities) nevet viselő doktrínában jelent meg. Lényege, hogy integrálják és szinkronizálják az elektronikai hadviselést, a kiberműveleteket és a frekvenciamenedzsment-műveleteket annak érdekében, hogy egymást kiegészítő és erősítő hatásokat érjenek el. Könnyen belátható, hogy a fenti tevékenységek közötti együttműködés hiánya csökkentené a műveletek hatékonyságát, az elektromágneses spektrumot használó eszközök és rendszerek között nem kívánt ütközéseket és interferenciákat hozhatna létre. (Haig, 2015 p122) A doktrína meghatározása szerint „ *A kiber-elektromágneses tevékenységek azok a tevékenységek, melyek biztosítják a szemben álló féllel és az ellenséggel*

szembeni előny megszerzését, megtartását és kihasználását a kibertérben és az elektromágneses spektrumban egyaránt, miközben akadályozzák és csökkentik a szemben álló fél és az ellenség lehetőségeit ugyanerre és megóvják a saját vezetésirányítási rendszert."(FM 3-38, 2014)

Ezt a koncepciót az alábbi ábra szemlélteti:

3. ábra Kiber-elektromágneses tevékenységek

(forrás: Kovács Z. 2014)

A számítógéphálózati hadviselést két fő csoportra oszthatjuk. A támadó jellegű műveletekre, melynek célja az ellenség hálózatba kötött informatikai rendszereinek feltérképezése, működésük befolyásolása, lerontása, megbénítása és a védelmi jellegű tevékenységekre, amely a saját számítógép-hálózataink megóvását jelenti a szemben álló fél információs támadásaival szemben.

A számítógéphálózati támadás szoftveres vagy hardveres úton történő behatolást jelent a megtámadott fél informatikai rendszerébe, annak érdekében, hogy az ott tárolt adatokat megsemmisítsük, módosítsuk vagy hozzáférhetetlenné tegyük, illetve magának a rendszernek a működését ellehetetlenítsük. Ezeket a támadásokat jól felkészült informatikai szakemberek, úgynevezett hackerek végzik, akik az informatikai rendszereket a mindenki által elérhető szint felett ismerik, képesek a hálózatok gyenge pontjain keresztül illegálisan belépni, ott jogosultságokat szerezve, különféle műveleteket végezni. (Haig, Várhegyi, 2005 p228) Fontos megjegyezni, hogy ezek a szakemberek nem mindig rosszindulatú céllal használják szaktudásukat, a rendszerek gyenge pontjainak kijavítása érdekében is dolgozhatnak, ekkor etikus hackelésről beszélünk.

A számítógépes támadások eszközei közül ki kell emelnünk a rosszindulatú programokat, amelyeknek számos alfaja létezik. A mindenki által ismert vírusok olyan programok, amelyek saját programkódjukat hozzáfűzik egy másik programhoz, így szaporodnak, terjednek. Általában két fő részük van, az egyik a terjedésért felelős, a másik pedig a mag, amelyben a végrehajtandó tevékenység található. A programférgek önálló programok, akik képesek a szaporodásra, önmaguk terjesztésére. A felépítésük hasonló, mint a vírusoké, általában pluszban külön programrész felel az álcázásért, hogy nehezebben lehessen felfedezni őket. A trójai típusú programok látszólag hasznos funkciókkal bíró alkalmazások, azonban eredeti funkciójuk mellett nem kívánt műveleteket is végrehajtanak. Ezeken kívül léteznek még különböző kémprogramok, billentyűzetfigyelő programok és ezek kombinációi. (Haig, 2015. p131) Egy másik gyakran használt módszer a botnetek vagy zombi hálózatok használata. A zombi számítógép olyan számítógép, amelyet valamilyen trójai szoftverrel irányítása alá vesz egy rosszindulatú támadó. A számítógép erőforrásait ezután a saját céljára, sokszor DDoS-támadások[4] lebonyolítására

4 Distributed Denial of Service – elosztott szolgáltatásmegtagadással járó támadás

használja. Botnetnek ezeknek a zombi gépeknek a hálózatát nevezzük. Ha elegendő mennyiségű zombi számítógép áll a támadó rendelkezésére, képessé válhat a kiválasztott célpont túlterhelésére és ezáltali működésképtelenné tételére. (Orbók, 2015) Az ilyen irányított gépeket használják egyébként spamek, azaz kéretlen levelek tömeges küldésére is. Fontos megjegyezni, hogy ezen eszközök nem csak a kiberhadviselés eszköztárában vannak jelen, ezt használják a kiberbűnözők és az egyéb rossz szándékú támadók is.

A védelmi jellegű műveletek értelemszerűen a saját informatikai rendszereink megvédése az ellenség támadó tevékenységével szemben. Ezek eszközei például a tűzfalak, amelyek az illegális hálózati forgalmakat szűrik ki, a különböző vírusvédelmi szoftverek, amelyek a rosszindulatú kódokat ismerik fel és semmisítik meg.

Nagyon lényeges kiemelni, hogy kiberhadviselésről csak abban az esetben beszélhetünk, ha egy ország egy másik ország számítógépes hálózatai, kritikus informatikai infrastruktúrái ellen indít támadást informatikai és fizikai eszközökkel saját nevében vagy egy harmadik fél bevonásával. E harmadik fél lehet állam, valamilyen szervezet vagy csoport. Ezt azonban az elmúlt évek kibertámadásaiban még egyszer sem sikerült bizonyítani, hiszen minden, hírbe hozott ország határozottan tagadta a vádakat.

A következőkben bemutatom az elmúlt időszak nagyobb kibertámadásait.

Habár a szakirodalom szerint a legelső dokumentált kibertámadást 1997-ben egy Srí Lanka-i terrorszervezet, a *Tamil Tigrisek* követték el (Haig, Kovács, 2008), úgy gondolom, nem mehetünk el szó nélkül az 1982-es szibériai gázvezeték-robbanás mellett sem. Thomas C. Reed, az amerikai Nemzetbiztonsági Hivatal egykori munkatársa 2004-ben megjelent könyvében leírja, hogy a robbanás nem a véletlen műve volt, hanem a szovjetek elleni gazdasági hadviselés része. A Szovjetunió megpróbált embargós nyugati technológiához jutni, az Egyesült Államok viszont meg akarta akadályozni, hogy a szovjetek valutabevételhez jussanak a nyersanyagszállításokból.

Egy, a KGB-be beépült ügynök juttatta el a CIA-hoz azt a listát, amelyen a szovjetek által beszerezni kívánt technológia szerepelt. Ezen találták azt a bizonyos szoftvert, amelyet a nyersanyagvezetékek irányítási rendszereihez használtak volna. Egy kanadai vállalaton keresztül a CIA adta el a szovjeteknek a szoftvert, amelybe azonban olyan hibákat építettek, hogy néhány hónapos

kifogástalan működés után összezavarta a szállítási folyamatokat. Ezt a vezeték irányítószelepeinek precízen megtervezett fals működtetésével érték el. Ennek eredménye volt az eddigi legnagyobb, nem nukleáris eredetű robbanás, amely a szovjet gazdaságot is megrázta 1982 nyarán.

Ez az emberéletet nem követelő, de hatalmas kárt okozó robbanás indította el a hidegháború utolsó felvonását – állítja a könyv szerzője. Mert noha a szovjetek rájöttek, hogy manipulált technológiát vettek, innentől kezdve nem bízhattak meg egyetlen beszállítójukban sem. (Kettmann, 2004)

Ebben a történetben az a furcsa, hogy mind a szovjet, mind az amerikai kormány hevesen tagadta a szerző állításait. A szovjetek a hanyag munka rovására írták a robbanást, az amerikaiak pedig nem ismertek el semmilyen szoftvermódosítást. Technikailag elképzelhető a kivitelezés, de mivel csak egyetlen forrás áll rendelkezésünkre, ezért kezeljük fenntartással a történetet annak ellenére, hogy a Wikipédia „Cyberwarfare in the United States" szócikkében szerepel az esemény mint kibertámadás más nemzet ellen.[5] Mindenesetre jól mutatja, hogy a számítógép-vezérlésű eszközök sebezhetősége és támadhatósága nem napjainkban keltette fel a potenciális támadók figyelmét.

1999-ben szerb hackerek – a NATO szerbiai bombázásaira válaszul – támadták meg a szövetség szervereit és néhányat DDoS módszerrel tettek átmenetileg elérhetetlenné, valamint feltörtek néhány weboldalt és propagandaüzeneteket helyeztek el rajtuk.

Az első kibertámadás, amelyet egy ország ellen indítottak, 2007-ben következett be. Az igen fejlett informatikai kultúrával rendelkező Észtországban 2007. április 27-én zavargások törtek ki a tallinni szovjet hősi emlékmű eltávolítása miatt. Az első túlterheléses támadások jelei néhány nappal az első tüntetések után jelentkeztek a parlament, kormányhivatalok, minisztériumok, bankok, telefontársaságok és médiacégek szerverei ellen. A célpontok kiválasztása, a támadások összehangoltsága, precíz kivitelezése és hatékonysága arra mutatott, hogy e támadások hátterében szervezett erők állnak. Néhány esetben szakértők megállapították, hogy a támadások orosz szerverektől indultak, amit az orosz hatóságok természetesen tagadtak. Ugyanakkor a megtámadott szerverek jellegéből adódóan nyilvánvaló, hogy a támadások célja

5 Kiberhadviselés az Egyesült Államokban – https://en.wikipedia.org/wiki/Cyberwarfare_in_the_United_States

egyértelműen a balti állam kritikus információs infrastruktúrájának bénítása volt. Az ország online adatforgalmát irányító kulcsfontosságú szerverek naponta omlottak össze, sok állami intézmény hálózatát kénytelenek voltak ideiglenesen leválasztani az internetről. Az elektronikus banki forgalom és kereskedelem részint megszűnt, részint erősen akadozott. Egyes szakértők szerint a kibertámadás sokkal súlyosabb gazdasági károkat okozott Észtországnak, mint amit azok a kereskedelmi szankciók okoztak volna, amikkel Oroszország a krízis első heteiben fenyegetőzött.

Bár kezdetben NATO-szakértők is részt vettek a támadások felderítésében, azok jellegéből adódóan a támadók azonosítása szinte lehetetlen volt. Számos támadót lehetett ugyan azonosítani orosz területen, de annak egyértelmű igazolása, hogy kormányzati szerverek voltak, sikertelennek bizonyult. Általánosan elterjedt nézet szerint orosz hazafias érzelmű hackerek olyan botnet-hálózatot hoztak létre, amelybe orosz gépeken kívül még 178 ország területén lévő számítógépeket is beszerveztek a tudtuk nélkül (zombi gépek), és ezeken keresztül hajtották végre a támadásokat. (Haig, Kovács, 2008)

A 2008 augusztusában kitört orosz-grúz háborúnak is volt kiberaspektusa. Mint az köztudott, a hosszú évek óta tartó grúz-oszét és a grúz-abház konfliktust a grúz elnök 2008. augusztus 8-án katonai úton próbálta megoldani az említett területek megtámadásával. Rosszul mérte fel azonban az erőviszonyokat, amikor nem számolt azzal, hogy Oroszország nem fogja szó nélkül hagyni a támadást, már csak azért sem, mivel csapatai ENSZ-felhatalmazással békefenntartó missziót teljesítettek Dél-Oszétiában. Az orosz csapatok erőteljes válaszcsapásokat mértek a grúz erőkre, és öt napig tartó heves harcok után a grúzok kénytelenek voltak fegyverszünetet kérni. (Németh, Hajzer, 2008)

A fegyveres konfliktussal egy időben megindult Grúzia ellen egy kiberhadjárat is. Az internetforgalmat ellenőrzése alá vonta Oroszország – vagy legalábbis valakik Oroszországból, állította a grúz kormány, amely valóságos kiberemigrációba kényszerült, és a hadi jelentések mellett sorra jelentette meg a virtuális támadásokról szóló közleményeit.[6]

6 http://georgiamfa.blogspot.hu/2008/08/cyber-attacks-disable-georgian-websites.html

A leglátványosabb hacker-akciók ugyanis az ország kormányzati weboldalai ellen indultak, amelyeket kívülről megbénítottak, illetve a tartalmukat kicserélték[7]. Az orosz földről érkezett hackerek Mihail Szakasvili elnök portréjával vandálkodtak. Az államfő képére Hitler-bajuszt rajzoltak, és egy sor olyan képet tettek ki róla az oldalra, ahol a náci diktátor pózaiban ábrázolták, vagy a történelem nagy gonosztevői közé kopírozták be az arcmását.

A megtámadott oldalak között volt az elnök saját weblapja mellett a grúz külügy- és hadügyminisztérium is. Szakasvili elnök erre válaszul a hazája ügyét nyíltan támogató Lengyelország vezetőjétől kért és kapott segítséget: az államfő, illetve stábja Lech Kaczynski hivatalos, angol nyelvű oldalán is lehetőséget kapott arra, hogy tájékoztatást adjon a háborús eseményekről. Még ezt a hivatalos, nagyban gesztusértékű lépést megelőzően a honlap nélkül maradt grúz külügyminisztérium blogot indított a Google által birtokolt Blogspot blogszolgáltatónál.

Mindezekkel egy időben megindultak az ország lejáratását célzó, dezinformációs céllal indított weboldalak is – a hiteles forrásokat a konfliktusról percről percre beszámoló blog a linkek között listázta. A kaukázusi országban a .ru végződésű webcímek is elérhetetlenné váltak, amelyeket egyes források szerint maga a grúz kormányzat tilttatott le, hogy útját állja az orosz propagandának, és a Tbilisziben lévő orosz nagykövetség munkatársai szerint a mobil- és vezetékes telefonszolgáltatásban is fennakadások voltak a túlterhelés miatt (igaz, ennek inkább a katonai offenzívához lehetett köze). (Vámosi, Szedlák, 2008)

Véleményem szerint a grúz kormány erősen eltúlozta az ellene indított kibertámadásokat, hisz korántsem rendelkezett olyan infrastruktúrával, mint például Észtország, így a támadásoknak sem volt olyan hatása, nem bénult meg a bankrendszer, illetve a kormányzat. Az interneten keresztül zajló nagyszabású támadások akkor különösen hatékonyak, ha egy olyan ország ellen irányulnak, amely erőteljesen támaszkodik információs technológiára és annak infrastruktúrájára. Grúzia esetében ez nem mondható el: az interneten keresztül a támadók nem tudtak nagyobb károkat okozni, mint az or-

7 Ezt nevezi az internetes szaknyelv defacementnek.

ság földjére lépő orosz katonák. Hétköznapi ésszel érthetetlen, hogy a kormány miért foglalkozott olyan erőteljesen a kiber-támadásokkal, miközben városait, infrastruktúráját lőtte és bombázta az orosz hadsereg. Mindazonáltal ennél a konfliktusnál mutatható ki először, hogy a hagyományos katonai műveletek támogatására kiberműveleteket is alkalmaztak.

Mind az orosz-észt, mind az orosz-grúz konfliktus vonatkozásában elmondhatjuk, az orosz hivatalos szervek kategorikusan tagadták, hogy közük lenne a támadásokhoz. A konfliktusok lezárulta utáni elemzések csupán azt tudták kimutatni, hogy orosz nacionalista érzések vezérelték a támadókat, ám az orosz állam közreműködését nem sikerült bebizonyítani.

Nem szabad figyelmen kívül hagyni azokat a támadásokat sem, amelyek célzottan valamely kritikus infrastruktúra ellen irányulnak. Ezek lehetnek áramszolgáltatók, erőművek vagy más létfontosságú rendszerek. Több olyan támadás is volt már a világon (Brazília, Törökország), ahol kibertámadás következtében állt le az áramszolgáltatás. Legutóbb 2015 decemberében regisztráltak ilyen jellegű támadást Ukrajnában, melynek következtében egy, hétszázezer embert érintő áramszünet következett be. Idén januárban a kijevi repülőtér számítógépes rendszerében találtak rosszindulatú kódokat, amelyek akár a repülés biztonságát is veszélyeztethették volna.

A kritikus infrastruktúrák, ipari folyamatirányító rendszerek támadásának eszközéül használt rosszindulatú kódok egyre fejlettebbek és kifinomultabbá váltak az utóbbi években. Ezen kódok készítői nagy hangsúlyt helyeznek programjaik rejtőzködő képességének fejlesztésére, ezáltal nehezítve a felderítésüket. Tipikus és hírhedt példája ezeknek a programoknak a fehérorosz VirusBlokAda cég által 2010 júniusában felfedezett új rosszindulatú kód, amelyet Stuxnetnek neveztek el.

Az új féreg Microsoft operációs rendszereken terjedt és kizárólag ipari folyamatirányító rendszerek ellen lett kifejlesztve. A Stuxnet kivételes mivoltát és specializáltságát erősíti az a tény is, hogy az említett ipari felügyeleti, vezérlő és adatgyűjtő rendszereket egyetlen cég, a **német Siemens gyártja (SIMATIC WinCC HMI és WIMATIC STEP 7)** és alapvetően a nehézipari szektorban, illetve az energiatermelés és szállítás területén használják, azaz fenyegetést alapvetően csak olyan létesítményekre jelent, melyek egy része kritikus infrastruktúrának minősül. (Berzsenyi, Szentgáli, 2010)

A Stuxnet végső célja ipari vezérlő rendszerek automatikus folyamatainak újraprogramozása volt. Elsősorban PLC[8] szoftvereket támadott. A WinCC/Step 7 szoftver volt mindezek közül az elsődleges, amelyet a Stuxnet megcélzott. Ez a szoftver adatkábelen keresztül kapcsolódik a PLC-hez és eléri a memóriatartalmat, képes folyamatokat újrakonfigurálni, programokat feltölteni és a végrehajtás során rendelkezik bizonyos nyomkövetési funkciókkal is. Ha a PLC már programozásra került, akkor lekapcsolható róla, és a PLC már önmagában is képes a működésre. A Stuxnet e szoftver segítségével juttatta be kódblokkjait a PLC-be, majd ezeket el is rejtette.

A Stuxnet a PLC-ken bizonyos konkrét ipari eszközök, nevezetesen nagy sebességű motorok frekvenciaátalakítói után kutatott és csak akkor lépett akcióba, ha a finn Vacon és az iráni Fararo Paya készülékeire talált, valamint a felügyelt eszköz 807 és 1210 Hz között működött. Ilyen frekvenciaátalakítók és motorok szinte kizárólag az iráni urándúsítókban használatosak. (Cserháti, 2011)

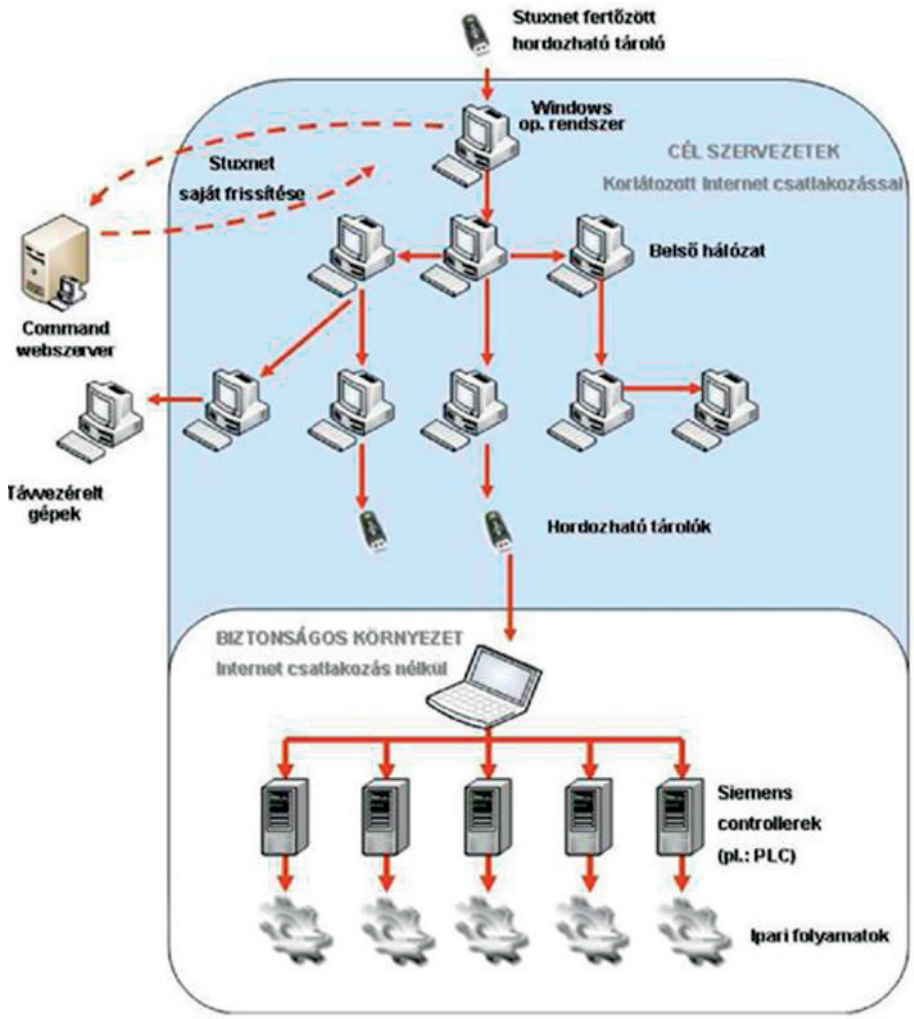
A vírus egyértelmű célja az urándúsító centrifugák észrevétlen tönkretétele és a dúsítási folyamat megzavarása volt. Ezt a célt sikeresen el is érte, hisz legalább 1000 centrifugát tett használhatatlanná a Natanzban lévő dúsítóban és mértékadó vélekedések szerint legalább két évvel vetette vissza az iráni atomprogramot.

A támadó kód megírásának profizmusára utal, hogy egyszerre négy zero-day[9] fenyegetést is kihasznált a terjedéséhez és két lopott digitális aláírással is tudta igazolni legitimitását.

Terjedését a következő ábra mutatja be.

8 A PLC – Programmable Logic Controller, azaz programozható logikai vezérlő. PLC-ket nagy számban az ipari szabályozástechnikában, a különböző villamos, illetve az ilyen módon működtetett folyamatok irányításában használják.

9 A zero-day/zero-hour, vagyis nulladik napi támadás kifejezést azokra a számítógépes biztonsági fenyegetésekre használják a szakemberek, amelyek egy adott számítógépes alkalmazás még felfedezetlen, nem publikált sebezhetőségét használják ki. A támadó a sebezhetőség felfedezését követően úgynevezett zero-day exploitot készít, amely az a tényleges számítógépes kód, ami képes a sérülékenység kiaknázására. Azonban a sérülékenységek nehéz és bonyolult detektálhatósága miatt a kártékony programok készítői számára jelentős értéket képvisel egy újonnan felfedezett sérülékenység, ezért egy program általában csak egy sérülékenység kihasználására épül. Ezen támadások idején a megtámadott alkalmazás fejlesztőjének még többnyire nincs tudomása a sérülékenységről, vagy még nem tudott javítást készíteni hozzá.



(forrás: Kovács, Sipos 2010)

4. ábra A Stuxnet terjedése a belső hálózaton

Származásáról sokáig nem voltak pontos adatok, de mindenki rögtön az Egyesült Államokra és Izraelre gondolt mint olyan országokra, amelyeknek érdekében és módjában is állhatott az iráni atomprogram elleni akció. Ralph Langner hamburgi vírusbiztonsági szakértő blogjában mélyrehatóan foglalkozott a Stuxnettel és a 2010. december 31-i bejegyzésében az alábbiakat írta:

„Egy ilyen nagy horderejű támadás mögött feszülő hatalmas erőket elég könnyű érzékelni. A Stuxnet kártevő kifejlesztéséhez extrém mennyiségű hírszerzési adat kellett a natanzi dúsító mű elrendezéséről, teljesen meg kellett érteni az IR-1[10] működését (amihez feltehetően rendelkezésre állt egy üzemképes tesztelő rendszer is), valamint a Siemens érintett termékeiről rengeteg bennfentes tudásra volt szükség. Mindez igen kevés szervezetre szűkíti le a világon azt a kört, amely a feladat megoldására vállalkozhatott." (Langner, 2010)

2016 februárjában mutatták be a Berlini Nemzetközi Filmfesztiválon Alex Gibney dokumentumfilmjét, Zero Days címmel, amely ezzel a témával foglalkozott. A filmben megszólal Michael Hayden tábornok is, aki a CIA[11] és az NSA[12] vezetője is volt. Itt elismeri, hogy a Stuxnetet Izraellel együttműködve fejlesztették ki, célzottan Irán atomprogramja ellen. (Magyar Nemzet Online, 2016)

Ám a Stuxnet csak a kezdet volt az új generációs kártevők sorában. A Budapesti Műszaki Egyetem Híradástechnikai Tanszékén működő CrySyS Adat- és Rendszerbiztonság Laboratórium munkatársai fedezték fel 2011-ben a Duqu és 2012-ben a sKyWiper kódokat, amelyek szintén nagyon fejlett, kifinomult eszközök, voltak és kifejlesztésükben szinte biztosra vehető volt az állami segítség. 2015 elején a Kaspersky Lab talált egy új kártékony kódot, amelyet Duqu 2 néven vált ismerté. Az új kód a legkifinomultabb, amivel eddig találkoztak, készítőinek gondolkodásmódja és filozófiája teljesen újszerű. A cég vezető kutatója szerint a kémprogrammal mintegy száz célpontot támadtak meg, köztük olyan luxusszállodákat is, amelyekben az iráni atomfegyverprogram megfékezését célzó nagyhatalmi tárgyalások folytak. (SG1, 2015)

Ezek az adatok is azt támasztják alá, hogy a világ számos katonai és kormányzati szerve törekszik arra, hogy a kibertérben is meghatározó befolyást szerezzen, ott nem csak a támadások elhárítására törekedjen, hanem támadó kapacitással is rendelkezzen.

10 A pakisztáni P-1 urándúsító centrifuga iráni változatának a külvilág által adott neve.
11 Central Intelligence Agency – Központi Hírszerző Ügynökség
12 National Security Agency – Nemzetbiztonsági Ügynökség

Az informatikai támadások elhárítása mára elsőrendű problémává lépett elő a világban. Mindenhol felismerték, hogy a kiberbiztonság fejlesztése elengedhetetlen, és a kulcsfontosságú információs rendszereket meg kell tudni védeni a kibertámadásoktól. Ezzel összhangban 2008 májusában alakult meg a Kooperatív Kibervédelmi Kiválósági Központ (NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE)). Május 14-én írták alá az Együttműködési Nyilatkozatot az alapító országok, a balti államok, valamint Németország, Spanyolország, Olaszország és Szlovákia. A Központot az Északatlanti Tanács döntése alapján 2008. október 28-án jogi értelemben is nemzetközi katonai szervezetté nyilvánították. Jelzésértékkel bír, hogy a Központ Tallinnban, Észtország fővárosában jött létre. A Központ feladatai közé tartozik többek között a tagállami kiberképességek kialakításának, tagállami doktrínák, koncepciók és stratégiák kidolgozásának támogatása, az információbiztonság oktatása, folyamatos képzések és gyakorlatok lebonyolítása és a kiberhadviselés jogi vonatkozásainak elemzése. Vagyis a szervezet nem a NATO kiber támadóerejét jeleníti meg, hanem mint kutatási és oktatási központ működik. Hazánk 2010. június 23-án csatlakozott a Központ munkájához.

2013-ban jelent meg az a kiadvány, melyet nemzetközi hírű jogászok, technikai szakemberek és kutatók segítségével állítottak össze és a „Tallinn Manual on the International Law Applicable to Cyber Warfare[13]" címet viseli. Ez a kézikönyv több mint 300 oldalon, 2 részben, 95 fő szabályra lebontva részletesen tárgyalja a kiberhadviselés szabályait. Az első rész a „Nemzetközi kiberbiztonsági jog", a második a „Kiberhadijog" címet viseli. Az első részben határozzák meg, hogy a kibertámadás fegyveres támadásnak minősíthető, így a megtámadott állam jogosan használhat önvédelemből akár hagyományos fegyvereket is. Azonban nem tekinthető fegyveres támadásnak a kiberkémkedés, az információlopás és a honlapok feltörése. Az államok felelősséggel tartoznak ugyan ha a fennhatósági területeiről az ellenőrzésük alatt álló szervezetek más ország ellen kibertámadást hajtanak végre, az azonban, hogy egy támadást egy adott országból indítottak, még nem bizonyítja az adott ország felelősségét. Elképzelhető ugyanis, hogy más államok használták az adott ország kiberterét a támadás lebonyolítására.

13 Tallini kézikönyv a nemzetközi jog alkalmazásáról a kiberhadviselésben.

A második részben többek között kitérnek arra, hogy a hagyományos fegyveres konfliktusokhoz hasonlóan el kell kerülni a civil áldozatokat, tehát például tilos a civil célpontok, kórházak, atomerőművek, vízierőművek vagy gátak támadása – ezt egyébként a genfi egyezmények most is tiltják a hadviselő felek számára. Védekező és támadó kiberhadműveletekkel kapcsolatban megállapítják, hogy akkor minősül egy művelet a kibertérben elkövetett támadásnak, ha annak hatására személyek sérülnek vagy halnak meg, illetve vagyontárgyak rongálódnak, illetve semmisülnek meg. A támadások célszemélyei lehetnek a fegyveres erők és szervezetek tagjai. A hadviselés eszközei és módszerei kapcsán ügyelni kell arra, hogy nem szabad felesleges sérülést és szükségtelen szenvedést okozni ellenfélnek. A kiberhadviselésre is vonatkozik az arányosság elve, amelynek alapján a megtámadott fél nem okozhat sokkal nagyobb veszteséget a támadónak, mint amennyit elszenvedett.

Elmondhatjuk, hogy kiemelkedő jelentőségű mű született a kiberhadviselés szabályozásáról, amely ugyan nem tartalmaz kötelező jellegű ajánlásokat, de a széles körben történt egyeztetések során olyan elveket fektettek le, amelyet az egyes országok jól hasznosíthatnak jogalkotásukban. (Gyebrovszki, 2014)

Azt, hogy a NATO komoly kihívásnak tekinti a kibertérből érkező támadásokat, jól bizonyítja, hogy a 2016. július 8-án és 9-én Varsóban megrendezett csúcstalálkozón az állam- és kormányfők kiemelt figyelmet szenteltek a kiberbiztonságnak. A tagállamok a kiberteret új műveleti környezetként ismerték el, melyben a NATO-nak ugyanolyan hatékonyan kell védekeznie, mint a szárazföldön, a tengeren vagy a levegőben. Célul tűzték ki a kibervédelem fejlesztését, a tervezési folyamatokba történő nagyobb fokú integrálását, a nemzeti és szövetséges hálózatok fokozott védelmét a legmodernebb technológiák felhasználásával. A 2014-es walesi csúcstalálkozó után ismét deklarálták a kollektív védelem kibertérre történő kiterjesztését is. (Warsaw Summit Communiqué. 2016)

Mint említettem, a tallinni Központ nem a NATO kibertámadási képességeit fejleszti, ilyen típusú programja nincs is a szervezetnek, azonban egyes tagországok foglalkoznak a támadókapacitások fejlesztésével is, még ha ez nem is a nyilvánosság előtt zajlik. A világ sok országában indult kutatás a kibervédelem minél nagyobb szintre fejlesztése mellett arról is, hogy a támadási képességeket is kiterjesszék.

5. Kiberképességek a világban

Az Egyesült Államok, úgyis mint az internet szülőhazája és mint a világ vezető hatalma, igen nagy erőfeszítéseket tesz a kibertérben elfoglalt pozíciójának megőrzésére. Erre való tekintettel a Védelmi Minisztérium elhatározta egy katonai parancsnokság létrehozását, amely összefogja a kibertér védelmét az országban. A USCYBERCOM[14] az Egyesült Államok Stratégiai Parancsnokságának alárendeltségében, a Maryland állambeli Fort Mead-ben kezdte meg tevékenységét 2010-ben. Küldetésnyilatkozatuk szerint:

„*A USCYBERCOM tervezi, koordinálja, irányítja és vezeti azon tevékenységeket, amelyekkel megvédheti a Védelmi Minisztérium információs hálózatait, felkészülhet a kibertérben végrehajtott katonai műveletek végrehajtására, valamint minden területen biztosítja az Amerikai Egyesült Államok és szövetségesei számára a cselekvési szabadságot a kibertérben és megakadályozza a szemben álló felet annak használatában.*" (DoD, 2010)

A Parancsnokság fennhatósága alá került valamennyi fegyvernem kiberműveletekkel foglalkozó egysége: a Hadsereg Kiberműveleti Parancsnoksága (U.S Army Forces Cyber Command), a Légierő Kiberműveleti Parancsnoksága (24th USAF), a Haditengerészet Kiberműveleti Parancsnoksága (Fleet Cyber Command) és a Tengerészgyalogság Kiberműveleti Parancsnoksága (Marine Forces Cyber Command). Várhatóan a létszámát 2016-ra töltik fel teljesen, így 6200 fő fog itt szolgálatot teljesíteni. Tevékenységét az elektronikai felderítéssel foglalkozó NSA-vel összhangban végzi. Az egység mindenkori parancsnoka egyben az NSA főigazgatója is. (NSA, 2016) A kiberműveleti képességek fejlesztését az Egyesült Államok katonai és polgári informatikai hálózatainak egyre növekvő veszélyeztetettsége indokolta. A Parancsnokságnak az országot ért hagyományos és informatikai támadások esetén is képesnek kell lennie a megfelelő válaszcsapás végrehajtására a kibertérben. Kibertámadást az Amerikai Egyesült Államok elnöke rendelhet el, az ország katonai vagy civil számítógépes hálózatai elleni támadásra válaszul vagy ilyen támadás megelőzésére. Az Amerikai Egyesült Államok elleni kibertámadások elleni védekezés és a válaszcsapás módjai a 2011-ben megjelent Nemzetközi Kiberbiztonsági Stratégiában kerültek rögzítésre.

14 United States Cyber Command – Az Egyesült Államok Kiberernetikai Parancsnoksága

A stratégia szerint az amerikai kibervédelem a megelőzésre és az elrettentésre épít. A megelőzés alapja a nemzetközi együttműködés. Olyan nemzetközi rendészeti együttműködés kialakítását szorgalmazza, amely lehetőséget teremt a kiberbűnözés és a kiberterrorizmus elleni küzdelem továbbfejlesztésére. Az Amerikai Egyesült Államok elleni, egy nemzetállam által indított kibertámadást követő ellencsapás jogi megalapozásaként a stratégia megállapítja, hogy az kibertérben zajló tevékenységek is a nemzetközi közösséget alkotó szuverén nemzetállamok felelősségi körébe tartoznak. A stratégia szerint az Amerikai Egyesült Államok vagy szövetségesei elleni kibertámadás esetén az Amerikai Egyesült Államok minden szükséges diplomáciai, gazdasági és katonai ellenlépést megtehet. A stratégia alapján az Amerikai Egyesült Államok kibertámadásra akár hagyományos katonai válaszcsapással is felelhet. (International Strategy for Cyberspace, 2011)

Feltétlenül ki kell térnünk az NSA szerepére az amerikai kibertevékenységek kapcsán. A szervezet a Védelmi Minisztérium alárendeltségében működik, Alapvetően rádióelektronikai felderítésre hozták létre 1952. november 4-én. Tevékenységi körébe tartozik a külföldre irányuló rádiófelderítés, a kriptográfia, azaz a külföldi rejtjelfejtés és az amerikai rejtjelzés biztonságának védelme, valamint mindennemű elektronikai felderítés. (NSA2, 2016)

Az NSA volt az egyik főszereplője a még a hidegháborúban indult, de utána is évtizedeken át folytatott ECHELON műveletnek is, amelyben az Egyesült Államok, Nagy-Britannia, Ausztrália, Kanada és Új-Zéland vett részt, és amelynek fő tevékenysége a kereskedelmi távközlési műholdak adatforgalmának ellenőrzése volt. Ez a szoros együttműködés az öt ország között a mai napig fennáll (a szakirodalom csak „Big Five"-ként emlegeti őket). Edward Snowden, az NSA korábbi szerződéses munkatársa 2013 nyarán számos dokumentumot hozott nyilvánosságra, amelyek fényt derítettek az NSA globális lehallgató tevékenységének méreteire. A leleplezések óriási világvisszhangot váltottak ki.

Nyilvánosságra került, hogy az NSA világszerte több mint egymilliárd ember telefonos és internetes kommunikációját követi figyelemmel, és nem csak a terrorizmusról, hanem külpolitikai, gazdasági, konkrét kereskedelmi témákról is adatokat gyűjt. 2012 közepén az ügynökség naponta több mint 20 milliárd kommunikációs eseményt, úgynevezett metaadatokat (internet és telefon) rögzített.

Az NSA kiterjedt kémtevékenységet folytatott az Európai Unió, az Egyesült Nemzetek Szervezete és számos olyan kormányzat ellen is, amelyek egyébként az Egyesült Államok szoros szövetségese. A szervezet képességeiről a teljesség igénye nélkül csak annyit, hogy hozzáfér a legnagyobb online szolgáltatók szervereihez, be tudja kapcsolni a mobiltelefonok kameráját és mikrofonját távolról, titokban megcsapolja a tenger alatti adatkábelek forgalmát, távolról le tudja hallgatni a wi-fi forgalmat. A szervezet egyik legfontosabb egysége a TAO[15], melynek tagjai jól képzett hackerek. Feladatuk a külföldi szervezetek által működtetett számítógépes hálózatok azonosítása, megfigyelése, az azokba való behatolás és azokból információszerzés. A TAO együttműködik más hírszerzési szervekkel, mint a CIA és az FBI, ha szükség van rá, be is segít. A helyszínre juttatják, akár repülővel a hackereket, hogy a helyi hálózatokhoz vagy akár az internetről elzárt hálózatokhoz is hozzáférjenek. (Greenwald, 2014)

Tehát, mint láthatjuk az Egyesült Államok deklaráltan is képes támadóműveletek végrehajtására a kibertérben.

Kína az elmúlt évtizedek szédületes fejlődése után mára a világ második legnagyobb gazdaságává vált. Habár a 2008-as válság nem hagyta érintetlenül a kínai gazdaságot sem, a növekedés nem állt meg. Természetes, hogy a katonai képességek terén is töretlen a fejlesztés. 2016-ban a GDP növekedését meghaladó mértékben, 7,6 %-kal növelik a katonai kiadásokat, amely így eléri a 135 milliárd dollárt. Folyamatosan fejlesztik a kiberhadviselési képességeiket is. Az internetet potenciális háborús eszköznek tekintik, beleértve szakértők, hackerek kiképzését és felszerelését, hogy behatoljanak az ellenfél katonai információs hálózatába. Egyetemi kurzusokat indítottak a kibertámadásokra és azok kivédésére való felkészítés céljából, tanulmányozzák a hackerek módszereit, a számítógépvírusok tervezését és alkalmazását, a hálózati biztonság problémáit. (Jordán, 2011)

A világ vezető hálózatbiztonsági cégeinek jelentéseiből kitűnik, hogy a kibertámadások jelentős része kínai támadókra vezethető vissza. Több jelentés is említi a Sanghajban állomásozó 61398-as számú katonai egységet, melynek munkáját Kína államtitokká nyilvánította. Az egység bázisa Pudongban, a sanghaji pénzügyi központban van, és több ezer tagja lehet, akik

15 Tailored Access Operations (magyarul kb. „Testre szabott hozzáférési műveletek")

jól beszélnek angolul, illetve kiváló számítógépes ismeretekkel rendelkeznek. A jelentések szerint 2006 óta több száz terabyte adatot loptak el 141 szervezet számítógépeiről. (Mandiant, 2013 p3) A kínai védelmi minisztérium természetesen kategorikusan cáfolta, hogy Peking valaha is támogatott volna hackertevékenységet. Az azonban elgondolkodtató, hogy ekkora mennyiségű és ilyen típusú adatokkal egyszerű hackerek vagy kiberbűnözők mit kezdtek volna.

A kibertér harmadik nagy szereplője Oroszország, amely bevallása szerint szintén nem rendelkezik kiberhadsereggel. Ennek ellenére ők voltak az első számú gyanúsítottjai az észtországi incidensnek és a grúziai támadásoknak. Egyes vélemények szerint Oroszország kiberműveleti képességeinek alapjait kiberbűnözői csoportok képezik. Ezek a csoportok az orosz kormány hallgatólagos engedélyével végzik tevékenységüket, bevételeiket klasszikus kiberbűnözéssel szerzik. Képességeiket pedig szükség szerint az orosz vezetés által kijelölt célpontok ellen használják fel. Szakértők szerint az orosz kiberképességek alapját botnetek[16] képezik, emellett az orosz hackerek vezető szerepet töltenek be a számítógépes programok feltörésében is. A legismertebb orosz számítógépes bűnözői csoport a Russian Business Network (RBN), amelynek botnetjei a 2007. évi, Észtország elleni túlterheléses támadásokban is részt vettek. Egyes források szerint az RBN vezetői és az orosz államigazgatás, illetve a titkosszolgálatok között személyi összefonódás mutatható ki. (Flook, 2009) A kiberműveletekben részt vevő orosz titkosszolgálatok – elsősorban a Szövetségi Biztonsági Szolgálat, a Szövetségi Védelmi Szolgálat – számítógépes biztonsági szakértők szerint információs műveleti tevékenységüket fantomcégek létrehozásával, illetve az RBN és más számítógépes bűnözői csoportok működésének utánzásával fedik el. Oroszország – Kínához hasonlóan – rendszeresen támadja az Amerikai Egyesült Államok és más NATO-tagállamok számítógépes rendszereit. A botnetek természetéből adódóan azonban nem bizonyítható, hogy e tevékenységek valóban az orosz kormány irányításával zajlanak. (Nagy, 2012) Propaganda célokra előszeretettel használják a közösségi hálózatokat is. Egy Szentpéterváron működő cég két volt munkatársának beszámolója szerint a váltott műszakban dolgozó bérkommentelők százai,

16 Rosszindulatú kódokkal megfertőzött számítógépek sokasága, amelyeket egy vezérlő számítógép segítségével irányítanak. Tipikusan DDoS-támadásokhoz használják.

szigorúan szabályozott keretek között dolgoznak, hogy nyugatellenes, Kreml-barát híreket osszanak meg hazai és külföldi portálokon. A témákat az adott nap elején jelölik ki, és meghatározott számú kommentet kell meghatározott számú profillal elhelyezni. Ez a tevékenység azonban nem csak Oroszországra jellemző, más országok is használják a közösségi hálózatokat propagandaterjesztésre. Nagy-Britanniában a hadseregen belül hoztak létre egy egységet, 77-es dandár néven, melynek feladata a közösségi hálózatokon történő lélektani műveletek végrehajtása (Bányász, 2016)

A kisebb országok is fejlesztik kiberképességeiket; Irán például az urándúsítóját ért 2010-es kibertámadás után kezdte fejleszteni a Forradalmi Gárdán belül felállított katonai egységét, amely alig egy évre rá, sikeresen átvette az irányítást egy amerikai RQ-170-es pilóta nélküli lopakodó technológiájú gép felett és azt sértetlenül leszállította.

Észak-Korea szintén felállított egy kiberhadviselési egységet a hírszerzésen belül, a 121-es osztagot. Szakértők szerint az egység létszáma már elérte a 6000 főt, ebből több százan külföldön dolgoznak. Fő célpontjuk Dél-Korea, de hozzájuk kötötték a 2014-es Sony elleni támadást is, amelyet állítólag az Interjú című film miatti bosszú motivált.

Meg kell még említeni Izraelt, mely mindig is élen járt az elektronikai fejlesztésekben – hadseregük használt például először frekvenciaugratásos rádiókat – és jelenleg szakértők szerint a világ kiberbiztonsági piacának 10 százalékát tudhatja magáénak. Az Egyesült Államok mellett Izrael is részt vett a Stuxnet kifejlesztésén és bevetésén az iráni urándúsító ellen, habár ezt hivatalosan sosem ismerték el. 2016 elején jelentették be, hogy Beér-Sevában létrehoznak egy technológiai parkot, ahol magáncégek bevonásával nemzetközi kiberbiztonsági központot akarnak kialakítani. A tervek szerint 15000 ember foglalkozik majd itt IT-biztonsággal. Ide fogják áthelyezni a fegyveres erők kibervédelmi egységeit is, illetve itt kap helyet a hadsereg kiberhadviseléssel foglalkozó, most alakuló egysége is. (SG2, 2016)

Németországban 2009-ban alakult a Bonn melletti Rheinbachban lévő Tomburg-kaszárnyában egy 76 fős Információs és Számítógépes Hálózati Műveleti Részleg nevű különleges csoport a Stratégiai Felderítő Parancsnokság alárendeltségében. A részleg tagjait a Bundeswehrrel együttműködő egyetemek informatikai tanszékeiről toborozzák és a legújabb technikákat sajátítják el.

A tervek szerint képesek lesznek észrevétlenül behatolni idegen hálózatokba, ott felderítéseket végezni, információkat szerezni vagy módosítani, illetve szerverek és hálózatok elleni támadásokat végrehajtani. (SG3, 2009) Ursula von der Leyen német védelmi miniszter 2016 áprilisában jelentette be, hogy a német hadseregen belül létrehoznak egy Cyber/IT (CIT) nevű egységet, amelynek fő feladata a kiterjedt kibervédelem megszervezése lesz. A tervek szerint 2021-ig 13500 katonát és civil alkalmazottat vesznek fel az egységhez. (HVG, 2016)

Úgy gondolom, a fent említett országokon túl még jó néhány ország törekszik a kibertámadási képességek kifejlesztésével. Arra már mindenki rájött, hogy a kibervédelem nagyon fontos. Több ország – köztük hazánk is – megteremtette azt a jogszabályi hátteret, amely elősegíti a védelem megszervezését. A NATO-tagállamok nagy része már kidolgozta a kiberbiztonsági stratégiáját, ezeket meg is osztották egymással. A stratégiák nyilvánosak, a Kiber Kiválósági Központ honlapján megtekinthetők, több NATO-tagsággal nem rendelkező ország ilyen típusú dokumentumaival egyetemben. Itt megtalálhatjuk többek között Oroszország, Kína, Japán, Szaúd-Arábia, Új-Zéland, Dél-Afrika nemzeti kiberbiztonságról szóló anyagait. A nemzetközi összefogás azonban elengedhetetlen, hisz a kiberbűnözést és a kiberterrorizmust csak így lehet visszaszorítani. Ennek jegyében született nemrég két nagy horderejű bilaterális szerződés Oroszország és Kína, illetve az Egyesült Államok és Kína között.

Oroszország és Kína 2015. május 8-án írt alá egyezményt, amelyben kifejezték eltökélt szándékukat a kibertérben történő törvénytelen cselekedetek megakadályozására, a kiberbűnözés és a terrorizmus minden formájával szembeni közös fellépés szükségességéről. Megegyeztek abban, hogy nem támadják egymás rendszereit és nem támogatnak semmilyen ilyen törekvést. Rendszeresen informálják egymást a kiberfenyegetésekről és a kutatás-fejlesztés terén közös tudományos, oktatási projekteket indítanak.

Egyes elemzők a szerződés aláírása után aggodalmuknak adtak hangot, mely szerint a két ország e szerződéssel össze kívánja hangolni az Egyesült Államok elleni kibertevékenységét. Remélhetőleg ez a szerződés azonban nem erről szólt. Ezt erősíti, hogy 2015. szeptember 25-én a Fehér Házban Barack Obama amerikai és Hszi Csin-ping kínai elnök is aláírt egy kétoldalú egyezményt, melyben a felek megegyeztek, hogy felgyorsítják a rosszindulatú

támadások esetén az információáramlást és a segítségnyújtást. Egyik fél sem folytat és nem támogat tudatosan szellemi tulajdon eltulajdonítására irányuló, kibertérben végrehajtott műveleteket, amelyek célja üzleti titkok és üzleti előnyszerzésre alkalmas más bizalmas információk megszerzése, valamint javítják a kiberbűnözés elleni együttműködést.

Összefoglalás

Összefoglalásul elmondhatjuk, hogy a technológiák fejlődésével elsőrendű kérdéssé vált a kiberbiztonság témaköre. Ezt mára már minden ország felismerte és lépéseket tett ezirányban. A nemzetközi összefogás elengedhetetlen a kiberbűnözés és a terrorizmus visszaszorítása érdekében. Minden arra mutat, hogy az informatikai rendszerek egyre jobban behálózzák nemcsak a mindennapi életet, hanem a hadseregeket is. A katonai vezetésirányító rendszerek, az intelligens fegyverek mind hálózatos elven fognak működni, így biztonsági kockázatnak lesznek kitéve. Tisztában kell lennünk azzal, hogy az elkövetkezendő évek konfliktusaiban egyre nagyobb szerepet fog játszani az ellenséges országok nemcsak katonai, hanem polgári hálózatos elektronikus információkezelő rendszereinek és létfontosságú információs rendszerelemeinek támadása. Azok az országok, amelyek nem fogják ezen irányú képességeiket kialakítani, jelentős hátrányba kerülhetnek, hiszen csak a kibervédelem kialakítása nem biztos, hogy elég lesz egy konfliktusban. Ezért a jövőben számítani kell arra, hogy egyre több energiát fognak a világ államai a kibertámadó potenciáljaik növelésére fordítani. Véleményem szerint hazánkban is fel kellene állítani egy olyan egységet, amely képes a kibertérben támadó jellegű műveletek végrehajtására is. Ahogy az a fentiekben is látható volt, más országok ezeket az egységeket katonai vezetés alatt állították fel, a fegyveres erők kötelékében. Ez biztosíthatja a komplex katonai műveletekben a kiberhadviselési képességek optimális kihasználását, más műveletekkel történő összehangolását. Ezért hazánkban is a Magyar Honvédség kötelékében kellene integrálni ezt a képességet, szoros együttműködést kialakítva a kibervédelemmel foglalkozó más hazai szervezetekkel.

Felhasznált irodalom

Könyvek

MUHA L., KRASZNAY Cs. (2014) *Az elektronikus információs rendszerek biztonságának menedzselése,* NKE, Budapest

Hadtudományi Lexikon (1995), MHTT, Budapest

GREENWALD G. (2014) A Snowden-ügy, HVG Kiadó, Budapest

HAIG Zs. (2015) Információ, társadalom, biztonság, NKE, Budapest

HAIG Zs., Várhegyi I. (2005) Hadviselés az információs hadszíntéren, Zrinyi Kiadó, Budapest

Publikációk

CSERHÁTI A.: A Stuxnet vírus és az iráni atomprogram

Nukleon IV. évfolyam 1. szám Budapest 2011. p.: 85

HAIG Zs., Kovács L.: Fenyegetések a cybertérből

Nemzet és biztonság I. évfolyam, 5. szám. Budapest, 2008. pp.: 61–69

HAIG Zs.: Internet terrorizmus, *Nemzetvédelmi Egyetemi Közlemények*, XI. évfolyam, 2. szám Budapest, 2007. pp.: 81–93.

GYEBROVSZKI T.: Stuxnet – mint az első alkalmazott kiberfegyver – a Tallini Kézikönyv szabályrendszere szempontjából, *Hadmérnök* XI. évfolyam 1. szám Budapest, 2014 pp.: 164–174

JORDÁN Gy: A kínai katonai modernizáció, *Nemzet és biztonság* IV. évfolyam 2. szám. Budapest, 2011. pp.: 32–49

KOVÁCS L.: Információs hadviselés kínai módra, *Nemzet és biztonság* II. évfolyam 7. szám. Budapest, 2009. pp.: 35–44

KOVÁCS L: Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I., *Hadmérnök* VII. évfolyam 2. szám Budapest, 2012 pp.: 302–311

KOVÁCS L: Az információs terrorizmus eszköztára, *Hadmérnök különszám* Budapest, 2006. november 22.

KOVÁCS L., Sipos M.: A stuxnet és ami mögötte van, *Hadmérnök* V. évfolyam 4. szám Budapest, 2010. pp.: 163–172

KOVÁCS Z.: Védett vezetők hordozható infokommunikációs eszközeinek védelme a rádiófrekvenciás tartományban, *Bolyai Szemle* XXIII. évfolyam 4. szám Budapest, 2014. pp.: 58–77

NAGY V.: The geostrategic struggle in cyberspace between the United States, China and Russia, AARMS Vol. 11, No. 1 Budapest 2012. pp.: 13–26

BÁNYÁSZ P.: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében, *Szakmai Szemle* 2016. I. szám, Budapest pp.: 61–81

Dokumentumok

JP 1-02 Department of Defense Dictionary of Military and Associated Terms, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Tallinn Manual on the International Law Applicable to Cyber Warfare https://ccdcoe.org/tallinn-manual.html

FM 3-38 Cyber Electromagnetic Activities, http://www.fas.org/irp/doddir/army/fm3-38.pdf

Magyarország Nemzeti Kiberbiztonsági Stratégiája, http://www.mysec.hu/download/MK2013_47_M_N_Kiberbiztonsagi_Stratagiaja.pdf

Számítástechnikai Bűnözés Elleni Egyezmény, http://www.jogiforum.hu/publikaciok/50

International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World, https://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

Warsaw Summit Communiqué, http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

Internetes forrás

Internet World Stats, http://www.internetworldstats.com/stats.htm [elolvasva: 2016. február 12.]

BUSSELL, J. (1995) Cyberspace – Enciklopedia Britannica, http://www.britannica.com/topic/cyberspace [elolvasva: 2016. február 12.]

NORTON (2012) Norton Cybercrime Report, http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/assets/downloads/en-us/NCR-DataSheet.pdf [elolvasva: 2016. február 12.]

Securelist (2013) Red October" Diplomatic Cyber Attacks Investigation, https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/ [elolvasva: 2016. február 14.]

CERT (2012) Újabb taggal bővült a Stuxnet „család", http://tech.cert-hungary.hu/tech-blog/120810/ujabb-taggal-bovult-a-stuxnet-csalad, [elolvasva: 2016. február 14.]

VÁMOSI, G. (2010) *A kretének háborúja zajlott az Interneten*, http://www.origo.hu/techbazis/20101117-a-4chan-a-tumblr-ellen-a-kretenek-haboruja-zajlott-az.html [elolvasva: 2016. február 14.]

NEMES, D. (2008) *Hackerek a szcientológia ellen*, http://pcworld.hu/kozelet/hackerek-a-szcientologia-ellen-20080128.html, [elolvasva: 2016. február 14.]

RAWLINGS, N. (2013) *Anonymous Hackers Plead Guilty to PayPal Cyber Attack,* http://techland.time.com/2013/12/09/anonymous-hackers-plead-guilty-to-paypal-cyber-attack/ [elolvasva: 2016. február 14.]

DUBUIS, A. (2015) Anonymous declares war on Islamic State after Paris attacks in chilling video: ‚We will hunt you down', http://www.mirror.co.uk/news/world-news/anonymous-declares-war-islamic-state-6839030 [elolvasva: 2016. február 14.]

Anon – *Az Anonymous Operation Hungary adatlapja a Facebook-on,* https://www.facebook.com/OpHunAnon/info [elolvasva: 2016. február 14.]

HESS, P. (2009) *Levin: More e-mails from Ft. Hood suspect possible,* http://townhall.com/news/politics-elections/2009/11/21/levin_more_e-mails_from_ft_hood_suspect_possible [elolvasva: 2016. február 15.]

TIMOTHY, T. (2003) *Al Qaeda and the Internet: The Danger of "Cyberplanning"*, http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/03spring/thomas.pdf, [elolvasva: 2016. február 15.]

KETTMANN, S.: *Soviets Burned By CIA Hackers?.*, http://archive.wired.com/culture/lifestyle/news/2004/03/62806?currentPage=all, [elolvasva: 2016. február 14.]

NÉMETH J., HAJZER T. (2008): *Az orosz-grúz háború néhány jellemző vonása,* http://old.biztonsagpolitika.hu/?id=16&aid=709&title=az-orosz-gruz-haboru-nehany-jellemz337-vonasa [elolvasva: 2016. február 16.]

Magyar Nemzet Online (2016): *Visszafelé sült el Izrael fegyvere*, http://mno.hu/film/visszafele-sult-el-izrael-fegyvere-1329288, [elolvasva: 2016. március 30.]

SG1 (2015): *Izrael tagadja, hogy köze lenne a Duqu 2 kémprogramhoz*, https://sg.hu/cikkek/112940/izrael-tagadja-hogy-koze-lenne-a-duqu-2-kemprogramhoz, [elolvasva: 2016. március 30.]

BERZSENYI D., SZENTGÁLI G. (2010): *STUXNET: a virtuális háború hajnala*, http://old.biztonsagpolitika.hu/?id=16&aid=932&title=stuxnet-a-virtualis-haboru-hajnala [elolvasva: 2016. február 20.]

VÁMOSI G., SZEDLÁK Á. (2008) : *Az Interneten is zajlik az orosz-grúz összecsapás*, http://www.origo.hu/techbazis/internet/20080811-az-interneten-is-zajlik-az-oroszgruz-osszecsapas.html [elolvasva: 2016. február 20.]

LANGNER R. hamburgi vírusbiztonsági szakértő blogja 2010. december 31., http://www.langner.com/en/blog/page/13/ [elolvasva: 2016. február 20.]

FLOOK. K, (2009): Russia and the Cyber Threat, http://www.criticalthreats.org/russia/russia-and-cyber-threat, [elolvasva: 2016. február 25.]

ORBÓK, Á (2015): *Kibertér, mint hadszíntér,* http://biztonsagpolitika.hu/wp-content/uploads/2015/04/Orbok-Akos-A-kiberter-mint-hadszinter.pdf, [elolvasva: 2016. február 14.]

DoD (2010): *U.S. Department of Defense, Cyber Command Fact Sheet, 21 May 2010*, http://www.stratcom.mil/factsheets/2/Cyber_Command/, [elolvasva: 2016. március 30.]

NSA (2016): Leadership, https://www.nsa.gov/about/leadership/, [elolvasva: 2016. március 30.]

NSA2 (2016): About NSA, https://www.nsa.gov/ faqs/about-nsa-faqs.shtml, [elolvasva: 2016. március 30.]

Mandiant (2013): *APT1 Exposing One of China's Cyber Espionage Units,* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, [elolvasva: 2016. március 30.]

SG2 (2016): A Negev-sivatagban lesz Izrael kibervédelmi központja, https://sg.hu/cikkek/117093/a-negev-sivatagba-lesz-izrael-kibervedelmi-kozpontja, [elolvasva: 2016. március 30.]

SG3 (2009): Kiberháborús egységet hoz létre a Bundeswehr, https://sg.hu/cikkek/65536/kiberhaborus-egyseget-hoz-letre-a-bundeswehr, [elolvasva: 2016. március 30.]

HVG (2016): Kisvárosnyi létszámú cyberalakulatot hoz létre a német hadsereg, http://hvg.hu/vilag/20160426_Kisvarosnyi_letszamu_cyberalakulatot_hoz_letre_a_nemet_hadsereg/nyomtatas, [elolvasva: 2016. április 30.]

DR. PINTÉR ISTVÁN
(research@cgeopol.hu)

A virtuális tér geopolitikája

„Ha elveszítem a gyeplőt a sajtón,
három hónapig sem maradok hatalmon.”

(NAPÓLEON)

Absztrakt

Geopolitikai aspektusból a kibertér a gépi memóriákban meglévő adat- és információtömeg, míg a virtuális tér az emberiség memóriájában meglévő információtömeg. Aki uralja az info-kommunikációs termékek és szoftverek gyártását (kiemelten ezek standardizálását, fejlesztését), valamint az adatok továbbítását, és archiválását, az uralja a kiberteret. Aki uralja az emberek figyelmét, az uralja a virtuális teret. Aki uralja a kiberteret és a virtuális teret, az uralja a Földet.

Az infokommunikációs fejlesztések dominálta negyedik ipari forradalom talaján új bipoláris világrend alakult ki. Fő vetélytársak egyfelől a Kína-Oroszország tengely, másrészről az Amerikai Egyesült Államok vezette koalíció. Ez utóbbiban kiemelt szerepet játszanak a „Five Eyes" államok, amely együttműködés keretében Nagy-Britannia visszaszerezheti az I. világháborúban elveszített globális hatalmi szerepét.

A jövő geopolitikáját a Mesterséges Intelligencia dominálja.

Kulcsszavak: kibertér, virtuális tér, bipolaritás, geopolitika, Kína, USA, Nagy-Britannia, Oroszország, Öt szem, mesterséges intelligencia, kiber védőernyő

Abstract

From a geopolitical point of view, Cyberspace is the mass of data and information stored in the memory of machines, while Virtual Space is the mass of information in the memory of humankind. Whoever controls the production (and in particular, the standardisation and development) of information and communication technology (ITC) products and softwares, as well as the transmission and archiving of data, controls the Cyberspace. Whoever controls the attention of the people controls the Virtual Space. Whoever controls the Cyberspace and the Virtual Space controls the Earth.

On the grounds of the fourth industrial revolution dominated by the development of ITC, a new bipolar world order has emerged. The main rivals are, on the one side, the China-Russia axis, and on the other side, the coalition led by the United States of America. A special role is played in the latter by

the „Five Eyes" countries, a cooperation in the framework of which Great Britain may be able to regain its position of global power lost in World War I.

The geopolitics of the future will be dominated by Artificial Intelligence.

Key worlds: Cyberspace, Virtual Space, bipolar world, geopolitics, China, USA, Great-Britain, Russia, Five Eyes, Artificial Intelligence, cyber umbrella.

1. A geopolitika fejlődése

A geopolitika kifejezést először egy svéd geográfus, Rudolf Kjellén (1864–1922) használta a XIX. század végén. Szerinte a geopolitika olyan empirikus megközelítés, amely a földrajztudomány és a politológia közötti kapcsolatrendszeren alapul. A teret és a népet az állam tartóoszlopainak tekintette. A teret, mint „a testet" és a népet, mint a „lelket" határozta meg, de csak az előbbit tanulmányozta, mivel szerinte a második amúgy is megfoghatatlan, így meghagyva azok elemzését más tudományoknak (Kjellén, 1917).

A különböző geopolitikai iskolák képviselői közül a **német** Friedrich Ratzel (1844-1904) két tényezőre építette fel geopolitikai elméletét; ezek a tér (Raum) és a helyzet (Lage). Az ugyancsak német Karl Haushofer (1869–1946) szerint a geopolitika külön tudományág, amely a nemzetközi kapcsolatokat általában, valamint az államok, régiók, népcsoportok közötti kapcsolatokat részleteiben tanulmányozza. Haushofer tábornok szerint „A geopolitika lesz és kell, legyen az állam tudata. Ennek tárgya a mai ember alapvető kapcsolatainak a ma terében való tanulmányozása, és célja az állam térhez kötődő jelenségeinek koordinálása." Szerinte a módszertan a következő: a geopolitika a politikai passzió helyébe lép (Haushofer, 1936).

A világpolitika alakulását máig aktívan befolyásoló **angolszász** irányzatot a skót származású brit földrajztudós Halford J. Mackinder (1861–1947) alapozta meg. A földrajztudós gyakran idézett tételei szerint a földgolyón egyetlen hatalmas szárazföldi massza létezik, Európa – Ázsia – Afrika, amelyet Világszigetnek (World Island) nevezett el. Ennek központja a magterület (Heartland), amely Oroszországban található. Gyakran félreértik híres mondását, mely szerint „aki uralkodik Kelet-Európán, kormányozza a Magterületet, aki uralkodik a Magterületen, kormányozza a Világszigetet, aki uralkodik a Világszigeten, kormányozza a világot" (Mackinder, 1904).

Valójában Mackindert elsősorban nem a közvetlen földrajzi környezet és az egyes népek vagy civilizációk életformája, vagy akár politikai berendezkedése közötti lehetséges összefüggések érdekelték, hanem a földrajz áttételes hatása: az Ázsia és Európa közötti civilizációs konfliktus (Molnár, 1999).

A **francia** geopolitika megalapítója, Vidal de La Blache (1845–1918) szerint az ember éppolyan fontos „földrajzi tényező", mint a természet, de nem

annyira a külső befolyásokat elszenvedő ember, hanem inkább a „kezdeményező ember". Blache 1922-ben kidolgozta egy komplett emberföldrajz alapjait. Már 1917-ben megjelentette a „La France de l'Est" című könyvét, melyet Yves Lacoste, az első francia geopolitikai írásnak tekint. Ebben alapvetően a haza földjéről, a nemzet területéről van benne szó. Lacoste (1993) szerint „ez a kulcsfontosságú mű azt bizonyítja, hogy a földrajztudomány nem korlátozódhat kizárólag a föld tanulmányozására, hanem a nemzethez, a területhez és a határokhoz kapcsolódó kérdéseket is tárgyalnia kell, melyek maguk is a földrajz függvényei".

Az **Egyesült Államokban** az 1930-as évek során a német geopolitika nagy hatást gyakorolt.

Nicolas J. Spykman (1893–1943) egyesült államokbeli tudós a világ konfliktusait nem a tengeri és a szárazföldi hatalmak összeütközésében látta. Mackinder „külső körét" peremvidékként fogta fel. Spykman szerint két konfliktus létezik: egyrészt egy, a belső országokból álló koalíció és a tengeri hatalom között, másrészt konfliktus a tengeri hatalom és egy belső ország között.

A geopolitika fejlődése során sikerült a kezdeti földrajzi megközelítést kitágítani azzal a felismeréssel, hogy az ember éppolyan fontos földrajzi tényező, mint a természet (Blache, 1922). Ezt a felfogást csak erősítette és kiterjesztette Raymond Aron (1905–1983) „Háború és béke a nemzetek között" című munkájában, valamint Yves Lacoste (1929–), aki gyakran hivatkozik a „geopolitikai képzetekre". Azt is kihangsúlyozta, hogy a geopolitikai képzetek – a diskurzusokhoz hasonlóan – kezdetben nem egy állam vagy egy nép ügyét képezték, hanem azon személyiségekét, kis csoportokét, akik megfogalmazták vagy egyszerűen kitalálták őket. Még ha ezt követően az ügyet a nemzet nagy többsége hirdeti és el is fogadja, legelőször a politikusok (vagy tanácsadóik) ügye és az értelmiségieké – gyakran geográfusok vagy történészek –, akik annak a bizonyos államnak vagy kulturális csoportnak az érdekein kívül saját látásmódjuknak is hangot adnak (Lacoste, 1993). Véleménye szerint ezért a hatalmi rivalizációk elemzése során figyelembe kell venni a vezetők és főnökök személyes szerepét, a személyiségüket, illetve rögeszméik szerepét a stratégiák kiválasztásában vagy elvetésében. Elsőként vizsgálta a nemzetközi tényezők, illetve a média által világszinten terjesztett bizonyos képzetek és téveszmék szerepét is.

A geopolitikai elemzéseknél sokáig hiányzott a *kultúra* figyelembevétele. Ezt csak részben oldotta Vidal de La Blache emberföldrajzi felfogása, még akkor is, ha külön figyelmet szentelt az államok közötti kapcsolatoknak és információáramlásnak. A kulturális tényező elhanyagolása az Európa-centrikus gondolkodóknál a civilizáció mibenlétével kapcsolatos polémiára vezethető vissza.

> „A civilizáció a legtágabb kulturális entitás. A civilizáció ideálját a XVIII. század francia gondolkodói dolgozták ki, mégpedig a „barbárság" ellentéteként. A civilizált társadalom ennek megfelelően különbözött a primitív társadalomtól, mert megállapodott, urbánus és művelt volt. Civilizáltnak lenni jó volt, civilizálatlannak lenni rossz. A civilizáció eszméje a társadalmak megítélésére alkalmas normával szolgált, és a XIX. század folyamán az európaiak diplomáciai és politikai energiát szenteltek azon ismérvek kidolgozására, melyek alapján a nem európai társadalmakról meg lehetett ítélni, vajon eléggé »civilizáltak-e« ahhoz, hogy elfogadtassanak az európai dominanciájú nemzetközi rendszer tagjaként.
>
> Ugyanakkor az emberek egyre gyakrabban beszéltek a civilizációkról, így, többes számban. Ez szembefordulás volt azzal a feltevéssel, hogy létezne egyetlenegy mérce, mely – Braudel megfogalmazása szerint – »néhány kiváltságos népre vagy csoportra, az emberiség elitjére« korlátozná a civilizáció fogalmát. Immár több civilizációról volt szó, melyek mindegyike a maga módján mondható civilizáltnak." (Huntington, 1996)

Huntington ezen a helyen külön elemezte Németországot, ugyanis „a XIX. századi német gondolkodók élesen különválasztották magát a civilizációt, mely tartalmazza a műszaki, technikai és az anyagi tényezőket, valamint a kultúrát, amelybe az értékek, az eszmények és a társadalom magas intellektuális szintet képviselő művészi, morális sajátosságai tartoznak."

Szerinte valójában „a civilizációt meghatározó elemeket klasszikus formában az athéniak fogalmazták meg, mely szerint *a görögökben a vérség, a nyelv, a vallás és az életmód* volt közös."

A geopolitikai gondolkodásmód történeti fejlődésében az államtól mint kizárólagos tényezőtől eljutottak a *heterogén szereplők* figyelembe vételéig.

Az egyének, a közösségek és a nem etatikus intézmények (mint pl. az egyház) kezdetektől fogva befolyásolták a nemzetközi viszonyokat. „A XX. század végi korszak sajátossága a különböző fejlődési folyamatok felhalmozódásában áll: a határok megnyitása és az állam ellenőrzési mechanizmusának gyengülése, a nemzetközi környezet meghatározó súlya a nagyvállalatokra és a hatalmas gazdasági szektorokra. Kollektív, sőt egyéni szereplők váltak a piac, és legfőképpen a pénzpiac meghatározó szereplőjévé." (Moreau Defarges, 1994)

Az újra reneszánszát élő geopolitikai gondolkodásmód egyre szabatosabban tárja fel a hatalom, az erő, a nemzetközi kapcsolatok és a konfliktusok különböző szintjeit. Foglalkozik a legújabb folyamatok elemzésével, melyet Yves Lacoste (1993) már a sajtó szerepének felismerésével, valamint az egyén és az egyéni percepció hangsúlyozásával jelzett.

Időközben két generációja is felnőtt a geopolitikusoknak. Senkit nem megsértve megemlítjük az angolszász geopolitikai iskolából Zbigniew Brzezinsky, Samuls P. Huntington és Colin S. Gray, a német geopolitikai iskolából Heinz Brill, míg a francia iskolából Frédérick Douzet, Alix Desforges, Aymeric Chauprade és Stéphane Rosiere neveit. A Geopolitikai Tanulmányok Genfi Intézetéből (GIGS) pedig Csurgai Gyula, David Criekemans és Alexandre Vautravers munkássága érdemel figyelmet.

2. A technikai fejlődés és a tér

A pattintott dárdahegy felfedezésétől, a bronz- és vasmegmunkáláson keresztül az ipari forradalmak korszakáig az emberiség története a technikai fejlődés története. A Homo Sapiens találékonyságával, újításaival folyamatosan vette birtokba a rendelkezésére álló teret. Az innovációk révén hódította meg a szárazföldet, a virtuális teret, a levegőt, a világűrt, majd a kiberteret.

A korszakalkotó újítások, például amelyek egy új energia felhasználását tették lehetővé, forradalmasították az akkori termelést, és ugrásszerű fejlődést eredményeztek. Más technikai újítások a térben való mozgás lehetőségét növelték meg, azokat tették biztonságosabbá és gyorsabbá.

Mindezek a célok, következmények a jelen kor viszonyai között is fennállnak.

Számos nagyszerű újítás ugyanakkor a katonai fejlesztésekhez kötődik. Az ember természetéből fakadó felfedezési vágy, amellyel előbb a szárazföldet, később a tengert, majd a légteret is meghódította, erőteljes birtoklási vággyal párosul. A technikai fejlődést már a kezdetekben is jelentősen motiválta a területszerzési igény, mások legyőzése, amely genetikailag a fajfennmaradási ösztönökből vezethetők le. A kereket személy- és áruszállító szekérhez ugyanúgy fel lehetett használni, mint a harci szekerek készítéséhez. Az önvédelemhez, illetve az élelem megszerzéséhez szükséges dárdákból hamar kifejlődött az íj, majd azok a szerkezetek – lásd az ókori tudósok vagy Leonardo da Vinci találmányai –, amelyek a harcmezőn voltak használatosak. Az ember védekezésképpen lakóhelyét előbb fából és földből épült, majd kőből készült falakkal vette körül, míg más emberek elkészítették a faltörő kost, a hajítógépet, később a puskapor feltalálását követően az ágyút.

2.1. A geopolitikai terek birtokba vétele

Egyes gondolkodók szerint a fejlődés első hullámát a mezőgazdaság forradalma jelentette, amely mintegy 9000 évvel ezelőtt kezdődött (Toffler, 1980). Amikor az ember csak a **szárazföldet** birtokolta, a kerék feltalálása volt az egyik kiemelkedő momentum, amellyel megkönnyítette, megváltoztatta a saját életét. Amikor a szekér elé egy háziasított lovat fogott, a saját erejét sokszorozta meg.

Ahogy az emberiség meghódította a szárazföldet, hamar rájött arra, hogy a **tenger** is bővelkedik élelemforrásokban. A tengerek meghódítását szintén felvázolhatjuk technikai újításokkal, a csónak, a bárka tervezése, építése külön iparágat hozott létre. A vitorla felhasználásával az emberiség már egészen korán használatba fogta a szélenergiát, ennek fejlődése mind a mai napig folyamatos. Ugyanakkor csak kevesen emlékeznek arra, hogy a nagyméretű hajók elterjedését egy olyan technikai újítás alapozta meg, mint a szélmalmokra épült deszkavágó gép feltalálása. Míg korábban a fatörzsekből a hajóépítéshez szükséges deszkákat kézzel faragták ki, ami jelentős mértékű forgácsmennyiséggel járt, a Hollandiában feltalált deszkavágó gép megsokszorozta a minimális veszteséggel legyártható hajódeszkák mennyiségét. Ez az újítás tette lehetővé egy teljesen új iparág felvirágzását, előbb a hadihajók, majd a kereskedelmi hajók számának rohamos növekedését, világméretű elterjedésüket. A tengerek meghódításánál is szerepet játszottak az újfajta

erőforrások, elsősorban az ipari forradalomhoz köthető gőzgép, majd a Dieselmotor feltalálása és elterjedése.

Mivel a **virtuális tér**, a jelen tanulmányban alkalmazott definíciója szerint nem más, mint az „az emberiség memóriájában meglévő információtömeg" (Pintér, 2009), tehát keletkezése az ember öntudatra ébredéséhez köthető. Az egyes ember tudata nagyban függ a közvetlen észlelésektől (az érzékszervek útján: látás, hallás, tapintás, ízlelés, szaglás), valamint az őt körülvevők kommunikációjától. Már a barlangrajzoktól kezdve az ember törekszik a képszerűségre, miközben hajlamos a misztikumra.

Toffler (1980) szerint „Emlékeink feloszthatók a tisztán személyes (magánjellegű) és a közös (társadalmi) emlékek csoportjaira. A magánjellegű emlékek meghalnak az egyénnel. A társadalmi emlékezet tovább él. Fajunk evolúciós sikerének titka az a figyelemreméltó képesség, hogy elraktározzuk és visszanyerjük a közös emlékeket. És ennél fogva bármi, ami jelentősen megváltoztatja azt a módot, ahogyan társadalmi emlékezetet felépítjük, raktározzuk és használjuk, sorsunk alakulásának alapvető forrásait érinti.

A történelem során az emberiség már kétszer forradalmasította társadalmi emlékezetét. Ma az új infoszféra kiépítésével egy újabb, hasonló mélységű átalakulás közepére érkeztünk.

Kezdetben az emberek csoportjai kénytelenek voltak a közös emlékeket ugyanott tárolni, ahol az egyéni emlékeket, vagyis az egyes személyek agyában. Ezeket az emlékeket a törzsek vénei, a bölcsek és más emberek hordozták magukban történetek, mítoszok, tanítások és legendák formájában, és átadták gyermekeiknek beszéd, énekszó és példamutatás útján. Hogyan kell tüzet gyújtani, mi a legjobb módszer a madárfogásra, hogyan kell egy tutaj gerendáit összekötözni vagy a tárógyökeret puhítani, hogyan kell az ekét élesíteni vagy az ökröket gondozni – a csoport minden összegyűjtött tapasztalatát az emberi lények idegsejtjeiben, speciális agyi szöveteiben és szinapszisaiban tárolták.

Mindaddig, amíg ez igaz maradt, a társadalmi emlékezet kiterjedése szigorúan korlátozott volt. Akármilyen jó volt az öregek memóriája, s bármilyen könnyen megjegyezhetők voltak a dalok vagy a leckék – mindössze ennyi raktározási hely volt egy-egy népesség koponyáiban.

A második hullám (az ipari forradalmak kora – a szerk.) civilizációja eltörölte a memória korlátait. Elterjesztette a tömeges írni-olvasni tudást. Rendszeres

üzleti feljegyzéseket vezetett. Könyvtárak és múzeumok ezreit építette fel. Feltalálta az iratrendező szekrényt. Vagyis a társadalmi emlékezetet kivette a fejekből, új módszereket talált annak tárolására, és így korábbi határain jóval túlra terjesztette ki. Az összeadódott tudás raktárkészletének növelésével felgyorsította az innováció és a társadalmi változás minden folyamatát, biztosítva a második hullám civilizációjának a leggyorsabban változó és fejlődő kultúrát, amit a világ addig ismert.

Ma ismét azon a ponton vagyunk, hogy a társadalmi emlékezet teljesen új szintjére ugorjunk. A média radikális demasszifikálása, az új médiumok bevezetése, a Föld műholdakról való feltérképezése, a kórházi betegek állapotának elektronikus érzékelők útján való nyomon követése, a vállalatok iratállományának számítógépre vitele – mindez azt jelenti, hogy a civilizáció tevékenységeit a legfinomabb részletességgel rögzítjük. Ha csak el nem hamvasztjuk bolygónkat, társadalmi emlékezetünkkel együtt, rövid időn belül igen közel jutunk egy totális emlékezetű civilizáció kialakulásához. A harmadik hullám civilizációjának több információ – és sokkal árnyaltabban szervezett információ – fog rendelkezésére állni önmagáról, mint azt akár csak egy negyedszázaddal ezelőtt is el lehetett képzelni."

A virtuális tér fejlődése megegyezik az emberiség fejlődésével, bár a korai időkre jellemző volt az egyszer már felfedezett ismeret feledésbe merülése. Kiemelendő a beszéd, majd az írás kifejlődése, az azokat rögzítő technikai találmányok, mint az égetett agyagtáblák, a papirusz illetve a papír feltalálása. Az íráson belül is a kép-, és ékírás, majd a ma is elsősorban használatos betűírás elterjedése, a vallás és a kultúra megjelenése. Meghatározó csomópont a tudás tárolására használatos kézírásos kódexek meghaladása a Gutenberg-féle könyvnyomtatással. Ennek következményei – a jóval árnyaltabb kifejezésmódot lehetővé tevő beszéd háttérbe szorulása, az információ olcsóvá és tömegessé válása, az olvasóközönség atomizálása – máig hatnak. A fejlődést az ipari forradalmak találmányai gyorsították, gyorsítják meg: a gőzgépre alapozott betűszedőgép tette lehetővé az újságok, magazinok kiadását és elterjedését, majd elérkezett az elektromosság feltalálása utáni időszak. Történelmi léptékben gyors egymás után következett a távíró, a távbeszélő és a távolba látó készülékek feltalálása, majd az ezek használatát könnyebbé tévő, vagy hordozható változatainak kidolgozása (telefonközpont, tranzisztoros rádió, hordoz-

ható színes TV stb.). A folyamat ma is egyre gyorsul, az e-könyv helyett a Q generáció már az okostelefont használja elsődleges információforrásnak.

Az emberiség régi vágya a repülés, a **légtér** meghódítása. Az ógörög Ikarosz története már bizonyíték arra, hogyan gondolkodtak a levegő meghódításáról, bár a történetíró akkor még nem sejthette, hogy minél magasabbra száll az ember, annál hidegebb van, így a Naphoz való látszólagos közeledés nem okozza a szárnyak megolvadását. Leonardo da Vinci számos rajzában megtalálhatók olyan szerkezetek tervei, amelyek a levegő meghódítására készültek. Végül is az egyesült államokbeli Wright fivérek jutottak el a megvalósításig. Feltalálták azt a szárnyprofilt, amely – megfelelő sebességgel haladva – elegendő felhajtóerőt jelent ahhoz, hogy az egyébként a levegőnél súlyosabb tárgyak repülhessenek. A sikerhez szükséges volt egy olyan kisméretű benzinmotor feltalálása, amely a légcsavar segítségével biztosítja a szükséges sebességet a felszálláshoz.

A döntő találmány megszületése után egyenes út volt a nagyobb méretű és gyorsabb repülők kifejlesztéséig. Egy sor technikai újításnak kellett bekövetkeznie olyan új anyagok feltalálásával (például az alumínium), és ipari méretű előállításának kidolgozásával, amelyek egyre könnyebbé és szilárdabbá tették a repülők szerkezetét. Kezdetben itt is a katonai felhasználás dominált, bár az első repülőgép-hálózatok az információhoz kötődtek. Olyan postahálózatokat alakítottak ki, amelyek hamarosan már a tengereken átnyúlva is információk gyors továbbítására voltak alkalmasak. Sajnos a levegőbe való emelkedés képességét az emberiség az I. világháborútól kezdve előbb a légi felderítéshez, majd bombák levegőből való ledobásához használta fel.

A következő nagy lépés a **világűr** meghódítása volt, amely ma is folytatódik. Ahhoz, hogy az emberiség kilépjen a világűrbe, és ma már bolygóközi utazásokat tervezzen, a legelső lépéseket azok a tudósok, feltalálók tették meg, akik újfajta rakétatesteket, újfajta rakétahajtó anyagokat, hajtóműveket, navigáló és életfenntartó eszközöket terveztek. Ezen II. világháborús hadi eszközök továbbfejlesztése tette lehetővé, hogy a Szovjetunió Föld körüli pályára bocsássa fel az első műholdat, majd Lajka kutyát is a világűrbe küldve, előre vetítse az ember űrutazását. Az adott történelmi kor bipoláris szembenállása ugyanakkor ezen fejlesztésekre alapozódva erőteljes fegyverszerzési versenyt indukált. A Szovjetunió és az Egyesült Államok erőforrásaikat nem kímélve

tettek erőfeszítéseket az interkontinentális ballisztikus rakéták kifejlesztésére, a megfigyelő és elhárító műholdak világűrbe juttatására, majd mindezeket kombinálva az atom- és hidrogénfegyver kifejlesztésével a kipusztulás szélére sodorták a Földet. Csak csekély vigaszt jelentett egy olyan momentum, mint az ember Holdra való lépése.

A bipoláris szembenállás megszűnésével ezek az erőfeszítések egyre inkább a polgári felhasználás irányába tolódtak. A műholdakat a katonai felhasználás után kommunikációs célra kezdték alkalmazni. Ennek következtében kialakult egy olyan világméretű rendszer, amellyel az információt a világűrből egyenesen a családok tévéképernyőjére lehet sugározni. Mint minden olyan technikai találmány, amely tömeges méretekben terjed el, természetesen ez is számtalan társadalmi hatással is jár. Nemcsak az emberiség, hanem az egyes ember élete is teljesen átalakult és folyamatosan alakulóban van. Ez a folyamatos változás igaz az emberek egymás közötti viszonyaira, az emberi közösségek kialakulására, újrarendeződésére, működésére is. Ma az emberiség már bolygóközi utazást tervez, rendelkezésére áll az az újfajta űrhajómotor, amely a bolygóközi térben áramló részecskék felhasználásával nagy távolságokat lehetővé tevő utazásokat tesz lehetővé. Eközben elértük a Jupitert, és leszálltunk a 67P/Csurjumov-Geraszimenkó üstökösre.

Egy újabb nagy ugrást jelentett az emberiség fejlődésében a számítógépek feltalálása és kifejlesztése. Ehhez jelentős mértékben járult hozzá a magyar Neumann János, aki elméleti megalapozását adta a ma is használatos számítógépes rendszereknek. Itt is jellemző az a fejlődési ív, amely a szűk körű katonai alkalmazásoktól néhány évtized alatt a háztartásokban is használatos személyi számítógépekig terjedt A számítógépek tették lehetővé azt, hogy azokat egymással összekötve (akár kábelen, akár műholdakon keresztül) egy újabb globális hálózat alakuljon ki. Ez a hálózat nemcsak a kommunikáció továbbításának gyorsaságát növeli, hanem megfelelő tárolókapacitásokkal összekötve egy újfajta teret alakít ki, melyet **kibertérnek** neveztek el. A földrajzi távolságok megszűntek, amikor a Föld bármely részén a szobája számítógépénél ülő egyén közvetlenül kommunikálni tud a világ bármely más részén lévő társával. *A kibertér az első olyan geopolitikai tér, amelyet nem a természet hozott létre, hanem az emberi kreativitás eredménye* (pontos meghatározásának nehézségeiről lásd a 3. fejezetet).

A számítógépek fejlődése mind a méretüket, mind a gyorsaságukat tekintve robbanásszerű volt az utóbbi évtizedekben, amely egy újabb ipari forradalmat jelentett, és további ipari forradalmak előfutára, illetőleg megalapozója. Ilyen forradalomnak tekinthető a miniatürizálás, illetve a mobilitás forradalma, amelynek kézzelfogható eredménye az okostelefonoknak nevezett mobilszámítógépek és azok lehetőségeinek globális hálózatban történő alkalmazása.

2.2. Az ipari forradalmak kora

Sokan az ipari forradalmat az ipari találmányokkal azonosítják, holott valójában több tényező egymásra hatásával alakult át a XVIII–XIX. századi Anglia. Nem kétséges, hogy ekkor a gőz erejének munkára fogásával az ember olyan új, hatékony erőforráshoz jutott, amely átalakította az egész termelést. A gőzgéptől hamar eljutottunk a vasút feltalálásáig, a vasúthálózatok kiépítéséig. Ezek a találmányok nemcsak, hogy megkönnyítették az emberek mozgását, lehetővé tették áruk nagy távolságokra való szállítását, de az egyik helyről a másikra való eljutáshoz szükséges időt is lerövidítették.

A technikai fejlődés nagyban kiterjesztette az emberiség uralmát a szárazföld és a tengerek felett, de ennek eléréséhez a találmányokon kívül szükség volt még valami másra is. Kialakult a tudati feltétel; ekkor vált általánossá a *tőkés gondolkodásmód,* amely mindent a haszon és a profitszerzés szempontjából ítélt meg.

Az eredeti tőkefelhalmozás és a szabadversenyes kapitalizmus fogalmai gyakran elfedik a valóságot: a falusi közösségek jogellenes megfosztását a közösségi földektől, ezzel a lakosság nagyobb részét földönfutóvá téve. A városokba özönlő nincstelenek éhbérért való foglalkoztatását, élelmiszer-tolvajlás esetén kötél általi kivégzésüket. A gyarmatosítás során a szabad népek rabszolgasorba való züllesztését, a korrupció elterjesztését.

A technikai fejlődésen kívül három tényező érdemel kiemelt figyelmet:

- hatékony nemzetközi hálózatok alakultak ki a kereskedelem terén;
- a kizsákmányolással, kifosztással felhalmozott tőkét fejlett hitelszervezeti (bankok, takarékpénztárok) és biztosítási tevékenység egészítette ki;
- új jogrendszer alakult ki, mivel a polgári forradalom korai győzelme

(1640) elhárított minden akadályt a tőkés fejlődés elől. Az új politikai berendezkedés gyorsan meghozta a számára előnyös jogszabályokat, melyek közül kiemelkedik az 1624-es *szabadalmi törvény*. Ez anyagilag tette érdekeltté a feltalálókat találmányaik szabadalmaztatásában, egyben meghatározott ideig kizárólagosságot biztosított a számukra. Ez a védettségi idő látszólag rossz, hiszen monopóliumot teremt az innovációk terén, amikor meghatározott ideig a szabadalmi oltalmat megszerzett fél dönt vagy saját maga használhatja a találmányát vagy hasznosításba adhatja. Valójában az anyagi érdekeltség meghatározott ideig való biztosítása egyrészről hatalmas emberi, szellemi tőkéket szabadított fel, másrészről biztonságosabbá és kockázatmentesebbé tette a befektetéseket, nagyobb volt a valószínűsége a megtérülésnek, mint azelőtt.

A pénz mindenhatóvá válásával kialakult a ma is ismert kapitalizmus. A profit maximalizálását a tőkések egy része a technikai fejlesztések bevezetésével, a találmányok hasznosításával és a tömegtermelés racionális megszervezésével igyekeztek elérni. Mások ezt erőfölénnyel, csalással, hazai és gyarmati politikusok megvesztegetésével vagy éppen a gyerek- és női munkaerő barbár kihasználásával érték el.

1871 és 1914 között következett be a második ipari forradalomnak nevezett időszak.

Ez a számozás csak Angliára és az Amerikai Egyesült Államokra igaz, hiszen a többi országban ez volt az első ipari forradalom. Az I. világháborúig eltelt időben demográfiai, társadalmi, strukturális és urbanizációs paradigmaváltás is lezajlott. Több lényeges folyamat zajlott egyszerre; például új anyagok kifejlesztése, előállításának kidolgozása, új energia- és erőforrások hasznosítása, valamint a gépesítés és a munkaszervezés új formáinak bevezetése. Találmányok sokasága született a vegyészetben, az elektromosságban, az acéliparban és az olajiparban egyaránt. Az árucikkek tömegtermelése fejlődésnek indult, a lakosság alapvető szükségletein kívül a közlekedés, a korai rádiók és gramofonok előállítása emelkedett. Erre a korra jellemző az ún. harmadik szektor, a szolgáltatóipar megjelenése és előretörése. Anglia egy kissé háttérbe szorult, annak ellenére, hogy katonai stratégiája megfelelő flotta kiépítésével a világtengerek uralmát tűzte ki célul. Vele egy sorban lehet

említeni az új és növekvő hatalmú Németországot és az Amerikai Egyesült Államokat.

Európa ekkor virágkorát éli, létrejön a német és olasz egység, Ausztria kiegyezik Magyarországgal és sikerre vezetik az Osztrák-Magyar Monarchiát. Oroszországban II. és III. Sándor gazdasági reformokat vezet be, III. Napóleon liberális reformjai sok tekintetben előremutatóak voltak. A későbbi tengelyhatalmak országai felismerték, hogy az ipari találmányok átvételével és továbbfejlesztésével versenyelőnyre tehetnek szert. Mivel nem álltak rendelkezésükre gyarmatok, amelyeknek nyersanyagforrásait és piacait felhasználva erős nemzetközi kereskedelmet tudtak volna kiépíteni, ezért hiányzott náluk az eredeti tőkefelhalmozás korszaka. Ezt erős bankrendszer kiépítésével pótolták, nem sokkal a német egység létrejötte után már öt jelentős bank létezett: Deutsche Bank, Handelbank, CreditAnstalt, Wiener Bank, Kereskedelmi és Hitelbank.

A nemzetközi specializálódásnak megfelelően Magyarországon az élelmiszeripari, az elektromos berendezések gyártása (Siemens, Ganz, Láng) és a vasúti gépgyártás fejlődött az átlagot meghaladóan. A belsőégésű motorok fejlesztésében a magyarok is élen jártak (mint Csonka János), de az egész ipart forradalmasító futószalag-rendszerű tömeggyártás az amerikai Ford Autógyárban valósult meg (1898-tól). A híres T-modell tervezőmunkáinak oroszlánrészét a magyar származású Galamb József és Farkas Jenő végezte. Déri Miksa, Bláthy Ottó, Zipernowsky Károly kidolgozták a transzformátort, Jedlik Ányos bencés szerzetes találta fel a dinamót. Ez még akkor is igaz, ha a szabadalmi oltalomra való igényt más hamarabb nyújtotta be. Az első kormányozható léghajó, a német Zeppelin után az amerikai Wright testvérek megalkották a repülőgépet. Jellemző folyamat volt ugyanakkor a monopóliumok kialakulása amikor a nagyobb vállalatok bekebelezték a kisebbeket. Maguk a nagyvállalatok még tovább koncentrálódtak. Konszernek, kartellek, szindikátusok és trösztök jöttek létre.

A fejlődéshez döntő mértékben járult hozzá az a 43 békeév, amely a poroszfrancia háború és az I. világháború között telt el. Ezt csak rövid időre szakította meg az 1873. évi nemzetközi méretű válság. A legszembetűnőbb jelenség az volt, hogy Nagy-Britannia fokozatosan elveszítette az ipari vezető szerepét és helyét a korábbi gyarmata, az Amerikai Egyesült Államok foglalta el.

Az új energiaforrások két legfontosabbika az elektromosság és a kőolaj volt. A technikai fejlődés éppen a 19. század közepén tette lehetővé mindkét energia gyakorlati alkalmazását. Ha eleinte nem is, de az 1888-as évektől kezdve mindkét energiaforrás fokozódó mértékben alakította át az ipari forradalmat a maga képére. Az elektromosság először a vasutak felszerelésében, majd a távírótechnikában jelentkezett, a mindennapi életben, a városi közlekedésben, a lakások energiaellátásában, majd később a motorok működtetésében inkább a 19. század végén jutott fokozatosan növekvő szerephez. Ettől kezdve még gyorsabban alakította át a közlekedést (villamos, villanyvonat), a kohászatot, s jelent meg a vegyiparban, majd a gépiparban, általában az ipari termelésben. A kőolaj pedig meghatározó szerepet, a robbanómotor megjelenésével, alapvetően a közlekedésben kapott. A 19. század végén rohamosan meginduló autóforgalom, a motorkerékpár, a teherautó s az autóbusz megjelenése gyorsan átalakította a közlekedést. Új utakat építettek, új megoldásokat alakítottak ki a városi közvilágításban, a lakások világításában. Az autó elterjedésével megszületett az ipari forradalom harmadik hullámának új húzóágazata, amely legalább akkora vonzerőt gyakorolt az egész termelési folyamatra, mint korábban a vasútépítés. Az autógyártás a gépipar szinte teljes egészét befolyásolta, új ágazatokat fejlesztett ki, jelentősen átalakította az infrastruktúrát, s nem utolsósorban nagymértékben befolyásolta az ipari termelés üzemi módszereit. Hatással volt a fémfeldolgozásra, az acélöntésre és a vegyiparra. A kaucsuk- majd a műgumigyártás kifejlődése érintette ez utóbbit, amiként a kőolaj feldolgozása is jelentősen hozzájárult a vegyipar fejlődéséhez. A vegyipar új területeket nyitott a műtrágya- és a festékgyártásban, s a kőolaj mellett a barnaszén felhasználásával. A 19. század végén lehetővé vált a vízi energia átalakítása villamos energiává ipari méretekben, s ez a jelzett iparágakat kivétel nélkül átformálta. A drót nélküli távíró, majd az első világháború után a rádió, új lehetőségeket nyitott a hírközlésben, a telefon, a hangrögzítés (gramofon) mellett a fototechnika is átalakult, megjelent a mozgókép, a film."

(http://tudasbazis.sulinet.hu/hu/tarsadalomtudomanyok/tortenelem/az-ujkor-1492-1914/a-feltartoztathatatlan-iparosodas/az-ipari-forradalom-ujszakaszai, Utolsó letöltés: 2016.08.14.)

Napjaink **4. ipari forradalma** középpontjában a rendszereknek az a képessége áll, hogy „gyártási (működési) eseményeket tudnak rögzíteni, felismeréseket

levezetni, s ennek alapján meg tudják változtatni saját működésüket. Célunk, hogy a nagy mennyiségben keletkezett működést leíró adatok tárolása és elemzése után tapasztalatok szerzésére és következtetések levonására alkalmas információkat állítsunk elő, azaz a „zaj jellegű adattömegből" értékes információ keletkezzen. A jövő intelligens gyáraiban a megosztott és összekapcsolt létesítmények sikeres megvalósításának legfontosabb tényezőit az intelligens gyártási rendszerek és folyamatok, valamint a célszerű műszaki tervezési módszerek és eszközök fogják alkotni." (http://industry4.hu/hu/, Utolsó letöltés: 2016. 08. 12.)

2.3. Technikai fejlődés a bipoláris szembenállás idején

A második nagy világégés mérhetetlen károkat okozott mind emberéletben, mind anyagiakban. Megerősítette ugyanakkor az I. világháború geopolitikai átrendeződését: az Amerikai Egyesült Államok globális hatalommá válását, Nagy-Britannia és vele egész Európa meggyengülését, a romokban lévő Szovjetunió befolyási övezetének kitolását egészen Berlin központjáig.

Ismét a katonai fejlesztések kerültek előtérbe. A háború végére került kifejlesztésre az atombomba, amely később új energiaforrást jelentett. A repülőgépipar, a harckocsigyártás, a fegyveripar ugrásszerű fejlődésen ment keresztül, de Németországnak a nyersanyag-forrásoktól való elszigetelése miatt a kémiai találmányok és eljárások (pl.: műbenzin) is fejlődtek. Ekkor dolgozták ki a rakéta technika alapjait, amely később elvezetett a holdraszállásig. Ne feledjük, hogy maga a számítógép és annak hálózatba kötése is katonai igényeket volt hivatva kielégíteni.

Az Amerikai Egyesült Államok és a Szovjetunió szembenállása a Föld bipoláris megosztottságához vezetett. A szövetségi rendszerek közül a Varsói Szerződés tagállamai elsősorban a katonai fejlesztések terén, míg a NATO-tagállamok mind a technikai, mind a gazdasági, társadalmi és politikai területen is versenyképesek voltak. Ez utóbbiakban való lemaradását a Szovjetunió egy olyan ideológiával pótolta, amellyel igyekezett a kapitalizmus pénz- és profitcentrikusságát elkerülni, a társadalmakat pedig egy távolabbi közös cél érdekében mozgósítani. A hidegháborút (más szerzők szerint a harmadik világháborút) az Egyesült Államok nyerte. Mindeközben az emberiség belépett az atomkorba, meghódította a Föld közeli világűrt, és olyan globális

hálózatokat épített ki, mint a műsorszóró műholdak vagy a tengeri szállítás hálózata. A nyugat globalizálta a híráramlást, a pénzügyeket és kulturális termékeivel monopol helyzetre törekedett. A számítógép rendkívüli fejlődésnek indult, mind a teljesítmény, mind az energia-felhasználás, mind a miniatürizálás terén.

Az, hogy a szocialista világrendszer ilyen hosszan (1945–1989) fenn tudott maradni, nem kizárólag a II. világháborút lezáró nagyhatalmi megállapodásoknak, hanem a társadalmak információktól való elzárásának is köszönhető volt. Vizsgáljuk meg ennek technikai hátterét:

2.4. A technika hatása a politikai berendezkedésre

Nem kétséges, hogy ez a hatás az idők kezdete óta érvényesül. Az ókori népek a háborús állapotokat tekintették állandónak, és a békét kivételesnek. Folyamatosan területszerző háborúkat folytattak, melyek kimenetele közvetlenül függött nemcsak az emberi tényező felkészültségétől, hanem azoktól a hadieszközöktől (fegyverek, hadihajók), melyek eldönthették egy-egy csata sorsát. A technikának azonban nemcsak ilyen közvetlen hatása létezik a politikai berendezkedésre, hanem léteznek közvetett hatások is. Amennyiben egy ország vagy nép előnybe kerül az innovációban, az iparát, mezőgazdaságát hatékonyabban tudja működtetni, az előnybe kerül a többiekkel szemben. A gazdasági alapokra ezután hatékonyabb államigazgatás építhető fel, amely az adott állam polgárainak jólétében mutatkozhat meg.

A technika és a politikai berendezkedés közötti kapcsolat azonban ennél szorosabb. A számítógépek elterjedésével, a kommunikáció felgyorsulásával, a televízió és az okostelefonok tömeges méretű elterjedésével megváltozik a politikai berendezkedés. Több szerző felhívta már a figyelmet arra, hogy az ellenőrizetlen információáramlás nem kívánt és nem szándékolt társadalmi változásokhoz vezethet.

Most nézzünk egy olyan példát, amely megmutatja, hogy a technika és annak standardizációja milyen szerepet játszott a bipoláris világrend fenntartásában és a Szovjetunió összeomlásában. Ahhoz, hogy a II. világháború végén kialakított nagyhatalmi rendet meg lehessen őrizni, a népeket és a nemzeteket a Szovjetunió oldalán lehessen tartani, el kellett őket zárni a nyugati világról érkező minden információtól, és helyettesíteni kellett manipulált,

az ideológiai szembenállásnak megfelelő, az állampártok – végső soron a Szovjetunió Kommunista Pártja – által gondosan kidolgozott információtartalommal.

Az információtól való elzárás alapját a határok hermetikus lezárása jelentette. A II. világháború előtti szabad, persze az anyagi lehetőségektől függő, utazás megszűnt, nyugatról csak vízum kiadása után lehetett a Varsói Szerződés tagállamaiba beutazni. A keletről nyugatra való utazás csak kivételes esetben és elsősorban a kiváltságos kommunista elithez kötődőknek volt engedélyezve. A határellenőrzés igen szigorú volt, propaganda anyagnak minősülő újságok bevitelét tiltották. A nyugati sajtóhoz csak az állampárt legfelsőbb rétege és a nyugatiakat fogadó szállodák férhettek hozzá; ez utóbbiak tiltott területnek minősültek a hazai állampolgárok számára, és erős belbiztonsági ellenőrzés alatt álltak. Szállodaigazgató is csak az állampárt által kinevezett személy lehetett, maga a pozíció szerepelt az úgynevezett „nómenklatúra listán".

A politikai rendszer fenntartásához a nyugati világ információitól való elzárás alapvető volt. Ezzel szemben a technika fejlődése már a II. világháború után létrehozta a rádióhullámokon keresztül történő információközvetítést, már léteztek rádióállomások, amelyek képesek voltak a lezárt határ túloldalán lévő embereket elérni. Ugyanakkor létezett az a nagyhatalmi politikai akarat, hogy a status quo-t technikai eszközökkel is fenntartsa. Az ENSZ keretében nemzetközi rádióforgalmi egyezmények születtek, megalakult az ITU, amely koordinációs szerepet töltött be a rádiózásra alkalmas és más frekvenciákat illetően. A nemzetközi egyezmény felosztotta a frekvenciákat, így a határokon való átsugárzás – azzal az ürüggyel, hogy a rádióadók ne zavarják egymás adásait – csak minimális mértékben érte el a határok túloldalán élőket. Ez az egyezmény mind a mai napig él.

A bipoláris szembenállás növekedésével, a Szabad Európa Rádió elindításával az Egyesült Államok kísérletet tett az információk keletre juttatására. Ezen adásokat azonban a zárt országok adótornyokkal zavarták, így téve lehetetlenné a rádióadások vételét. Rendkívüli helyzetekben, például a magyar 1956-os forradalom és szabadságharc idején ez a rádiózavarás megszűnt, a hírek egy rövid ideig szabadon áramlottak nyugatról, keletre. Így jutottak

el a fegyveres ellenállás folytatására, illetve a nyugati segítségre vonatkozó felhívások a szabadságharcosokhoz.

A televízió feltalálásával és elterjedésével újabb kihívás érte a zárt államok csoportját. A rádióhoz hasonló sugárzási elven működő televízió adásait szintén lehetett zavarni, de az egyre szaporodó adótornyok által sugárzott információ, különösen a keleti és a nyugati életszínvonalak közötti különbség bemutatása, veszélyeztette az állampárt egyeduralmát.

Erre a technikai fejlődésre (a tv megjelenésére és elterjedésére) technikai választ találtak a Szovjetunióban, ugyanis a televíziózásra több sugárzási rendszer is képes. Így alakult ki, hogy a nyugati országok a PAL-rendszerben működtették az adótornyokat, a keletiek azonban SECAM-ban. Egymás adásainak vételére még a vevőkészülékek sem voltak alkalmasak. Ezzel a technikai megoldással biztosítani lehetett az „ellenséges információk" határokon való megállítását.

A szocialista világrendszer összeomlásának és a Szovjetunió tervszerű visszavonulásának csak egyik oka volt a fegyverkezési versenyben való alulmaradás. Az, hogy az Egyesült Államok sebezhetetlenné tegye magát a Szovjetunió interkontinentális ballisztikus atom- és hidrogénrakétáival szemben, még a mai technikai fejlettségi színvonalon sem lehetséges tökéletesen. A valódi okok között találhatók a déli államok iszlám népességének növekedése éppúgy, mint a fegyverkezési verseny miatt stagnáló életszínvonal. A nyugati és keleti államok közötti életszínvonal-különbségek azonban mindaddig rejtve voltak a népek előtt, amíg működött az állampárt információs monopóliuma. A technikai fejlődés azonban ennek megszűnésével fenyegetett, így ez lehetett az egyik fő oka a Szovjetunió tervszerű visszavonulásának. A fejlődés egyrészről a műsorszolgáltatási műholdak méretének csökkenésében, elterjedésében jelentkezett, de a nagy kommunikációs újdonság a www (world wide web) létrehozása volt. Mindezek azzal fenyegettek, hogy az információk nem állíthatók meg többé a határokon, nyilvánvaló lesz a zárt országokban élő népek számára, hogy hogyan élnek a szabad országokban, hogyan védik az egyéni szabadságjogokat, illetve a demokratikus berendezkedés mit is jelent a valóságban (például a szabad választások lebonyolítása).

3. A tér geopolitikai fogalmának változása

3.1. Történelmi előzmények

A geopolitikai tér fogalma szükségszerűen elkülönül más tudományok térfelfogásától. Nemcsak a természettudományágak és a társadalomtudományok közötti különbség jellemzi, hanem elsősorban annak flexibilis, időben fejlődő és az emberi szellemi fejlődés által determinált volta miatt.

A geopolitika elnevezés megalkotója, a svéd Kjellén a teret és a népet tekintette az állam oszlopainak. A teret mint a „testet" és a népet mint a „lelket" határozta meg, de csak az előbbit tanulmányozta, mert szerinte a második amúgy is megfoghatatlan.

A korai geopolitikusok a Föld és az állam közötti összefüggést elemezték. Így tett Friedrich Ratzel (1923) is, aki szerint csak a földfelszín negyedét, amely – leszámítva a sarki területeket – a tenger levonulása után megmaradt, lehet belakni és államterületekre feloszlatni: de az egész Föld tárgya a politikai földrajznak, mert minden egyes politikai terület arányaiban úgy viszonylik a Föld felszínéhez, mint a rész az egészhez. Mint ahogy a népek részei az egységes emberiségnek, úgy részei az országok ennek az egyetlen legnagyobb politikai térségnek, nevezetesen a Föld felszínének.

A korszakok adott szakaszaitól függött, hogy az államok milyen nagyra növekedhettek ahhoz, hogy „világhatalmak" legyenek, azaz hogy az ismert földet politikailag átfogják és befolyásolják. De azt is kifejtette, már a XX. század elején, hogy a politikai térigények az ismert terekkel együtt növekedtek. Minden időben világhatalomnak nevezhetjük azt a hatalmat, amely ismert a Föld minden részén, és különösen a döntő helyeken birtokai révén, hatalmának teljes súlyával van jelen. Olyan hatalom, mely térben oly nagy és oly kiterjedt, hogy a Föld minden országában és tengerén közvetlenül képviseli magát, még napjainkban is csak egy van, s ez a Brit Birodalom. A széles e világon mindenütt megoszló érdekek még nem eredményeznek világhatalmi állást: a világforgalom lehetővé teszi a beszűkült államoknak is, mint Belgium és Svájc, hogy ilyen terveik legyenek. Ratzel beszél még modern tértendenciákról is, ezalatt azonban Alberoni bíborosnak a XVIII. század harmincas éveiben tett javaslatát hozza példaként az Európai Egyesült Államokról, amely európai birodalmi gyűléssel rendelkezne.

Már akkor is úgy gondolta, hogy Európának is egy, a földrészt vagy legkevesebb annak egy részét kitöltő politikai egész ideálja lesz fenntartva. Ha ez a nagytér – Európa – földrajzi megosztottsága és etnográfiai szétforgácsoltsága fölött mindenekelőtt mint gazdasági gondolat tudna diadalmaskodni, akkor ez a legnagyobb teljesítmény lenne, amire az egyáltalán képes.

A francia Jean Brunhes elmélete is teljesen területi, sőt térképészeti. Tanulmányát szántszándékkal azokra a jelenségekre korlátozta, amelyeket beírhat a térképbe. Camille Vallaux-val együtt írt művében az államot csak mint a terület, az út, a határ és a főváros írja le (Le sol et L'État – A Föld és az állam).

Jacques Ancel Geopolitika című művében ugyanakkor felhívta a figyelmet arra is, hogy „a Földön konkrétan elhelyezkedő szervezeteken kívül kell egy olyan lényeges faktor is, amit Edward Meyer „a csoportosulás örökkévalósága tudatá"-nak nevez: jogi szervezettség nélkül csak együtt élő emberek vannak és erkölcsi szervezettség nélkül csak elkülönült egyedek. És a francia történész Vidal de La Blache-hoz csatlakozik, amikor kimutatja a csoportok közti cserék szerepét – „ezek a befolyások olyan civilizációs terek kialakulásához vezetnek, amelyek a faji, nyelvi, továbbá etnikai csoportok határain átnyúlva, egymáshoz kötik a különböző politikai alakulatokat és egymás között létrehozzák a formák, életmódok és felfogások közösségét".

Mennyivel másabb Dieter Wieser térségfelfogása, aki szerint „a geopolitika térségei" rendkívül összetett karakterrel rendelkeznek. Nem csupán egy, a természet által különböző módon kialakított földfelszín-darabról van itt szó, hanem arról is, hogy benne a társadalmi erők a legkülönfélébb kifejezési formát öltve fejtik ki hatásukat számos, egymással kauzálisan és funkcionálisan összefonódó kölcsönös kapcsolat révén. Ezek a fizikai tényezők és politikai folyamatok közötti kölcsönös kapcsolatok szintén a technikai és a szocioökonómiai fejlődésnek egyik funkcióját jelentik, azaz a hely, távolság, elosztás és például a nyersanyagok rendeltetése, földrajzi dimenzióinak a technika mindenkori állása és a körülmények megszabta társadalmi fejlődés teljesen különböző jelentőséget kölcsönöznek. Például az uránlelőhelyek is teljesen érdektelenek lennének, ha egy adott helyen a kitermeléshez és az értékesítéshez nem állna rendelkezésre megfelelő technológia.

A bipoláris világrend korszaka után – ami a szovjet gazdaságot versenyen kívülivé tette – a geopolitikai szakértők megpróbálták megmagyarázni a politikai tér változását is.

A tér fogalmának átalakulását Albert Bressand és Catherine Distrel már 1995-ben elemezte a La Planète Relationnelle című munkájukban. Ezt fejlesztette tovább Michel Foucher 1997-ben, amikor a következőket írta le: „A világ új értelmezésére van szükség (a hidegháború korszaka után – a szerk.), amihez a földrajzi megközelítés nem kevésbé fölösleges, mint a kontinentális biztonság sémáinak kifejezése. Egy valóban új, a parancsokat osztó központok szerint világosan hierarchizált világról van szó, amely központokhoz újításra képes laboratóriumok és nagyon produktív térségek kapcsolódnak, s amelyeket az ipari ágazatok és cégek közötti áramlások kötnek össze egymással."

A tér átalakul, „csomópontjaival" („Hubs") és „kerékagyaival" („Spokes"), irányítóközpontjaival és a távolsági kényszereket legyőzni képes áramlásaival. A földgolyót relációk hálózata fogja át, és létre kell jönni az olyan államoknak, amelyek képesek a parancsnoki központok befogadására, a kapcsoló személyzet elhelyezésére és virágzó létének biztosítására. *Megtízszereződik a technológiai és a pénzügyi hatalom súlya.* A központok egymás között – cserével és versennyel – kooperációs kapcsolatokat tartanak fenn…

A tér változásánál érdemes megemlíteni a francia Albert Demangeon (1872–1940) munkásságát, aki Vidal de La Blache tanítványaként az emberek és tények aprólékos számbavételével a Sorbonne-on tanuló hallgatók százait oktatta. A Brit Birodalom című művében a brit civilizációt elemezte, ahol a szellemi tények, a nyelv, a vallás, a szabadság szeretete materiális tényekkel társulnak; az életmóddal, a teázástól kezdve egészen a különféle sportok űzéséig. Az erős kapcsolatokat elemzi, a kommunikációkat, a cseréket, a tőkéket, a kormányzás és a társadalom elképzelésének közös módját, de a „problémákat" is, azaz az új földrajzi területek befolyását, amelyek eltérő nemzettudatot hozhatnak létre. Demangeon szerint a nemzet elemzésénél a tér csak puszta adat, amely nem tartalmazza valamely tény egész geográfiai értékét („Les Iles Britanniques").

A tér felfogásának változását leginkább Vidal de La Blache emberföldrajzi felfogása jelentette, aki bevezette az életmódok fogalmát. Szerinte az embercsoportok életmódját az környezet határozza meg, amelyben a csoport kialakult. Így jutunk el a „civilizációs terek" körülírásához, hogy Eduard Meyer kifejezését alkalmazzuk.

A már bekövetkezett változásokat utólag próbálta meg új térfelfogással feldolgozni Michel Foucher (1979) A geopolitika vége című tanulmányában, ahol egyrészt a földgömb egészére kiterjedő piaci rend gazdasági teréről, másrészt a zárt és a nyílt társadalmak politikai teréről és ezek összeütközéséről értekezett.

Raymond Aron A háború és béke a nemzetek között című művében kifejti, hogy „… a világ új rendje a hosszú távra kialakított érdekszférák újbóli meghatározásának alapján jön létre: a tét valójában a hosszú ideig elzárt és most már szélesre tárt politikai tereken múlik". Szerinte a lokalizált, de életfontosságú gazdasági tér felismerése Franciaországban 1973 óta érvényesül, és a geostratégia iránti érdeklődés megélénkülésében mutatkozik meg: például hogyan csökkenthető az olajellátás sebezhetősége (a Hormuzi-szoros vagy a Szuezi-csatorna fölött elhelyezkedő szállítók bevonásával).

„A végre hozzáférhető nyersanyagok birtoklásáért folytatott versenyhez társul a tengereken folyó szállítások ellenőrzése iránti megnövekedett érdeklődés, amely 1996 óta a tengerjogról, a part menti vizek hatékony elhatárolásáról és a kizárólagos gazdasági zónák körülírásáról szóló ENSZ-egyezmény alkalmazását követően, mintegy ennek folyományaként, tovább erősödött. A logisztika és a meghatározott áramlások diadala ez, aminek következtében a tengeri utak a vasútvonalakhoz váltak hasonlatossá. Valójában a földet körülvevő óceánok a növekedésben lévő régiók technikai tartozékaivá válnak, s a nagy piacgazdaságok kolosszális logisztikai vállalkozásokká szerveződnek, mint II. Fülöp földközi-tengeri birodalma idején, de ez alkalommal az egész földre kiterjedő mértékben." (Aron, 1996)

Az előző fejezet bemutatta, hogy technikai fejlődéssel a kibertér hogyan jelent meg az emberiség történetében, miután a számítógépek létrejöttek. Az információs és kommunikációs technikák robbanásszerű fejlődése nemcsak újfajta tér-idő viszonyokat alakítottak ki, hanem látszólag feloldották a nemzetállamok történelmileg kialakult és a nemzetközi kapcsolatokban, szerződésekben pontosan kidolgozott határait.

Erre reflektálva a geopolitikai gondolkodás eljutott odáig, hogy Virilio kinyilvánította: „Tér már nem létezik tovább a földrajzban, a geopolitikától a kroo-politikához vezető tendencia figyelhető meg: a tér disztribúcióját felváltja az idő disztiribúciója". (Mező, 2006)

Eközben a számítógépes memória és a processzor megalkotása az emberiség történetében először hozott olyan teret létre, amely függetlenedhet az embertől, és amely, megteremtette a lehetőséget ember és gép párbeszédére. Elnevezése a **kibertér** (Cyperspace), a görög kyber (hajózni, navigálni) szóból ered, melyet Gibson az 1984-ben megjelent Neuromancer című regényében úgy ír le, mint a hálózatba kapcsolt számítógép-terminálokról közvetlenül elérhető digitális, navigálható teret. A kibertér Gibson szerint egy olyan mátrix, amely színes, elektronikus, karteziánus adattájkép (Dataspace), amelyben az egyének és a cégek interaktív kapcsolatba lépnek az információval, sőt kereskednek vele.

A geopolitikai térfogalmak folyamatos változása során figyelmen kívül hagyjuk Gibson eredeti elképzelését, amely szerint a kibertér az információs és kommunikációs technikák világában megnyilvánuló térfogalom, és nem magának a technológiának a neve.

M. Castells (1996) azt is felveti, hogy a térhez és időhöz hasonlóan a földrajzi távolság is szétfoszlik az áramlások (folyamatok) terében úgy, hogy a kibertér hely nélküli (placeless) tér lesz. Mészáros Rezső (2001) kifejtette, hogy „a kibertér térgeometriái tehát bonyolult tartománygyűjteményekből épülnek fel, ezek közül némelyeknek kifejezetten térbeli, és közvetlen földrajzi mintái (hivatkozási alapjai) vannak, mások mintáikat ugyan a való világból veszik, de kifejezetten térbeli formájuk és a térre jellemző tulajdonságaik nincsenek (névsorok, weboldalak), és vannak olyanok is, amelyeknek nincs a földrajzi világból vett mintájuk, térformáik és a térre jellemző tulajdonságaik sincsenek (ilyenek a számítógépes adatállományok allokációs táblázatai). De bármelyik esetet vesszük, akármilyen geometria fedezhető fel bennük, azt mesterséges úton állították elő, és csak megjelenített (kivetített) térkonstrukció formájában léteznek."

3.2. A kibertér és a virtuális tér elhatárolása

A kibertér és a virtuális tér gyakran azonos fogalomként jelennek meg, így történt ez K. Memarzia (1997) vagy Mészáros Rezső (2001) munkáiban. Ezt az összemosódást erősítette M. Benedickt 1991-ben írt tanulmányában, szerinte ugyanis a kibertér „a gondolatvilágunkban létező közös földrajz" (common mental geography) olyan közeg, amelyben a mitikus és képzeletbeli terek

láthatóvá válnak, az euklideszi geometria és a karteziánus térképezés uralma alól felszabadult képzeletvilág elvont terei, olyan terek, ahol „a topológia és geometria alapigazságait, amelyekről eddig kötelező érvénnyel hitték, hogy a természet szerves részei… és a fizika sok törvényét is meg lehet szegni vagy újra kitalálni".

Mészáros (2010, p.361) újabb tanulmánya szerint a virtuális valóság (Virtual Reality, VR) a kibertér leginkább fejlődő területe. Szerinte „A virtuális valóságnak azokat a számítógépes alkalmazásokat nevezzük, amelyek segítségével olyan mesterséges, háromdimenziós világokat lehet alkotni, amelyeket a felhasználó bejárhat, felfedezhet – sőt, némelyiken most már maga is továbbmódosíthat, alakíthatja azt. Tehát a virtuális valóság egy nagyon speciális formája az ember-számítógép kapcsolatnak, amely arra épül, hogy a kibertérben a valóság minél teljesebb megjelenítésének lehetőségét adja meg."

Valójában még a legmodernebb geopolitikusok sem igen tudnak mit kezdeni a virtuális tér és a kibertér fogalmával, melyet gyakran egymás szinonimájaként használnak. Ezért van az, hogy a kiberteret olyan „rétestésztának" próbálják beállítani, melynek különböző rétegei között kölcsönhatás van. A kutatók 3, 4, 5 vagy akár 7 rétegről is értekeznek.

Frédérick Douzet (2014) az egyszerűség kedvéért négy réteget mutatott be; az első a *fizikai réteg,* amelyet az internet struktúráját adó, főleg tenger alatti és szárazföldi kábelek összessége, a távközlési rendszerek és számítógépek jelentik, beleértve a Föld körül keringő vagy geostacionárius pályán lévő műholdakat is. A második réteget a *logisztikai infrastruktúra* alkotná, amelyek alatt mindazon szolgáltatásokat érti, amelyek lehetővé teszik az adatátvitelt, a hálózat egyik pontjából a másikba, vagyis az információáramlást. Ez a logisztikai felépítés egy közös nyelvezeten alapszik, amely lehetővé teszi, hogy minden számítógép egymás között kommunikálhasson (internet protokoll – TCP/IP). Az útválasztó szolgáltatások a hálózati forgalomirányításhoz szükségesek, ezenkívül van Azonosító (a hálózati azonosító vagy felhasználói név) és a Hálózati Cím, amely átalakítja a címeket jelölő számsorozatokat olvasható szavakká a felhasználó számára. A harmadik réteg az *alkalmazások*ból, azaz az informatikai programokból állna, amelyek lehetővé teszik, hogy bárki anélkül használhassa az internetet, hogy maga ismerné a számítógépes programozást (web, e-mail, közösségi oldalak, keresőmotorok stb.).

Végül a negyedik réteg a *társadalmi információ* interakció rétege, amit néha kognitív vagy szemantikai rétegnek is neveznek.

Douzet a rétegek pontos megjelölése után mégiscsak tett egy próbát a kibertér fogalmának meghatározására a következőképpen: „A kibertér lenne egyszerre mindez: emberek, adatok és számítógépek hálózata – és egyre inkább mobileszközök hálózata is (telefonok, tabletek és hamarosan hűtőszekrények, karkötők, sportcipők…). Információs tér, területhez nem kötött információcsere, amelyet nehéz megérteni. Materiális infrastruktúrából áll, amelyet fizikai területre építenek, ideértve a világűrben megtalálható műholdakat is." Végezetül feladja a próbálkozást, amikor kijelenti, hogy „a felhasználó és céljai szerint a kibertér jelenthet fizikai infrastruktúrát vagy teljesen más fogalmat".

Újfajta megközelítéssel Pintér István (2009) definíciójában határozottan különválasztotta a virtuális és a kiberteret. Szerinte a „*Virtuális tér: az emberiség tudatában megjelenő információk halmaza*."

Ez a fogalom egyben új választ ad arra a filozófiai kérdésre is, hogy „a hátam mögött lévő alma létezik-e?" E szerint a virtuális térben csak akkor igen, ha az emberiség bármelyik másik egyede észleli azt.

A fogalom egyik központi eleme a percepció, mégpedig az egyén percepciója. A emberiség tudata úgy jelenik meg, mint az egyének tudatának összessége.

Az információ lehet bármi: egy észlelés, hír, kép, vélemény, tanulmány, egy szóbeli közlés (vagy csak egy levegőrezgés), elektromágneses hullám (fény) vagy akár egy számítógépes hálózaton megjelenő elektronikus jel.

Pintér ezzel az adattömegre és az információtömegre alapozott fogalommal egyrészt Yves Lacoste nyomdokain halad, aki a képzet szerepét hangsúlyozza, és munkáiban kiemeli a sajtó által terjesztett információ fontosságát. Másrészt visszatér az alapokhoz, amennyiben figyelembe veszi Gibson adatterét (Dataspace), amelyben az egyének és a cégek interaktív kapcsolatba lépnek az információval, sőt kereskednek vele.

Pintér (2009) szerint „az információk osztályozása számtalan módon történhet, származási hely, előállítási eszköz, időtényező (múltbeli, jelenbeli, jövőre vonatkozó információk), de az egyik leglényegesebb osztályozás az, hogy az **információ lehet igaz vagy hamis**. Pontosabban: a valóságot a lehető legpontosabban, megközelítően vagy a valóságot manipulálva tartalmazza-e az

információ. Ki kell emelnünk az emberi percepció korlátait, mint lényeges hibahatárt. E szerint a *kibertér* definíciója: olyan információhalmaz, amely digitális formában létezik, és az egyén számára elsősorban számítógépes rendszereken, szoftverek segítségével érhető el." Tanulmányában kifejtette még, hogy a „kibertérben olyan új veszélyek jelentek meg, mint pl. az automatikus válasz-generálás. A tőzsdei értékek előre beállított mértékben történő elmozdulása esetén automatikus vételi vagy eladási utasítás kiküldése, avagy a digitalizált percepciós eszközök manipulálásával atomerőművi vagy vegyi folyamatok távolról történő befolyásolása tekinthető például ilyennek. A kibertér befolyásolja és átalakítja a virtuális teret (lásd: virtuális társadalom), a kölcsönhatás egyelőre a kibertér behatolására utal: ez részben természetes, hiszen az újdonság természetesen hat a régi struktúrákra. A kibertér túl gyors terjeszkedése azonban nem csak előnyére alakíthatja a virtuális teret."

A 2009-es definíció megtartásával most lehetőség van a kibertér pontosabb meghatározására. E szerint:

> *Geopolitikai aspektusból a kibertér a gépi memóriákban meglévő adat- és információtömeg, míg a virtuális tér az emberiség memóriájában meglévő információtömeg.*

3.3. A kibertér hatásai

D. Haraway (1991) úgy látja, hogy a kibertér azáltal módosítja az éntudatot, hogy új lehetőséget nyújt a test hatásainak kiterjesztésére.

Mészáros Rezső (2001) szerint a kibertér nem az információ szállítására, feldolgozására van a legnagyobb hatással, hanem a társadalmi viszonyok, kapcsolatok alakulására.

S. McRae (1997) nagyon határozottan érvel amellett, hogy a kibertérben folyó interaktív társadalmi érintkezés jelentős hatással van az emberekre, megváltoztatja világnézetüket, sőt értékrendjüket is.

Ez az interaktív számítógépes társadalmi kapcsolatok segítségével folytatott játék az egyén személyiségével azt jelenti, hogy a kibertér használói új közösségeket és új társadalmi struktúrákat alakítanak ki, amelyek nem arra épülnek, hogy milyen a résztvevők külső megjelenése vagy hogy hol élnek, hanem arra, hogy mit gondolnak, mondanak, hisznek, és mi érdekli őket. Sőt, a ki-

bertér megjelenésének egyik legfontosabb eredménye az olyan új közösségek kialakulása, amelyek mentesek a tér korlátaitól, és a kölcsönhatások új fajtáira és a társadalmi kapcsolatok új formáira épülnek.

H. Rheingold (1993) úgy határozza meg a virtuális közösségeket, mint „olyan társadalmi csoportosulásokat, amelyek akkor alakulnak ki a Hálón, ha elég ember folytat elég hosszú ideig tartó nyilvános vitát egymással, és elég emberi érzést visz bele ebbe a tevékenységbe ahhoz, hogy személyes kapcsolatok hálózatát alakítsák ki egymással a kibertérben".

Ezek a közösségek nem a földrajzi közelségre, az egymásmellettiségre épülnek, hanem az egymással folytatott kommunikációra. Mészáros Rezső már korábbi művében is felhívta a figyelmet arra, hogy kevésbé kutatottak az információs és kommunikációs technikák fejlődésének társadalmi, kulturális, politikai következményei. Szerinte a kibertér potenciálisan gyengíti a földrajzi közösségeket azzal, hogy olyan központot kínál, amely a földrajzi közelség helyett a közös érdeklődésen alapul. Attól lehet tartani, hogy ahogy az emberek visszahúzódnak a kibertérbe, a földrajzi tér tovább aprózódik, és darabjaira fog széthullni, és így a társadalom egyre antiszociálisabbá válhat. Szerinte ennek a bomlasztó, pusztító hatásnak három típusa van; egyrészt a globális kultúra terjeszkedése, a világméretű szervezetek szerkezetátalakítása és harmadikként egy olyan alternatív tér létrejötte, amelyben az „én" határozatlan körvonalú és testetlen, a közösség pedig inkább a közös érdeklődés, mint a közös lakóhely alapján alakul ki.

Azt is kifejti, hogy fenntartással kell kezelni azt a népszerűsítő állítást, hogy a kibertér az egyenlőség színtere, oda mindenkinek szabad bejárása van. Az adatok egyértelműen bizonyítják, hogy az internetes hozzáférés nagy területi és társadalmi egyenlőtlenségeket mutat. A kibertér használatával együtt járó társadalmi, politikai és gazdasági előnyök a hagyományos térbeli és társadalmi megoszlások mentén helyezkednek el. Ebből többen arra következtetnek, hogy a kibertér újra fogja termelni, sőt, meg fogja erősíteni az egyes országokon, térségeken belül kialakuló egyenlőtlenségeket, a fejlett és fejletlen világ közötti különbségeket, és új egyenlőtlenségeket fog teremteni, ami fokozhatja a társadalmi megosztottságot.

Barabási (2003) hálózatelméleti oldalról támasztja alá Mészáros meglátásait, amikor a világhálón a szólásszabadságot csak látszólagosnak találja. „A webet feltérképező munkák legérdekesebb eredménye, hogy **a demokrácia, a tisztességesség és egyenlősdi teljesen hiányoznak a hálón**. Megtanultuk, hogy a web topológiája olyan, hogy a milliárdnyi meglévő dokumentum közül csupán egy maroknyit vehetünk észre.

Ha a webről van szó, akkor többé nem az a kulcskérdés, hogy az Olvasó nézetei megjelenhetnek-e. Megjelenhetnek. Amint megjelentek, azonnal elérhetőek lesznek a világon bárki számára, akinek internetkapcsolata van. Az egymilliárd oldal dzsungelével szembesülve a kérdés inkább az, hogy ha ön kitesz a webre valamilyen információt, észreveszi-e azt bárki.

Ahhoz, hogy az ön oldalát elolvassák, az oldalnak láthatónak kell lennie. Ez az igazság regényírókra és kutatókra egyaránt érvényes. A weben való láthatóság mértéke a linkek száma. Minél több bejövő link mutat az ön oldalára, annál jobban látható. Ha a weben lévő összes dokumentumról lenne mutató az ön oldalához, akkor nagyon rövid idő alatt, mindenki megismerné az ön mondanivalóját. Az átlagos weboldalról csak 5 és 7 közötti mutató indul, amelyek mindegyike az egymilliárd meglévő weboldal egyikére mutat. Ezért annak az esélye, hogy egy átlagos dokumentum tartalmaz mutatót az ön oldalára, közel nulla."

Z. Sardar (1995) szerint a kibertér az amerikanizált világkép terjedésének kedvez, mivel „anyanyelve" az angol, műszaki fejlődését, tartalmát és szokásait az Egyesült Államok irányítja. Az interneten a legnagyobb és legnépszerűbb webhelyek többnyire amerikai tulajdonban vannak. A világ számítógépeinek legnagyobb része is amerikai operációs rendszereken, amerikai programokat futtat.

Mészáros Rezső (2001) szerint a hatalom gyakorlásának és ellenőrzésének egyik legfontosabb közege a tér. A tér megszervezése a területi határok kijelölése, a rend fenntartása a térben a hatalom bonyolult térgeometriájának a kialakulásához vezetnek. A tapasztalat arra utal, hogy a kibertér szétrombolja a hagyományos hatalmi geometriák működés-módszertani alapjait, és a befolyásolás gyakorlásának új technológiáját kínálja.

Álláspontom szerint a *kibertér* létrejövetele és hatása messze túlmutat mindezeken a felvetéseken. Nem vitatva annak jelenbeli társadalmi, gazdasági,

pénzügyi és politikai hatásait, **forradalmisága abban rejlik, hogy bölcsője a mesterséges intelligenciának**, amely előre vetíti az ember-gép viszony jövőbeni konfliktusait. A kibertér alkalmas arra is, hogy a virtuális teret fejlessze (a kommunikáció új formái révén), de tág teret adhat a manipulációnak, amely a jelenkori demokrácia egyik legnagyobb kihívása. Képes arra is, hogy az emberi érzékelést megtévessze, összezavarja, ezzel – adott esetben – helytelen döntések meghozatalát segítse elő. A téma – fontossága ellenére – ismételten a kapitalizmus pénzcentrikusságának eshet áldozatául, mint történt az az 1960-as években a transznacionális vállalkozások működése, később a sajtónak a demokrácia egészét érintő kérdései, vagy napjainkban az offshore pénzügyi területek vagy a nemzetközi korrupció esetében. „A haszon mindenek felett" hozzáállás gyakran vezet szabályozatlansághoz, a piac önszabályozó szerepének túlértékeléséhez. A társadalmi, kulturális hatások negligálása egy sor konfliktus kiinduló alapja.

A geopolitikai terek meghódítása

Geopolitikai terek	a meghódítás fő eszközei	néhány innováció	nemzetközi szabályozás
virtuális tér	beszéd,írásjelek, könyv, távíró, telefon, fotográfia, mozgófilm	ékírás, betűírás, agyagtáblák, papirusz, papír, könyvnyomtatás, telefon, telefonközpont, rádió, TV,	Emberi Jogi Egyezmények, ITU frekvencia megosztás, szabványosítás, pl.: ISO hiányzik: a nemzetközi média szabályozása
szárazföld	szekér, kerékpár, vasút, autó	új energiaforrások felhasználására: állati erő, szél, fosszilis, atom, nap stb.	a háború joga, az államok közötti kapcsolatok
tengerek	hajó	vitorla, gőzgép, Diesel-motor, deszkavágó gép, fémtörzs, atommeghajtás stb.	tengerjogi egyezmények
légtér	légballon, repülő, helikopter	erősebb motorok, fémszerkezet, napelemek	légtér definíciója + nemzetközi egyezmények
világűr	űrjárművek	rakétatörzs, újfajta ötvözetek, rakéta-hajtóanyag, rakétamotorok, giroszkóp, tájékozódás más formái stb.	nemzetközi egyezmények a világűrről (ENSZ)
kibertér	processzor, programnyelvek	mikroprocesszor, számítógépes memória, programok, számító- gépes hálózatok, internet, IoT	csak kétoldalú megállapodások (USA-Kína, Kína-Oroszország) + magánszabványok

4. Versengés a virtuális térben

Az emberiség fejlődése során döntő tényező volt a megszerzett tudás, információ összegyűjtése, feldolgozása, megőrzése és átörökítése a következő nemzedékekre.

Már az ókorban folytatott háborúk során is kiemelt célpontok voltak az ellenség könyvtárai. Vagy abból a célból, hogy az ott összegyűjtött tudást megszerezzék, vagy azért, hogy a könyvtárat felégetve tegyék bizonytalanná az ellenség jövőjét.

Gutenberg óta exponenciálisan növekszik az emberiség memóriájában meglévő, illetve a nem digitálisan tárolt információk tömege. A könyvnyomtatás révén a tudás széleskörűvé vált. Következményeként átalakult az iskolarendszer, az egyház hatalma meggyengült. A könyvek előállítására, terjesztésére egy egész iparág épült fel.

A forradalmi változásokat a virtuális térben is az ipari forradalmak találmányai okozták. Előbb a modern nyomdai gépek tették lehetővé a sajtótermékek elterjedését, az emberek közvetett úton történő, napi rendszerességű tájékoztatását. Néhány évtized múlva, a rádió és a televízió feltalálása után, a kommunikációs csatornák már közvetlenül az otthonokban végződtek. Miközben olyan új iparágak tűntek fel mint a filmgyártás, vagy a televíziós sorozatok előállítása, szinkronizálása. Mégis az egyik legfontosabb következmény nem anyagi természetű. Mivel a tömegtájékoztatási média képes befolyásolni a politikai választásoktól kezdve a gazdasági döntéseken át a társadalmi együttélés teljes spektrumát, joggal nevezhetjük **önálló hatalmi ágnak**. A törvényhozói, végrehajtói és a bírói hatalmi ágak azonban nem törekedtek az új hatalmi ág elismerésére, így a szabályozását is jórészt magukra a piaci szereplőkre bízták. Kialakultak az újságírói szervezetek és az újságírói etika, melynek megsértőit azért mégis fenyegették valamiféle szankciók. A hatalomra jutott polgárság törvényei elismerték a monopóliumokat, jogszerűsítették a kizsákmányolást; miért éppen a sajtót korlátozták volna? Azt inkább jogon kívüli eszközökkel (főként a pénz eszközül használásával) próbálták a maguk előnyére felhasználni. A gyáriparhoz hasonlóan az információiparban is hamarosan megjelentek a monopóliumok, amelyek mind a mai napig kontrollálják a világ híráramlását.

Az információ és a gazdaság összefüggése nem mai keletű. Például az 1929–1933-as világgazdasági válság egyik kiváltó oka a sajtóban végbement manipuláció volt. A kisemberek számára is elérhetők voltak azok a kötvények és részvények, melyeknek adásvételével a gyors meggazdagodást próbálták elérni. Az újságok ugyanakkor hamis híreket jelentettek meg az egyes vállalkozások termelési adatairól vagy kilátásairól. Korrupt újságírók manipulálták a híreket, mivel egyes cégvezetők rájöttek arra, hogy a termelés hatékonyságának növelése helyett a részvényárfolyamok emeléséhez elegendő kizárólag a híreket manipulálni.

A virtuális tér – azaz az emberi tudás – manipulálása mindig is jelen volt, legfeljebb annak mértékében történik változás. Az ipari forradalmakban megerősödött pénztőkének mindig is volt befolyása a virtuális tér alakulására.

A virtuális térben meglévő információk egy része ma is **hamis**. Nézzünk erre egy releváns példát az angliai ipari forradalom idejéből:

> Általánosan elterjedt nézet, hogy James Watt skót mérnök találta fel a gőzgépet és George Stephenson a gőzmozdonyt. Ez, a virtuális térben lévő és gyakran használt információ azonban hamis. Valójában Watt születésekor Thomas Newcomen gőzgépei már Anglia-szerte üzemeltek. Watt találmánya egy új, fontos részegység, a vízgőz lecsapására szolgáló gőzkondenzátor volt, amellyel a gép hatásfokát, gazdaságosságát növelte meg jelentősen. Mivel a gőzgép fejlesztésével lényegesen hozzájárult az ipari forradalomhoz, róla nevezték el a teljesítmény mértékegységét (Watt) az SI-rendszerben. A világ első gőzmozdonya a sikeres próbautat 1804. február 21-én tette meg. A tíz tonnányi vasáruval, hetven utassal és öt üres vagonnal terhelt mozdony a mintegy 16 km-es utat négy óra és öt perc alatt teljesítette, majdnem 4 km/h-s átlagsebességgel. Tervezője azonban nem Stephenson, hanem Richard Trevithick volt. Stephenson 1815-ben készült Blücher-e volt az első olyan jármű, amely az általa úttörőként alkalmazott peremes kerekeinek köszönhetően a síneken maradt, és 4 kilométeres óránkénti sebességgel 30 tonnás terhet tudott elvontatni. Alig 134 évvel később, az akkori ipari teljesítmény csúcsaként a britek megépítették a Mallard elnevezésű gőzmozdonyt, amely 1938-ban beállította a ma is érvényes óránkénti 202,6 kilométeres (125 mérföld/óra) sebességrekordot, legyőzve ezzel a német birodalmi

vasút DRG osztályának 05002-es pályaszámú gőzmozdonyát. (https://hu.wikipedia.org/wiki/Richard_Trevithick, utolsó letöltés: 2016. 08. 12.)

Már a korai vállalkozók is felismerték, hogy a termékekkel kapcsolatos híreket hatékonyabban tudják a nagyközönséghez eljuttatni, ha azokat kulturális vivőközegbe helyezik. Így tett a lőfegyvereket gyártó Colt cég is, amely minden könyv, cikk vagy filmalkotás szerzőjének jelentős honoráriumot fizetett, ha megjelenítik a terméküket. Tette mindezt titkosnak minősített szerződések alapján. Az ötvenes években nem létezett olyan mozifilm, ahol ne fogyasztottak volna cigarettát, vagy alkoholt. A televíziós korszakban a manipulációt a fizetett reklámok teljesítik ki. Egyetlen tisztítószer sem képes öt másodperc alatt csillogóra varázsolni a fürdőszobát. Ráadásul a reklámidő – annak drágasága miatt – a kis- és közepesvállalkozások számára elérhetetlen.

Ezt az igen jelentős reklámbevételt osztja fel újra az internet, amelyben a kereső programokat üzemeltető magáncégek pontosan tudják, hogy az adott személy milyen terméket vásárolna szívesen, hiszen minden kattintásukat nyilvántartják. Az új módszer segítségével a hirdetők reklámja sokkal pontosabban célba ér, mint a televíziós vagy újsághirdetések. Az olyan cégek, mint a Google vagy a Facebook árbevételük jelentős hányadát a globális reklámpiac újraelosztásából szerzik. A reklámbevételek helyi elmaradása teljes szektorokat lehetetlenít el. A jelenséget Pintér (2009) Manchester-effektusnak nevezte el. A bevételek globális centralizálása, a nemzetállami adózást elkerülő volta, a helyi közösségi feladatok finanszírozását veszélyezteti.

„A kommunikációt hagyományosan két fő szerkezeti részre osztják: egyrészt az információ, a vélemények és a szórakoztató anyagok termelésére, másrészt ezek terjesztésére. A gyakorlatban sohasem volt teljes a különválás és az átfedés, az egységes ellenőrzés ma gyakorta sokkal nagyobb, mint a múltban. A megkülönböztetésnek mégis van jelentősége, mivel sok ország kommunikációs rendszerének fejlesztése során elsőbbséget ad a terjesztésnek a termelés rovására. Ebből eredően függő viszonyba kerülnek az infrastruktúrába történő külföldi beruházástól, a külső szervezetek által összeállított hírektől és szórakoztató műsoroktól és általában minden olyan termelési erőforrástól, amelyre nincs befolyásuk.

Noha a legtöbb országnak már van nemzeti hírügynöksége, anyagi, technikai vagy személyi erőforrásaik gyakran korlátozottak, és ezért hírkínálatukat ki kell egészíteni külföldi anyagokkal. Többek között e miatt is függ a tömegtájékoztatás ezekben az országokban a nagy külföldi hírközlő szervek által válogatott és közvetített anyagoktól. A rádió és tévé műsorszerkezetét szintén megterheli a külföldi import, ugyanígy a hirdetési szektort is gyakran befolyásolják, ha éppen nem ellenőrzik a külföldi társaságok. Ez a rendszer sok esetben nagymérvű külföldi beavatkozáshoz, erős külső függéshez és a kommunikációs ipar anyagait előállító ágazatok fejlődésében egészségtelen versenyhez vezet.". (Halász László, 1985. pp. 492–495)

Smith szerint a nemzetközi információs monopóliumok a fő felelősei az UNESCO égisze alatt létrejött MacBride-jelentés (1980) által rögzített **információs egyensúlyhiánynak**, **egyenlőtlenségeknek** és a **szabad információáramlás hiányának**.

Eközben jelentős átrendeződés megy végbe, melynek következtében még a Financial Times is új tulajdonoshoz került 2015-ben. A napi 722 ezer olvasóhoz eljutott lap nyomtatott változata az elmúlt évtizedben elveszítette olvasóinak felét, de az online kiadás évi 21%-kal nőtt. A teljes előfizetői kör több mint 70%-a már a digitális változatot olvassa. Az 1844-ben alakult brit Pearson kiadócsoport – amelynek 50%-os részesedése van a The Economist kiadócégében is – úgy döntött, hogy azért értékesíti a nyereséges lapot, hogy a *digitális oktatási szolgáltatásokat* tudják fejleszteni. A vevőjelöltek (Thomson Reuters, Nikkei, Axel Springer, Bloomberg) közül a Nikkei vásárolhatta meg a lapot. 1 milliárd font vételárért.

Halász szerint a „kommunikációs ipar" magában foglalja az ún. „kulturális ipart" is. „A kommunikációs ipar termelési ága – kiadók, hírügynökségek, adatszolgáltatók, film- és hangfelvételgyártó, hirdetési ügynökségek – létfontosságú az egész ipar fejlődése szempontjából. Bár a tömegtermelésnek kétes aspektusai is vannak, igazságtalanság lenne azt állítani, hogy a kommunikáció iparrá válása káros. E nélkül a kommunikáció szintje kétséget kizáróan alacsonyabb lenne, bár az iparrá válás olyan kulturális környezetet is teremthet, amelyet nem kívánatos külső hatások befolyásolnak, és amelyet az egyhangúság és a sztereotípia jellemez." Tévedett azonban abban, hogy a tömeges terjesztés a kultúra népszerűsödését és nagyfokú demokratizálódását jelezné

olyan művek esetében is, amelyek eddig főként az értelmiség és a gazdagok kiváltságai voltak. Ez a megállapítás csak a könyvre volt igaz, a tömegmédiára és főképpen a világhálón terjedő tartalmakra már nem.

A tényleges hatást Rosengren (2000) a következőképpen írja le: „…számos, a média rendszerén belül létrejött innováció a művészet és irodalom szektorában helyezhető el. Azonban a tömegkommunikáció által közvetített újítások alkotóinak többsége, a magas kultúra alkotóihoz képest lényegesen korlátozottabb művészi függetlenséggel rendelkezik. A nemzetközi populáris kultúra rendszerén belül létrejövő innovációk többsége nem túlságosan eredeti – inkább néhány általános kulturális minta klónszerű variációinak tekinthetőek. Így van ez a populáris irodalom esetében is, a megjelenés formájától (televízió, rádió, hetilapok, magazinok, könyvek stb.) függetlenül. Sajnos túl gyakran találkozunk olyan sztenderdizált sémákkal, mint a „boldogan éltek, amíg meg nem haltak" típusú szerelmi történetek vagy a „jó és gonosz" harca. Többékevésbé sztenderd hősök és hősnők tettei többé-kevésbé sztenderd módon ismétlődnek újra meg újra, gyakorlatilag vég nélkül. Egy olyan speciális iparágról van szó, ahol a gazdasági és kommunikációs szakemberek szoros együttműködésben dolgoznak a művészekkel és a műszakiakkal."

Toffler (1980) szerint „A második hullám (a ipari forradalmak kora – a szerk.) ezzel szemben megsokszorozta azoknak a csatornáknak a számát, amelyekből merítve az egyén kialakíthatta a saját képét a valóságról. A gyermek többé nemcsak a természetből vette vagy más emberektől kapta képzeteit, hanem az újságokból, magazinokból, a rádióból és később a televízióból is. Az egyház, az állam, az otthon és az iskola továbbra is legnagyobb részt egybehangzóan beszélt hozzá, egymást felerősítve. De most már maguk a tömegtájékoztatási eszközök váltak óriási hangszórókká. Ezeknek az erejét már a regionális, etnikai, törzsi és nyelvi határokat átlépve használták fel, azzal a céllal, hogy egységesítsék a társadalom képzeletvilágában kialakuló képeket.

Bizonyos vizuális képeket például olyan tömegesen terjesztettek és oly sok ember memóriájába ültettek be, hogy valósággal ikonokká váltak. Lenin képmása – diadalmasan felszegett állal, a hullámzó vöröslobogó alatt – éppúgy ikonszerűvé vált emberek milliói számára, mint Krisztus képe a kereszten. Charlie Chaplin keménykalapos, sétapálcás figurája; Hitler dühöngése Nürnbergben; a fahasábok módjára egymásra rakott emberi holttestek képe

Büchenwaldból; Churchill, amint két ujjával mutatja a győzelem jelét vagy Roosevelt fekete köpenyében, Marilyn Monroe széltől felfújt szoknyája; médiasztárok százainak és univerzálisan felismerhető kereskedelmi termékek ezreinek képei; az Ivory márkájú szappané az Egyesült Államokban, a Morinaga csokoládé Japánban, a Perrier palacké Franciaországban – mind-mind standard elemekké váltak a képek univerzális tárházában. Ez a központilag előállított képtár, amelyet a tömegek „agyába" plántált a tömegtájékoztatás, segített az ipari termelési rendszer által megkívánt szabványviselkedés kialakításában.

Ma a harmadik hullám mindezt gyökeresen megváltoztatja. Ahogy a változás felgyorsul a társadalomban, bennünk magunkban is ezzel párhuzamos gyorsulást kényszerít ki. Minduntalan új információ jut el hozzánk, és emiatt kénytelenek vagyunk folyamatosan átrendezni saját képzeteink tárházát, egyre gyorsabb és gyorsabb ütemben. A múlt valóságán alapuló régebbi képeket mindig újabbakra kell felcserélnünk, mert ha ezt nem tesszük meg, tetteink elválnak a valóságtól és egyre kevésbé leszünk hatékonyak. Nem tudjuk tartani a lépést.

…Ebben az örvénylő varázstükörben nehéz eligazodni, és pontosan megérteni, hogyan változik maga a képzetgyártó folyamat. Mert a harmadik hullám az információáramlás egyszerű felgyorsításánál többet tesz: átalakítja az információ mélystruktúráját, amelytől mindennapi tevékenységünk függ."

Az információáramlás ellenőrzése még ma is jórészt **állami monopólium**. Minden hatalmon lévő kormányzati elit az állami szuverenitás részének tekinti azt a tudást, hogy mi történik a területén, mit tesznek vagy terveznek az állampolgárai. Jogszabályok biztosította lehetőség mindenütt, hogy a személyes szabadságjogokat figyelmen kívül hagyva – több, kevesebb korlát és ellensúly biztosításával – lehallgassanak bárkit, ellenőrizhessék bárki levelezését, e-mail-forgalmát, vagy internetezési szokásait.

Napjainkra a technikai fejlődéssel ez az információáramlást ellenőrző lehetőség túlnyúlik az adott állam keretein. A nemzetállami szuverenitást, a hatalmi viszonyokat megalapozó információáramlást mások is képesek felderíteni, kontrollálni. Azzal, hogy a telefonálás már nem rézkábeleken, hanem jórészt mobileszközökön történik, alkalmat ad arra, hogy az elektromágneses hullámokat mások is lehallgassák. Nem véletlen, hogy Nagy-Britannia az

ilyen térben megjelenő információkat védtelen, „open source", azaz nyílt forrásúnak tekinti. Az elektronikus levélforgalom globális számítógép-hálózatokon keresztül történik, jórészt egyesült államokbeli multinacionális cégek eszközparkján. Itt olyan személyes adatok is megőrzésre kerülnek, melyeknek gyűjtését más állam joga kifejezetten tiltja.

Anthony Smith Az információ geopolitikája (The Geopolitics of Information) című, 1980-ban megjelent könyvében azt az aggodalmát hangsúlyozta ki, „amire a folyamatban lévő, szörnyen megfontolatlan telekommunikációs befektetések adnak okot. Az új ipari forradalomra való készülődés, amit a mikroelektronika és az új telekommunikációs rendszerek megjelenése tett szükségessé, úgy kellene, hogy történjen, hogy az figyelembe vegye ennek világszintű hatásait és nemcsak a transznacionális vállalatok és kvázi-monopóliumok rövid távú érdekeit, ami ezt a területet dominálja. Ez valóban egy olyan terület, ahol nemzetközi cselekvésre van szükség, mert a nélkül a világ szektorai közötti egyenlőtlenségek visszafordíthatatlanul hatalmasak lesznek. **A 20. század végén mindez nagyobb fenyegetést jelent a függetlenségre, mint maga a gyarmatosítás.** Egyre jobban ráeszmélünk, hogy a dekolonizáció és a szupranacionalitás nem a birodalmi kapcsolatok végét jelentette, hanem csupán tovább szőtte azt a geopolitikai hálót, amit már a reneszánsz óta fonunk. Az új médiumoknak olyan az ereje, hogy jobban be tud hatolni egy fogadó kultúrába, mint a nyugati technológia bármelyik korábbi manifesztációja. Ez hatalmas felfordulást eredményezhet, és a szociális ellentmondásokat erősítheti a fejlődő társadalmakban. Mi a Nyugaton azt gondoljuk a 2500 kommunikációs szatellitről, amelyek a Föld körül keringenek, hogy csupán információt terjesztenek. Ám sok társadalom számára a műholdak olyan pipettává változhatnak, amivel kiszippantják egy társadalom szuverenitását nyújtó adatait, hogy azokat egy távoli helyen feldolgozzák.

Habár nem tehetünk sokat, hogy a jelenlegi világ információs rendszerének tökéletlenségeit gyorsan kijavítsuk, bizonyára a kormányok képesek arra, illetve a vállalatok hosszú távon érdekeltek abban, hogy az új hálózatokat a valódi kölcsönös egymásrautaltság szellemében építsék meg. Ennek velejárója lehet, hogy a fejlődő társadalmaknak a rádiófrekvenciák elosztása esetében nem kívánatos koncessziókat kell megadnunk; vagy, hogy a számítógépgyártókat köteleznünk kell, hogy együtt dolgozzanak a harmadik világ

kormányaival. Mindenképpen része kell legyen az, hogy bátorítsuk a gyáripar és a fejlődő társadalmak közötti kapcsolatokat. Habár nehéz gyökerestől megszüntetni a múltból származó kiegyensúlyozatlanságokat, még mindig van rá remény, hogy az 1980-as és 1990-es években megjósolt „információs társadalom" valóban egy lehetőség legyen egy új kezdethez."

Ahogyan a tömegtájékoztatási eszközök annak idején megtörték az írott sajtó uralmát, a globális számítógép hálózatokon működő kommunikációs csatornák ma már dominálják a fiatalabb generációk figyelmét. A televízió uralma még tart, de csak az idősebb korosztályok körében. A határokon átnyúló információ-áramlás beigazolja Smith félelmeit. Mára **egybeforrt a közösségi média, az értékesítés és a hírgyártás**. Jelenleg meggyőzés helyett manipuláció áldozatai vagyunk. Professzionális szociálpszichológusok manipulálnak bennünket anélkül, hogy azt észrevennénk. Az tud hatékonyan manipulálni, aki ismeri az adott személy gondolatait és érzelmeit, de mindezen adatokat saját magunk adjuk át azzal, hogy használjuk az internetet, vagy képeket, információkat töltünk fel magunkról vagy családunkról. Nem véletlen, hogy a franciák oly kitartóan küzdenek a „felejtés jogának" érvényesüléséért a világhálón.

Az új kommunikációs szisztéma a demokrácia legnagyobb kihívása. Snowden óta tudjuk, hogy mindent összegyűjtenek rólunk, de a mai technológia azt is lehetővé teszi, hogy az információkat egyénre szabva juttassák el hozzánk. Többen felvetik, hogy az amerikai társadalom polarizálódásának egyik fő oka a hírfogyasztás manipulálása. A kirekesztést (magunk önbecsapását) avagy a fragmentációt erősítik az azonos érdeklődésű kiscsoportok, amelyek idegen információt nem fogadnak be. De nincsen választásuk, hogy milyen információkhoz jutnak, a használói létszám növelése érdekében csak az őket érdeklő híreket juttatnak el hozzájuk. Már a hagyományos sajtó is képes volt választásokat eldönteni, a közösségi média ezt még könnyebben megteheti. Ilyen körülmények között **itt az ideje újradefiniálni a szabad választások fogalmát és gyakorlatát, valamint új típusú egyensúlyi rendszert szükséges kidolgozni.**

A virtuális térbe juttatott valótlan tartalmú közlés (legyen az egy fénykép, video, vagy szöveges üzenet) sértheti az adott személy vagy vállalat jó hírnevét, súlyos anyagi és személyes következményekkel járhat. Egy jól felépített rémhíráradat a teljes bankrendszer összeomlását okozhatja. Mindezek kivédésére a nemzetállamok az évszázadok folyamán jogi szankciók egész rendszerét

építették ki. Ezek a védővonalak néhány év alatt semmivé lettek, amikor a nemzetközi hálózatokon terjedő valótlanságokat a hálózatra való felkerüléskor senki nem ellenőrzi, azért senki nem vállal felelősséget. A botrányos videók vagy fényképek már számtalan tragédiát okoztak, de a nézettség növelésében érdekeltek csak látszatintézkedéseket, vagy még azt sem tesznek.

A jó és a káros tartalmak különválasztásakor célszerű lenne az antropológia és evolúciós pszichológia elismert képviselői (Barkow, Dunbar, Bergman) munkásságát is figyelembe venni. Ugyanakkor nem egyszerű ezeket elkülöníteni egymástól, és ezt nem is várhatjuk el egy nyereségorientált globális cégtől. A mai gyakorlat mégis ez. A jó és a rossz különválasztása még az olyan negatívnak gondolt fogalom esetében sem egyértelmű, mint a pletyka. Szvetelszky (2008) szerint valójában „A pletyka nem jó vagy rossz, hanem értékváltó életjelenség, csak meghatározott kortól kezdve kapcsolódott hozzá a negatív jelentéstartalom". Csatlakozik azokhoz a tudósokhoz, akik szerint „a pletykálás az emberi faj egészére jellemző, kisebb közösségekben kialakuló, többszintű (polihierarchikus) szerveződésű kommunikációs hajlam. Nem pletyka az intrika, a rágalom, a fecsegés vagy a mobbing. A mobbing nem egyéb, mint munkahelyi vagy egyéb intézményi – például iskolai – konfliktusokból létrejövő és tovább burjánzó pszichoterror, amelyből tudatos vagy nem tudatos jogsértések származhatnak."

Szvetelszky szerint „a pletyka valamit fenn akar tartani, a rágalom valamit meg akar semmisíteni. A pletyka lehetőséget ad az empátia csoportos átélésére, megerősítve ezzel a csoporttudatot." A pletykának az önelemzés, a kapcsolat-, és közösségteremtés, a konfliktuskezelés, a kudarcfeldolgozás képességeinek elsajátításában lát szerepet.

Az államokra jellemző a propaganda, melyet Rosengren (2004) 2000-ben a következőképpen írt le: „ Propagandán nagyjából olyan, „többé-kevésbé elfogult információt értünk, amit egy kormányzat vagy más hatalmi pozícióban levő szervezet saját érdekei szolgálatára terjeszt". A szó eredete a Sacra Congregratio de Propaganda Fide (Hitterjesztés Szent Kongregációja) című pápai bullára (azaz a pápa által kibocsátott hivatalos dokumentumra) vezethető vissza. A bulla a 16. században Európában megjelenő különböző protestáns mozgalmak ellenében megindult ellenreformáció szellemében született. Ma a „propaganda" szó meglehetősen negatív konnotációkkal rendelkezik, de a tekintély-

elvű rendszerek – például a hitleri Németországban, a sztálini Szovjetunióban és a Mao vezetése alatt álló kommunista Kínában – pozitív értelemben használták. Az Egyesült Államok és a Szovjetunió között folyó hidegháború időszakában a nemzetközi propaganda meglehetősen kiterjedt volt. A jelenség természetesen ma is létezik, annyi különbséggel, hogy gyakran máshogy nevezik, például „nemzetközi hírtermelés" vagy Amerika Hangja (utóbbi egy közismert, hozzávetőleg negyven különböző nyelven sugárzó rádióállomás).

A gazdasági, politikai és vallási ügyeket érintő, közvetett és kevésbé erőszakos jellegű propagandát indoktrinációnak hívjuk. Nincs olyan ország, ahol a tömegkommunikációban megjelenő tartalmak egy része ne lenne indoktrinatív jellegű, és nemcsak a gazdasági és politikai kontextusokban, hanem a szórakoztatásban, a fikcióban és oktatás minden területén is. Általánosan fogalmazva a propaganda és az indoktrináció egyaránt a szocializáció és reszocializáció sajátos esetének tekinthető."

A fentiek tükrében a véleménynyilvánítás szabadsága, a „free speech" korlátok nélküli erőltetése nem csak a nemzetállamok keretében történt évszázados jogi fejlődést teszi semmissé, – így alkalmas azok meggyengítésére, hanem állandósítja az államokon belüli, és az államok közötti konfliktusokat is. Kirívó esetekben, például a terrorizmus éltetése, vagy a gyűlöletbeszéd (hate speech) kérdésében, utóbb már felmerült a korlátozás szükségessége anélkül, hogy az alapkoncepció önkritikus felülvizsgálata megtörtént volna. A politikusok lejáratását pedig a szépen hangzó „karaktergyilkosság" szóval illetik, amely elfedi annak a demokráciát alapjaiban megingató következményeit. Nemrégiben az izraeli ügyészség indított eljárást egy volt miniszterelnökkel szemben azzal a gyanúval, hogy politikustársát lejáratva, arab finanszírozást felhasználva távolította el őt a politikusi pályáról.

A megítélést nehezíti, hogy virtuális térben ma már olyan információ túlkínálat van, amely kikényszeríti az egyén döntését, hogy az adott információt egyáltalán meg kívánja-e ismerni vagy sem. Ezért folyik versengés **a figyelem** elnyeréséért, vagy még inkább a felkeltéséért.

Ha ez mégsem sikerül, az illető:

- átkapcsol másik csatornára,
- megnézi, érkezett-e e-mail – elolvasás nélkül törli,
- vagy az okostelefonján érkezett hírt elolvasás nélkül átlépi.

A Nielsen Globális Digitális Helyzetkép tanulmány szerint 2015-re „mások lettek a TV-nézési szokások, a médiaiparnak a változásokat fel kell karolnia, és stratégiákat kialakítania ahhoz, hogy alkalmazkodjon az új helyzethez, és ezáltal olyan vonzó és fontos tartalmat kínáljon, amit az emberek könnyen el tudnak érni különböző eszközökkel és csatornákon. A személyes találkozásokat, összejöveteleket felváltják a közösségi médián folytatott valós idejű beszélgetések, és a résztvevők ott cserélik ki véleményeiket kedvelt tévéműsoraikról. Társasági esemény lett a közös tévénézés, ami már kilépett a nappali vagy hálószoba falai közül.

A vizsgált országok válaszadóinak nagyobb része, 53 százaléka bizonyos tévéműsorokat azért néz meg, hogy utána tudjon róla csetelni a neten. Továbbá 49 százalék szívesebben megnéz videó programokat akkor, ha azok valamilyen módon kapcsolódnak a közösségi médiához.

A második, harmadik és néha a negyedik képernyő egyrészt megnöveli a nézők választási lehetőségeit, másrészt pedig tartalomszolgáltatóknak, valamint hirdetőknek további alkalmakat nyújt arra, hogy elérjenek nézőket, és kapcsolatba kerüljenek velük."

(http://www.mediainfo.hu/hirek/article.php?id=36278. Utolsó letöltés: 2016. 08.09.)

Komoly erkölcsi kérdéseket vet fel az a tény, hogy a figyelemért folyó versengés nemtelen eszközökkel is folyik. Korábban tiltott volt a mozifilmek képkockái közé rejtett olyan reklám, amely rövidségével csak a **nézők tudatalattijára** hatott. Ma MR (mágneses rezonancia) képalkotó eszközökkel tesztelik az emberi agy befogadóképességét és -készségét egy-egy reklám, vagy termék kapcsán. A legtöbb ország magára hagyja állampolgárait ezekben a kérdésekben, még a következmények felszámolásában sem minden esetben vállal felelősséget.

Tény, hogy minden ország igyekszik megakadályozni a rémhírek terjedését, legfeljebb igyekszik ezt diszkréten tenni. Ez az a terület, ahol a kettős mérce mindennaposnak mondható. Az új típusú kommunikációs csatornák szabályozását, és a negatív hatások megelőzését a Kínai Népköztársaság a többieknél határozottabban teszi, bár eljárása nem felel meg a nyugati elvárásoknak. Példa erre a következő eset:

Több kínai internetes kereskedelmi szolgáltató számíthat büntetésre online hírszolgáltatása miatt, mert a szabályokat megszegve nem hivatalos forrásból származó, hanem maguk által gyártott jelentéseket adtak ki – számoltak be hírügynökségek a kínai internetfelügyelet (CAC) legújabb intézkedéséről.

Az indoklás szerint nyolc vállalat, köztük a Sina, a Sohu, a Tencent, a Baidu, az iFeng és a NetEase nevű helyi internetóriások „súlyosan megsértették" a hatályos szabályokat. A vonatkozó paragrafus szerint ugyanis e portálok *kizárólag hivatalos forrásból származó információk utánközlésére jogosultak a forrás megjelölésével, a tartalom megváltoztatása nélkül."*

E szabályt, mivel betartásukat nem ellenőrizték szigorúan, az érintettek rendre megszegték, s nem ritkán nagy visszhangot kiváltó beszámolókat jelentettek meg.

A szóban forgó profitorientált kereskedelmi vállalatok közösségi média alkalmazásaikkal, mikroblog szolgáltatásukkal százmilliókat érnek el, portáljaikon azonban hivatalosan saját hírek előállítására és terjesztésére nincs engedélyük, újságírókat, szerkesztőket sem alkalmazhatnának.

Amikor tavaly ünnepélyes keretek között először „avattak" online újságírókat, vagyis ellátták őket a hagyományos médiában dolgozóknak járó újságíró-igazolvánnyal, e kereskedelmi portálok nem voltak a munkaadóik között.

A több mint 600 millió kínai internetező hatalmas versenyt generál a szolgáltatók körében, ezért igyekeznek olyan témákkal figyelmet kelteni, amelyek a társadalom jelentős részét mélyen érinti. Közöttük nem ritkák például a környezetszennyezéssel, élelmiszerhamisítással, vagy a rendfenntartók brutalitásával, jogsértésekkel kapcsolatos cikkek.

Egy július elején megjelent CAC-rendelkezés már megtiltotta, hogy a működési engedéllyel rendelkező hírportálok a közösségi médiából ellenőrzés nélkül átvegyenek híreket, híreszteléseket. Ezzel – állításuk szerint – a feltételezésekre és szóbeszédre alapozott, végeredményben „torzított" tartalmú hírek közlését szeretnék megakadályozni.

A sina.com-ot, a 163.com-ot és az iFeng.com-ot, valamint a Tencent szolgáltatót már akkor is megbüntették, amiért valótlan, illetve a tényeket eltorzító történeteket közöltek tudósításokként.
(http://888.hu/article-lebukott-a-kinai-444#, utolsó letöltés: 2016. július 26.)

Hasonló a szuverenitásfelfogása Oroszországnak is, amelyet a következő is bizonyít: 2013-ban új kiegészítést fogadott el az orosz törvényhozás a 2008-as, 149. számú internet-törvényhez. (Megjelent a «Российская газета» című lap, № 6271 számában, 2013. december 30-án) A *398-as számmal jegyzett törvény* a szélsőséges tartalmakat megjelentető site-ok **azonnali, *bírósági ítélet nélküli blokkolását*** teszi lehetővé. A Roszkomnadzor (Médiafelügyelet, Internetfelügyelet) a legfőbb ügyész utasítására köteles haladéktalanul kikapcsol(tat)ni azokat az internetszolgáltatókat, amelyek oldalain tömeges zavargásokra, a közrend megbontására vagy szélsőséges cselekményre szólítanak fel.

A nemzetközi folyamatokat árnyalja, hogy az állami szereplők mellett olyan globális vállalkozások tevékenykednek, melyek mozgástere meghaladja az előbbiekét. A legnagyobbak szolgáltatók döntenek a közlések, információk sorsáról. Jó és rossz között kell választaniuk, hiszen vagy elérhetővé teszik az információt, vagy nem. Teszik mindezt a saját szabályzataik szerint, bírói vagy más kontroll nélkül (különösen fájó a civil kontroll hiánya). Újabb adatok szerint például a Facebook a nemzetállamok törlési kéréseinek sem mindig tesz eleget, még akkor sem, ha azt jogerős bírói ítélet támasztja alá (Denardis, 2014). Ezen napi gyakorlat világosan kirajzolja a **virtuális tér új erővonalait**. *Ismételten rámutat a nemzetállamok és a klasszikus hatalmi ágak hagyományos felfogásának tarthatatlanságára.*

A virtuális térben kívánatos az államok és a nagy szolgáltatók közötti együttműködés, erre még van is remény, de a kisebb – főként nem állami – szereplők becsatlakozása szinte teljesen átláthatatlan. Néhány tőzsdei spekuláns finanszírozásában a sajtószabadság ürügyén ezrével képezik ki a „civil újságírókat", akiket ezután akár fizetett blogger-ként lehet foglalkoztatni. Az általuk közölt információkat független, megbízható forrásból származónak tűntetik fel, pedig csak a manipuláció eszközei. A virtuális tér tehát ma sem mentes a pénztőke befolyásától.

A hamis információk romboló hatásait felnagyítják, azok időbeliségét felgyorsítják a kibertérre épülő, új típusú kommunikációs csatornák. Minél több információt ismer meg, fogyaszt az emberiség a kibertérből, annál fontosabb lenne a hagyományos média etikájának megújított formájú alkalmazása. A folyamatok abba az irányba mutatnak, hogy a média, mint önálló hatalmi ág elveszíti befolyását, helyét az internetszolgáltató cégek vezetőségei veszik át.

(Ennek leképeződését lásd a következő fejezetben a vállalkozások rangsorának átrendeződésénél.)

A helyzet komolyságát mutatja Oroszországnak az a kezdeményezése, hogy az államok fogadják el az **„információs háború" tilalmát**, amely ráirányítja a figyelmet a virtuális tér egyik legjelentősebb kérdésére. Ennél a pontnál érdemes felidézni a II. világháború után elfogadott ENSZ Alapokmány rendelkezéseit a háború tilalmáról és a belügyekbe való be nem avatkozásról. A valóság már régen túlhaladta ezeket a rendelkezéseket azzal, hogy az országok egy csoportja nem tartja magát ezekhez az elvekhez. Teszik mindezt anélkül, hogy bármilyen szankció érné őket magatartásuk miatt. Oroszország az információs háború tilalmáról szóló javaslatával még mindig ragaszkodik ezekhez az elvekhez, de ennek bevezetéséhez politikai egyetértésre, míg kikényszerítéséhez egy újfajta nemzetközi szankció-rendszerre lenne szükség. Kína is hasonló javaslatokat terjesztett elő, míg a nyugati országok a jelenlegi információs status quo fenntartásában érdekeltek.

5. Versengés a kibertérben

5.1. A geopolitikai szereplők

A digitális gazdaságra való átállás alapja a nagymennyiségű adat, melyet egyre inkább a gépek memóriáiban tárolunk (lásd a kibertér fogalmát a 3. fejezetben). Kulcsfontosságú tehát, hogy ki uralja az adatközpontokat, az azokhoz vezető kiber-kommunikációs útvonalakat és mindazon szoftvereket (alkalmazásokat), és hardvereket, amelyek az adatokhoz való hozzáférést biztosítják.

A kibertér elemzése azért is igényel geopolitikai megközelítést, mert valóban forradalmi változások kezdődtek el, amikor a gazdasági, pénzügyi, társadalmi és politikai folyamatokat egyaránt a kibertérre alapozzák. Új iparágak alakulnak ki mint az adatipar, mások mint az információ-ipar, megújulnak. Mindezek alapja pedig az **információ**. Kialakul a közösségi (másnéven megosztott) gazdaság (shared economy), amely rátelepül a határokon átnyúló infokommunikációs hálózatokra. A közösségi gazdaság az olyan eddig állandónak bizonyult alrendszereket is érintheti, mint a nemzeti pénzkibocsátás, vagy a nemzetközi pénzügyi közvetítő rendszer.

A geopolitikai következmények is hasonlóak lesznek, mint más ipari forradalmak esetén: egyes országok, régiók felértékelődnek, mások elbuknak. Európában nehéz elhinni, hogy többleterőfeszítések nélkül nem tartható fenn tovább sem az életszínvonal, sem a világban elfoglalt, eddig kivívott szerep. Könnyű volt az európai döntéshozók éleslátását elhomályosítani az ismétlődő görög válságokkal, a hirtelen kirobbant ukrán válsággal, amely újra a melegháború rémét idézte fel a kontinensen. Legújabban pedig a migránsválság okoz kezelhetetlennek tűnő konfliktusokat, miközben folyik a digitális forradalom, és minden erőfeszítést ennek kellene alárendelni. Szerencsére van kivétel, amely példa megmutatja, hogy átgondolt, stratégiai irányvonal mentén egy ország még előnyt is remélhet a forradalmi változásokból. Ez a kivétel pedig Nagy-Britannia, amely kiberstratégiája mentén világos és várhatóan sikeres politikát készül megvalósítani.

A mostani folyamatok az Egyesült Államok kapitalizmusának világméretű győzelmét vetítik előre. Az általa évtizedek óta szorgalmazott globalizáció beteljesüléseként az új technikai találmányok (internet, okostelefon), és az ezeken áramló információk ugyanolyan erővel alakítják át a társadalmi, gazdasági, és pénzügyi viszonyokat, mint, azt tette az első kapitalista ipari forradalom a XVIII-XIX. századi Angliában. A hatás még ennél is nagyobb a kulturális területen, annak minden negatív következményével együtt. A forradalmi változások közül kiemelendő a munkaerőpiac globális átalakulása, amely alapvetően sérti a nemzetállami adózási rendszereket (mint eddig ezt tették az offshore területek Nagy-Britanniában, az USA-ban, az EU egyes országaiban és Ázsiában egyaránt). A nemzeti bevételek elmaradása a nemzeti felelősségi körökben maradó feladatok által igényelt forrásmennyiségtől, tovább erodálja a belső biztonságot és a békés egymás mellett élést.

Az **Amerikai Egyesült Államok** több hivatalos dokumentum szerint nemzetbiztonsági ügyének tekinti nemcsak a saját területéhez köthető kibertérrel kapcsolatos kérdéseket, hanem a globális információs útvonalak szabad átjárhatóságát egyaránt. Ezeket az érdekeit akár katonai erővel is kész megvédeni.

Oroszország: a hagyományos állami szuverenitás (az ENSZ Alapokmányában foglaltak szerint) talaján állva foglal állást a felmerülő kérdésekben. Álláspontja

szerint kibertér egyáltalán nem létezik, az csak a nyugati országok szemfényvesztése. Információs tér létezik, mellyel kapcsolatban a nemzetállamoknak továbbra is hasonló hatáskörük, feladatkörük van, mint a hagyományos sajtóval kapcsolatban.

Kína: Elsősorban a saját belső stabilitását óvja, ezen kívül aktív résztvevője a nemzetközi együttműködésnek. A második Internet Világkonferencia (WIC2015) megnyitóján Xi Jinping mint a világ legtöbb internethasználóval rendelkező ország elnöke beszédében számos kérdést érintett a kiberbiztonságtól a globális internetirányításig.

Az alábbiakban a legfontosabb gondolatait emeljük ki:
„*A kiberbiztonságról*
- A kibermegfigyelés, kibertámadások és kiberterrorizmus globális veszélyekké váltak.
- A kibertér nem válhat szabad harctérré, ahol országok küzdenek egymással, és ugyancsak nem szabad a bűnözés melegágyává válnia.
- Nem lenne szabad kettős mércét alkalmazni a kiberbiztonság fenntartásánál.
- Nem elfogadható, hogy egy vagy néhány ország biztonságos legyen, míg a többiek ki legyenek téve a veszélyeknek, és az országok nem törekedhetnek úgynevezett abszolút biztonságra önmaguk részére más országok biztonságának veszélyeztetése árán.
- Az összes országnak együtt kellene működnie az információtechnológiával való visszaélések kordában tartása, a kibermegfigyeléssel szembeni fellépés, valamint a kibertérbeli fegyverkezési verseny megállítása érdekében.

A kiberszuverenitásról
- A szuverén egyenlőség elvét az Egyesült Nemzetek Alapokmánya is tartalmazza, mint a jelenkori nemzetközi kapcsolatok egyik alapnormáját. Ez magában foglalja az államok közötti kapcsolatok minden aspektusát, így a kiberteret is.
- Tiszteletben kellene tartanunk az egyes országok arra vonatkozó jogát, hogy önállóan megválasszák saját kiberfejlődésük útját, valamint hogy egyenlő súllyal vegyenek részt a nemzetközi kibertér irányításában.

A kiberirányításról

– A kibertérre vonatkozóan jelenleg fennálló szabályok aligha tükrözik az országok többségének elképzeléseit és érdekeit.
– Nem lenne szabad egyoldalúságnak fennállni [az internetirányítási rendszer létrehozásában]. A döntéseket nem csak egyetlen félnek kellene meghoznia, illetve nem csak néhány félnek lenne joga erről tárgyalni egymás között.
– A kibertérben egyaránt szükséges a szabadság és rend.
– A kibertér nem esik kívül „a törvényi szabályok által lefedett területen".

A Kína általi nyitásról

– A kínai internet robusztus növekedése jelentős piacot biztosított minden ország vállalatai és startup vállalkozásai részére. Kína nyitott kapui soha nem fognak bezárulni. A külföldi befektetésekre vonatkozó kínai politika nem fog változni."
(http://www.wuzhenwic.org/2015-12/16/c_47742.htm. Utolsó letöltés: 2016. augusztus 13.)

Nagy-Britannia: kifinomult eszközökkel rendelkezik a lehallgatás, kiberbefolyásolás területén, a transzatlanti optikai kábelek nagy része a területén halad keresztül. Az Egyesült Államokhoz fűződő különleges kapcsolatait kihasználva (például egy hamisított titkosszolgálati jelentéssel rá tudta venni az USA-t az iraki háború megvívására), a Five Eyes országokat eszközül használva képes lehet visszaszerezni az I. világháborúban elveszített globális hatalmi pozícióját. Nagy előnye az átgondolt stratégia.

Az Európai Unió: országai nem egységesek, 2016. év elején fogadták el az új adatvédelmi irányelveket, amelyek azonban csak 2018-ban lépnek életbe. Előremutató viszont az internet semlegességével kapcsolatos szabályozási elképzelés. A francia bírói rendszer aktivizmusát kivéve mindenki arra vár, hogy a másik ország lépjen elsőként, a másik ütközzön elsőként az USA-val. Eközben az Egyesült Államok behozhatatlan előnyt szerzett, de a fejlődésbeli intenzitás-különbség az előny növekedését vetíti előre. Lássunk erre egy példát:

„Miközben az Unió évek óta dolgozik azon, hogy felhő-nagyhatalommá váljon, úgy tűnik, egyelőre nem jöttek be a számításai. 2012-ben még Neelie Kroes jelentette be az Európai Felhő Társaság (European Cloud Partnership) kezdeményezést, amelynek egyértelmű célja volt, hogy valamiféleképpen helyzetbe hozza az európai felhőszolgáltatókat a már akkor is domináns amerikaiakkal szemben. És mivel a felhős piacnak egyre jobbak a növekedési kilátásai, a verseny is egyre keményebb.

A Gartner becslése szerint csak a felhőbe költözés mintegy 1000 milliárd dollárnyi forgalmat generál öt év alatt.

Négy amerikaié a piac 40 százaléka

Az IDC adatai viszont azt mutatják, hogy minden erőfeszítés ellenére egyelőre inkább az amerikai szolgáltatók sikeresek az európai piacon is. A The Wall Street Journal egy összeállítása szerint például az olasz Enel energiaipari konszern is az Amazont választotta külső szolgáltatónak tavaly.

Elemzők szerint az amerikai szolgáltatók egyszerűbben olcsóbbak, mint az európai konkurenseik – még úgy is, hogy az európai áraik rendre magasabbak, mint az otthoniak. Az Amazon például ugyanazt Frankfurtban mintegy 8 százalékkal kínálja drágábban, mint pl. Virginiában, és az új szolgáltatások sem jelennek meg azonnal a globális piacon, hanem csak kisebb-nagyobb csúszással az amerikai piac után. Ezt a csúszást azonban bőven ellensúlyozza fejlesztési tempójuk.

Ez némileg megmagyarázza az IDC számait, melyek szerint jelenleg a nyugat-európai IaaS-piac 40 százalékát négy amerikai cég uralja: az Amazon, a Microsoft, az IBM és a Google. Ha a globális piacot nézzük, még nagyobb a súlyuk: a Synergy Research egy közelmúltban kiadott elemzése szerint a globális felhős piac 54 százalékát birtokolja ez a négy cég. Ráadásul növekedési ütemük gyorsabb, mint a piacé, így részesedésük is nőni fog."
(http://bitport.hu/az-amerikai-szolgaltatok-az-europai-piacot-is-lenyuljak)

5.2. Nyugat-Európa az Amerikai Egyesült Államok kiber védőernyője alatt

A II. világháború után az Amerikai Egyesült Államok nukleáris védőernyő alá helyezte a hozzá kötődő országokat. Mivel ezeknek az országoknak sem anyagi, sem technikai lehetőségük nem volt nukleáris katonai kapacitások

kiépítésére, ezért a bipoláris szembenállás idején elfogadták azt, hogy országukat végső soron az Amerikai Egyesült Államok nukleáris rakétákkal is megvédje. A Német Szövetségi Köztársaság esetében ez kényszerűség volt, de a többiek anélkül élvezték ezt a fajta biztonságot, hogy annak teljes árát megfizették volna. Két nyugat-európai ország volt az, amelyik saját nukleáris atomütőerőt épített ki, egyrészt Nagy-Britannia, másrészt Franciaország.

Ehhez a helyzethez hasonló a mostani, amikor a jelentős gazdasággal bíró országok is elfogadják az Egyesült Államok „kiber védőernyőjét".

A nukleáris védőernyő és a kiber védőernyő közötti különbségek:

- a kiber-védőernyő nemcsak véd, mint a nukleáris, de az amerikai cégek összegyűjtenek minden adatot, így lehetőségük van a korábbi partnereket megelőzni a kiberversenyben (a digitális gazdaság kiépítésében),
- a kidolgozás és a továbbfejlesztés jelentős versenyelőnyt jelent az USA-nak, és közvetlen partnereinek (Five Eyes),
- növeli az agyelszívást és ezen keresztül a társadalmi feszültségeket,
- a közvetlen pénzügyi előnyök is az USA-cégeknél jelentkeznek.

Németország kényes helyzetben

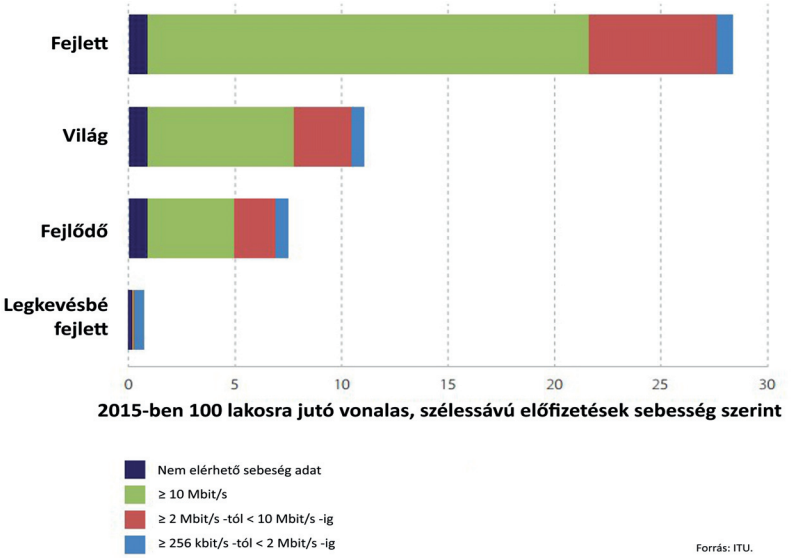
Németország egyrészről szívesen megspórolná az ICT-beruházások költségeit, különösen, hogy az európai egységes piac nem tudta kitermelni magából azokat a multinacionális befektetőket, akik felvehetnék a versenyt az amerikai erőfölénnyel. Ezen kívül szembe kell néznie az agyelszívással, azzal, hogy a német fiatalok egyre gyakrabban gondolkodnak amerikai karrierben. Ulfkotte (2014) szerint a helyzetet súlyosbítja a német sajtóban elterjedt korrupció.

Másrészt – bár kicsit megkésve – ráeszmélt arra, hogy az adatvagyont (beleértve az állampolgárok tömegeinek személyes adatait) az USA-beli cégek veszik birtokukba. E nélkül pedig döntő versenyhátrányba kerül a digitális gazdaságra való átállásban. Németország arról sem mondhat le, hogy a vezető ICT-iparágakban ne fejlesszen, miközben – elsősorban politikai okokból – mindezidáig tartózkodott az USA-cégekkel való nyílt konfrontációtól.

Más esetekben is kézzelfogható, hogy Németország versenyképességét csökkentő gyakorlatot folytatnak multinacionális cégek, a felhőszolgáltatást drágábban kínálják, vagy – ugyanazon árért – csak kisebb sávszélességű, vagy

lassabb internet-szolgáltatást nyújtva. (Lásd: a gazdasági és belügyminiszter együttes fellépése a kivételező internet-szolgáltatás ellen.) Válaszul önálló felhőszolgáltatást fejleszt Németország, ami egyrészt elkésett, másrészt inkább az Egyesült Államok kiber-védőernyője alá kellene helyeznie magát, ahogyan ezt teszi a BMW, amikor beköltözik az Amazon által nyújtott felhőbe.

5.3. A technológiai versengésről

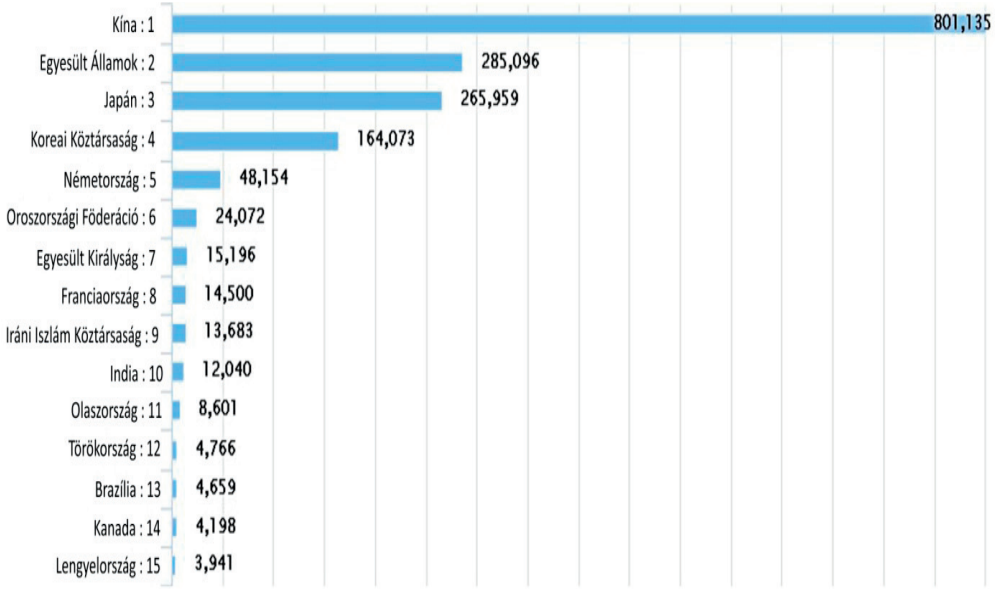


Az Egyesült Államok ma is élen jár az innovációban; kezdeti előnyét jól példázza az operációs rendszerek penetrációja. Barabási (2003, pp. 119–120) pontosan leírja, hogy

„…a Windows elterjedt annak ellenére, hogy a Microsoft nem az első jelentkező volt ezen a területen. Amikor a Windows első változata megjelent, úgy nézett ki, mint az Apple forradalmian új operációs rendszerének rosszul sikerült koppintása. Az Apple azonban mereven ragaszkodott hardverének monopóliumához, miközben a PC szabad utat adott az összes számítógépgyártónak. Ezért a PC-k lettek a számítógépek által uralt világunkban az uralkodók, és a hullám hátára vette Bill Gatest és az ő Windowsát.

Az operációs rendszerek piacán azonban az ilyen egészséges verseny és hierarchia teljesen hiányzik. Igaz, hogy nem csupán a Windows az egyetlen operációs rendszer. Minden Apple-terméken továbbra is fut a Mac Operációs Rendszer, a Macos. A DOS, a Windows előfutára még ma is sok PC-n fut. A Linux, a mindenki számára ingyenes operációs rendszer, és a Microsoft egyetlen kihívója – piaci részesedése növekszik. Az Unix többségében sok számolást igénylő számítógépeken fut, amelyet kizárólag kutatók és hálózati mérnökök használnak. De mindezen operációs rendszerek eltörpülnek a Windows árnyékában, amelynek különböző változatai a PC-k hihetetlenül nagy részén – 86%-án – zümmögnek. A második legnépszerűbb operációs rendszer, az Apple Macos rendszere, csak a piac 5%-ával rendelkezik. Ezt az ősi DOS követi szorosan 3,8%-kal, és utána a Linux következik 2,1%-kal. Minden más operációs rendszer – beleértve az Unixot is – a piac kevesebb, mint 1%-át birtokolja."

A 2003-ban leírt állapotot mára árnyalja, hogy a Google új operációs rendszert készít az IoT-k számára, és Oroszország is fejleszt. A technikai fejlesztéseket jól ábrázolja az egy országra jutó szabadalmi bejelentések száma. A **találmányi bejelentések** számánál Kína elsöprő fölényt mutat (2014).



forrás: world-statistics.org

A **szuperszámítógépek**kel kapcsolatban a 2016. augusztusi adatok új kínai fejlesztést mutattak ki:

„Lassan növekszik a szuperszámítógépek hatékonysága a legfrissebb **Green500 lista** szerint. Az elmúlt egy évben a top 10 átlaga szinte nem változott, a teljes listára levetített javulás pedig csak 20 százalék körüli. Ennek ellenére még van ok az optimizmusra, a készítők látnak még lehetőséget a nagyobb mértékű javulásra.

A lista első helyét továbbra is a Japánban található Shoubu foglalja el, mely Haswell-EP Xeon processzorokat és PEZY-SC gyorsítókat vonultat fel, melyek kombinációjával 6673,8 MFLOPS/watt eredményre képes. A második pozícióba egy nagyon hasonló konfiguráció mászott fel, a Satsukiban található processzorok és gyorsítók típusa egyezik, a rendszer számítási kapacitása

Green500 Rank	MFLOPS/W	Site*	Computer*	Total Power (kW)
1	6,673.84	Advanced Center for Computing and Communication, RIKEN	Shoubu - ZettaScaler-1.6, Xeon E5-2618Lv3 8C 2.3GHz, Infiniband FDR, PEZY-SCnp	149.99
2	6,195.22	Computational Astrophysics Laboratory, RIKEN	Satsuki - ZettaScaler-1.6, Xeon E5-2618Lv3 8C 2.3GHz, Infiniband FDR, PEZY-SCnp	46.89
3	6,051.30	National Supercomputing Center in Wuxi	Sunway TaihuLight - Sunway MPP, Sunway SW26010 260C 1.45GHz, Sunway	15,371.00
4	5,272.09	GSI Helmholtz Center	ASUS ESC4000 FDR/G2S, Intel Xeon E5-2690v2 10C 3GHz, Infiniband FDR, AMD FirePro S9150	57.15
5	4,778.46	Institute of Modern Physics (IMP), Chinese Academy of Sciences	Sugon Cluster W780I, Xeon E5-2640v3 8C 2.6GHz, Infiniband QDR, NVIDIA Tesla K80	65.00
6	4,112.11	Stanford Research Computing Center	XStream - Cray CS-Storm, Intel Xeon E5-2680v2 10C 2.8GHz, Infiniband FDR, Nvidia K80	190.00
7	3,775.45	Internet Service (B)	Inspur TS10000 HPC Server, Intel Xeon E5-2620v2 6C 2.1GHz, 10G Ethernet, NVIDIA Tesla K40	110.00
8	3,775.45	Internet Service (B)	Inspur TS10000 HPC Server, Intel Xeon E5-2620v2 6C 2.1GHz, 10G Ethernet, NVIDIA Tesla K40	110.00
9	3,775.45	Internet Service (B)	Inspur TS10000 HPC Server, Intel Xeon E5-2620v2 6C 2.1GHz, 10G Ethernet, NVIDIA Tesla K40	110.00
10	3,775.45	Internet Service (B)	Inspur TS10000 HPC Server, Intel Xeon E5-2620v2 6C 2.1GHz, 10G Ethernet, NVIDIA Tesla K40	110.00

azonban lényegesen kisebb, az overheadnek betudhatóan a teljesítmény/fogyasztás mutatója csak 6195,22 MFLOPS/watt. Mindkét rendszer a japán állami kutatóintézet-hálózat RIKEN intézetében található, előbbi a számítástechnikai és kommunikációs, utóbbi pedig az asztrofizikai részlegen működik.

A többé-kevésbé kísérletinek tekinthető, széles skálázódás helyett hatékonyságra optimalizált, PEZY-alapú szuperszámítógépeket azonban rögtön a legnagyobb hal, a TOP500-at vezető Sunway TaihuLight követi – ez elképesztően nagy dolog, és jól mutatja, **milyen hihetetlenül hatékony architektúrával támadnak a kínaiak**. A kínai fejlesztésű gép 6051,3 MFLOPS/watt eredménye nagyjából 10 százalékkal marad el az első helyezettől, ami annak fényében ragyogó eredmény, hogy a rendszerben nyoma sincs Intel processzoroknak vagy épp Nvidia (vagy PEZY) gyorsítóknak, itt saját fejlesztésekről van szó.

Ennél nagyobb probléma, hogy bár Moore törvénye szerint a szilíciumlapkára integrálható tranzisztorok száma kétévente megduplázódik, ennek hatékonyságra gyakorlott hatása nem tükröződött megfelelően az elmúlt időszakban. Amennyiben nem történik pálfordulás, úgy nehezen lesz tartható a 2020-ra prognosztizált első exascale (exaflops nagyságrendű) rendszer megjelenése. Ahhoz, hogy egy ilyen rendszer értelmezhető módon megépíthető legyen, a szakértők szerint nagyjából 50 GFLOPS/wattos mutatót kellene elérni, ami közel hétszerese a jelenlegi listavezető Shoubu 6,67 GFLOPS/wattos értékének.

A hatalmas ugráshoz szükséges lesz alapjaiban újragondolni a rendszerek felépítését, mint ahogy azt a Sunway TaihuLight esetében tették a kínai mérnökök. A rekorder gép ugyanis bizonyos helyeken inkább visszafejlődött, a gyorsító tárak és a memóriák felépítése egyszerűbb lett, kapacitásuk pedig csökkent. A rendszerben található 1,3 petabájt memória például elenyésző a 93 petaflopsos számítási kapacitáshoz képest, ez a szuperszámítógépek esetében általánosnak mondható 1 bájt per FLOPS értékhez képest csupán 0,014 bájt per FLOPS értéket eredményez. Megfelelő optimalizációkkal ezt sok esetben mégis sikerült kompenzálni, ami a **TOP500-ban első,** a Green500-ban pedig harmadik helyet jelentett.

Mindez jó példával szolgálhat egy eltérő, hatékonyabb irányhoz, ami az újabb technológiákkal párosítva (rétegezett memória, fejlettebb gyártástechnológiák, 3D XPoint, stb.) újraindíthatja a teljesítmény/fogyasztás mutató nagyobb mértékű emelkedését." (Asztalos, 2016)

(http://www.hwsw.hu/hirek/55984/green500-top500-szuperszamitogeplista.html, Utolsó letöltés: 2016.08.09.)

5.4. Technológiai trendek

A Távközlési Unió adatai szerint hétmilliárd ember (a világ lakosságának 95%-a) lakik olyan területen, amelyet mobiltelefonos hálózat fed le. A szélessávú mobil hálózatok (3G vagy fejlettebb verzió) elérik a világ lakosságának 84%-át, de a falun élő lakosság esetén ez az arány csupán 67%. Az LTE (negyedik generációs) hálózatok az elmúlt három év során gyorsan elterjedtek és mára már közel 4 milliárd embert érnek el (a világ lakosságának 53%-a), alaposan javítva az internet-felhasználás minőségét.

A Gartner Inc. 2015. október 6-án tette közzé a 2016-ban érvényesülő tíz legfontosabb technológiai trendet, amelyek stratégiai jelentőséggel bírnak majd a legtöbb szervezet számára. A Gartner a stratégiai technológiai trendeket olyan irányzatokként definiálja, amelyek valószínűleg erőteljes befolyást gyakorolnak az adott szervezetre. Erőteljes befolyásoló tényezőknek nevezhetjük mindazokat, amelyeknek hiánya fennakadásokat okozhatna a cégeknél, a végső felhasználóknál vagy az információ-technológia területén, amelyek tetemes beruházásokat igényelnek, vagy amelyeknek kései bevezetése jelentős kockázattal jár. Ezek a technológiák kihatással vannak a szervezet hosszú távú célkitűzéseire, programjaira és kezdeményezéseire.

„A Gartner 10 elsődleges stratégiai technológiai trendje egészen 2020-ig alakítani fogja a digitális üzletág fejlődését" – nyilatkozta David Cearley alelnök és a Gartner elemzője. „Az első három trend a fizikai és virtuális világok egybeolvasztásával, valamint a digitális háló kifejlesztésével kapcsolatos. Noha a szervezetek napjainkban elsősorban a digitális üzletágra összpontosítanak, az algoritmikus üzletág is feltörekvőben van. **Az algoritmusok – a kapcsolatok és összefonódó rendszereik – határozzák meg az üzleti világ jövőjét.** Az algoritmikus üzletágban sok minden zajlik a háttérben, melybe az emberek nincsenek közvetlenül bevonva. E folyamat mozgatórugói az okos

gépek, amelyekhez a következő három trendünk kapcsolódik. Az utolsó négy irányzat az IT új valóságát érinti, az új strukturális és platformtrendeket, amelyek a digitális és algoritmikus üzletág támogatásához szükségeltetnek."

A 10 elsődleges stratégiai technológiai trend 2016-ra tehát a következő:

- Az eszközháló
- A felhasználók környezetélménye
- 3 dimenziós nyomtatás
- Információtár (Information of Everything)
- Fejlett gépi tanulás
- Autonóm segítőtársak és tárgyak
- Alkalmazkodó biztonsági struktúra
- Fejlett rendszerstruktúra
- Hálóalkalmazás és szolgáltatásstruktúra
- Tárgyak Internete platformok

Fejlesztések, amelyek újabb technikai forradalmat generálnak

A mesterséges intelligencia mellett a britek által fejlesztett kvantumszámítógép hozhatja meg azt a nagy áttörést, amely elvezet a valóban forradalmi változásokhoz. Nem lesz szükség nyelvtanulásra, mert a fordítógép ott lehet a szemüvegünkben. Mindennaposak lesznek a robotok, és nem csak az internet vagy a telefon másik végén, hanem a szomszéd szobában is. Fejlődnek a számítógép memória és az adatátviteli rendszerek, életünket egyre több algoritmus irányítja. Eközben Oroszország olyan új programnyelvet fejleszt, amely újrafogalmazza az ember-gép kapcsolatát, és amely lehetővé tenné a teleportálást.

Néhány újdonság a közelmúltból:

> „A Facebook és a Skype egyaránt kísérletezik olyan megoldásokkal, hogy normál emberként feltűnő, de valójában mesterséges intelligencia által vezérelt csevegő partnereket építenek be a chatprogramokba – a Skype-on eddig a Bing kereső és a Getty Images kapott ilyen interfészt, ahol például sima beszélgetés formájában juthatunk el odáig, hogy milyen fotót keresünk az interneten.

A napokban került be a Skype-ba több új robot is, többek között a repülőjegyeket értékesítő Skyscanner, az utazási információkkal és szállás-helyekkel foglalkozó Hipmunk, a koncertekre, eseményekre belépőket árusító Stubhub, valamint a testre szabható üzeneteket küldő IFTTT. Emellett egy olyan szolgáltatás is elindult, amelynek elsőre nem nagyon látjuk értelmét, de persze nagyon cool – a Spock Bot a Star Trek univerzumból ismert karaktert személyesíti meg, és "a vulkáni logikával kapcsolatban" lehet vele beszélgetni." (Bátky, 2016)

„A Delft Műszaki Egyetem szakemberei olyan adattárolót fejlesztettek, ami 500-szor jobb, mint a ma létező legjobb merevlemez. A kutatók a klór atom pozícióit használták fel adategységként, így 100 nanométeren 1 KB információt sikerült eltárolniuk. Bár ez elsőre nem hangzik túl soknak, ez azt jelenti, hogy egy nagyjából 6,4 négyzetcentiméteres helyen 62,5 TB információ fér el.

A tudósok egy pásztázó alagútmikroszkóp segítségével keverték össze a klóratomokat a rézatomok felületén. Ennek köszönhetően olyan adatblokkok jöttek létre, amik pont úgy néznek ki, mintha QR-kódok lennének. Ezekben az egységekben tárolták el a kívánt információt.

Bár a megoldás igazán páratlan, keresni egyelőre felesleges a boltok polcain, a megoldás ugyanis csak -196 Celsius fokon működik." (hvg.hu, 2016)

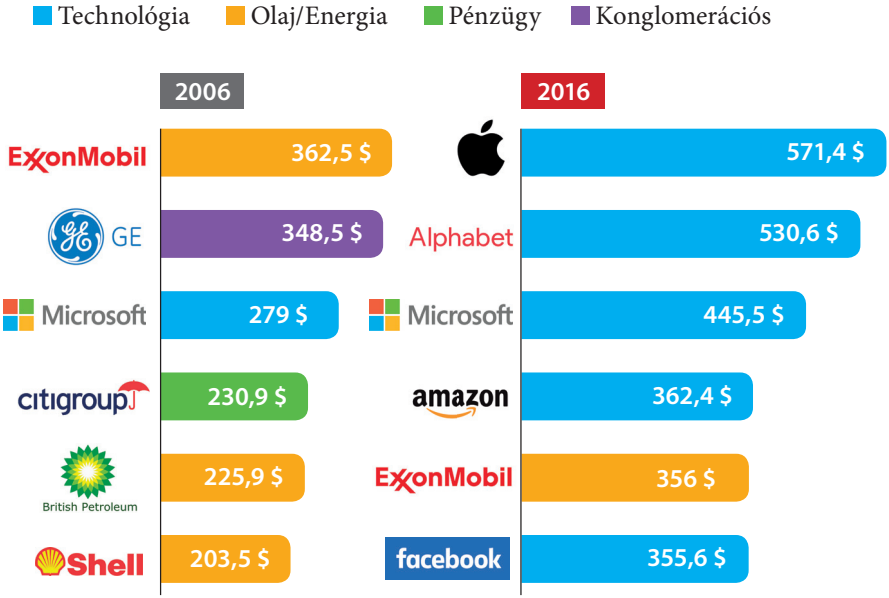
5.5. Felvásárlások és egybeolvadások

A fejlesztéseken kívül a hatalmi versengéseket jól példázzák a felvásárlások és egybeolvadások (mergers and aquisitions – M&A) is, amelyekből további következtetéseket vonhatunk le. Ne feledjük, hogy a vezető információ-kommunikációs cégek kevés idővel rendelkeznek, de tetemes a készpénzállományuk:

„Az Apple a világ leggazdagabb vállalata, és ez furcsa módon eléggé idegesíti a cég részvényeseit. A készpénztartalék a legutóbbi tőzsdei jelentések szerint 194 milliárd dollárra nőtt, ez pedig azért nem tetszik a tulajdonosoknak, mert csak áll parlagon, ahelyett, hogy a cég befektetné, kutatás-fej-

Eközben az **amerikai technológiai vállalatok** elfoglalták a világelső helyeket:

Tíz évvel ezelőtt a világ egészen más hely volt: jórészt hagyományos cégek uralták



A számok milliárd dollárban értendők. Forrás: Yahoo! Finance, Forbes, 2016. augusztus 1.

Bármilyen hihetetlen, de évtizede nem voltak a mai értelemben vett okostelefonok, s a **Facebook** is még gyerekcipőben járt. Akkor az olaj- és energiaipari (a diagramban sárga csík), a pénzügyi vállalkozások (zöld), és a konglomerátumok (lila) voltak a meghatározók, messze a high-tech cégek (kék) előtt.

Mint a Statista ábrázolja, 2006-ban tőkeértékben az **ExxonMobil** amerikai olaj- és gázcég, John D. Rockefeller Standard Oil nevű cégének utódja állt az első helyen 362 milliárd dollárral.

Augusztus elején a világ hat legértékesebb társasága közül az első az **Apple** volt (571 milliárd dollár), második az **Alphabet** (lánykori nevén: **Google**), majd a **Microsoft** és az **Amazon**.

Az **ExxonMobil** a tíz évvel ezelőttihez képest kicsit szerényebben ötödik, s ott kapaszkodik a sarkában a **Facebook**.

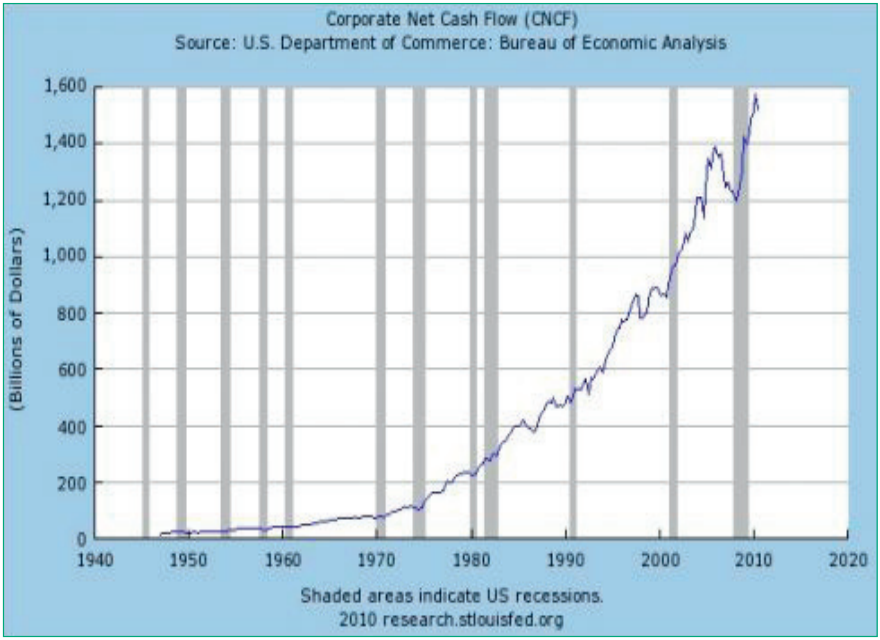
lesztésre, terjeszkedésre, felvásárlásokra költené, vagy akár osztalékként szétosztogatná a részvényesek között. Csakhogy ez nem olyan egyszerű, a pénz nagy része ugyanis adóoptimalizálási okokból az Apple európai leányvállalatánál van Írországban, onnan pedig Amerikába bevinni 35% adó megfizetésével járna." (Hanula Zsolt, 2015)
(http://index.hu/tech/2015/05/15/na_es_ha_az_apple_megvenne_gorogorszagot/ Utolsó letöltés: 2016.08.13.)

„A Moody's hitelminősítő 2013-as értékelése szerint az Apple kaliforniai konszern által összegyűjtött 147 milliárd dollár az amerikai cégek készpénztartalékának 10 százalékát teszi ki (ez az összeg 2015-re elérte a 150 milliárd dollárt – szerk.).

A Moody's a tanulmány elkészítésekor összesen több mint 100 olyan tengerentúli társaságot vizsgált meg, amelyekről rendszeresen készít beszámolókat. A készpénztartalék több mint 62 százaléka 50 vállalat birtokában van. Az első öt helyen négy IT-óriás található, sorrendben az Apple, a Microsoft, a Google, a Cisco. A TOP5 tagja még a Pfizer gyógyszergyártó; ennek az öt piaci szereplőnek a tulajdonában van a készpénztartalék több mint 25 százaléka. Az Apple annak ellenére van kiváló pénzügyi helyzetben, hogy tavaly év vége óta jelentős osztalékot fizetett ki és részvényeket vásárolt vissza. A vállalat tavaly márciusban jelentette be hatalmas készpénz-visszajuttatási programját, amelynek keretében összesen 45 milliárd dollárt költ el. Ennek ellenére a társaság 2012 vége óta körülbelül 9,5 százalékkal növelni tudta a tartalékát.

Az eredmények tükrében egyáltalán nem meglepő, hogy a legnagyobb készpénzmennyiséget, 515 milliárd dollárt a technológiai szektor halmozta fel. A második helyen az egészségügy és a gyógyszeripar található. Az IT-vállalatok kimagasló szereplése nem véletlen, hiszen a digitális javak értékesítése nem igényli a termékek mozgatását, miközben az adók jelentős része is megtakarítható. Az Apple belső dokumentumában azt írta, hogy a készpénztartalékának kereken 70 százalékát, több mint 100 milliárd dollárt tart külföldön, hogy elkerülje az USA-ban az adók fizetését. A Moody's becslése alapján ugyanez elmondható az amerikai óriáscégek teljes kész-

Az amerikai cégek készpénzállománya milliárd dollárban



pénztartalékának 62 százalékáról. A külföldön tartott összeg a tavaly év végi 840 milliárd dollárról 900 milliárdra nőtt, s a tendencia a közeljövőben aligha változik majd meg." (Berta, 2013) (https://sg.hu/cikkek/100254/hatalmas-mennyisegu-keszpenzen-ul-az-apple. Utolsó letöltés: 2016.08.14.)

A legújabb felvásárlások más fontos trendet jeleznek:

„Megvásárolta a korábban GraphLabként, illetve Dato néven is ismert, mesterséges intelligencia platformot fejlesztő Turit az Apple. A cég nem közölte hivatalosan a felvásárlás összegét, egyes források 200 millió dollárról beszélnek…

…Az Apple Siri virtuális asszisztensével a vetélytársaknál korábban elkezdte a különböző mesterséges intelligenciára építő megoldásokat lát-

ványosabban is a felhasználók szolgálatába állítani, termékét ugyanakkor a gyors rajt ellenére mára jórészt beérték a rivális megoldások, mint a Google Asszisztens vagy az Amazontól ismert Alexa – utóbbi az elmúlt év során látványos fejlődésen ment keresztül**.** Az említett online óriásoknak egyébként komoly előnyük, hogy hatalmas mennyiségű felhasználói adathoz férnek hozzá, míg az Apple jóval érzékenyebben kezeli ügyfelei információit. A vállalat egyelőre az egyre népszerűbb chatbotok felé sem mozdul, pedig a területre több óriás, mint **a** Facebook vagy a Microsoft is fogad, víziójuk szerint a botok jelentik a következő generációs UI platformot.

A felvásárlás az Apple-nek is komolyabb lökést adhat a területen, noha hogy pontosan mire használja majd a frissen szerezett kompetenciát egyelőre nem tudni – az AI-asszisztensek közötti verseny mindenesetre egyre szorosabb, a Google és a Microsoft termékei is szinte hónapról hónapra lesznek okosabbak." (Hlács, 2016)

(http://www.hwsw.hu/hirek/55978/apple-felvasarlas-akvizicio-turi-gepitanulas.html, Utolsó letöltés: 2016.08.08.)

Mesterséges intelligencia-startupot vásárol fel az Intel (digit.mandiner.hu/cikk/20160811, 2016. augusztus 11. 08:30)

A Microsoft nemrégiben vásárolta meg a LinkedIn szolgáltatót, amivel hatalmas mennyiségű személyes adat és személyes kapcsolati háló került a birtokába.

A **tőzsdei adatok** elemzésével további összefüggéseket fedezhetünk fel:

A TWILIO nevű cég részvényárfolyamának elemzése során felvetődik, hogy egy jelenleg veszteséget termelő, mindössze 28 ezer aktív felhasználóval rendelkező, 2007-ben alapított vállalat részvényárfolyama miért emelkedhetett néhány hét alatt a sokszorosára. A cég okos telefonokra fejleszt alkalmazásokat. A TWILIO részvényértékében már most is megmutatkozó piaci lehetőséget valójában az jelenti, hogy *a jelenlegi hardver- és hálózatigényes kommunikáció helyett, a kommunikáció áthelyeződhet az alkalmazásokon belüli kommunikációra.*

5.6. Új bipolaritás felé

A kibertér geopolitikájának jövőjét elsősorban az innováció, a technikai fejlesztések dominálják. Ez adja meg azt a keretet, amelyben a két világhatalom a stratégiáját kidolgozza és végrehajtja. Mindketten kiemelkednek abban, hogy képesek hosszabb távon gondolkodni, ezt Kína évezredes történelméből örökölte, míg az Egyesült Államok a megnyert világháborúk és a globalizáció építésében szerzett tapasztalataiból meríti. Matolcsy (2015) szerint „Az elmúlt kétszáz évben végig az jellemezte az amerikai politikát, hogy egyre pontosabb és mélyebb prognózisok alapján hozta meg stratégiai és politikai döntéseit, de ebben is fordulatot hozott a két világrendszer megszűnése. Amerika, bár csatákat vesztett, sőt hadjáratokat is – az 1812-es angol-amerikai háborút –, de végül megnyerte azt a hosszú, mintegy két évszázados háborút, amelyet a világhatalomért vívott. Ma egyedüli világhatalomként arra is képes, hogy a stratégiai elemzőműhelyekben kialakult „világforgatókönyvek" alapján ne csupán alakítsa a jövőt, hanem előre is hozza azt."

Toffler (1980, p. 22.) szerint: „Az emberiség előtt kvantumugrás áll – a jövőbe. Minden idők legmélyebb társadalmi felfordulásával és alkotó újrarendeződésével nézünk szembe. Anélkül, hogy világosan felismernénk, miről is van szó, mindannyian részt veszünk egy jelentős, új civilizáció megépítésében, mégpedig az alapoktól kezdve. Ez a harmadik hullám értelme.

Mostanáig az emberi faj két nagy változási hullámon ment keresztül. Mindkettő nagyjából eltörölte a korábbi kultúrákat vagy civilizációkat, és olyan életmódot hozott a helyükbe, ami a korábbi emberek számára elképzelhetetlen volt. A változás első hulláma – a mezőgazdasági forradalom – több ezer év alatt játszódott le. A második hullám – az ipari civilizáció kialakulása – csupán háromszáz évig tartott. Mára a történelem még jobban felgyorsult, és valószínű, hogy a harmadik hullám néhány évtized alatt végigsöpör történelmünkön és kiteljesedik."

„A harmadik hullám a családok szétszakításával, a gazdasági élet megrázkódtatásaival, politikai rendszereink megbénításával, értékeink összezúzásával mindenkire kihatással van. Próbára teszi a hatalmi viszonyokat, veszélyezteti a mai elitek előjogait és kiváltságait, és megteremti azt a hátteret, amely előtt meg fogják vívni a hatalmi harcokat a holnapi kulcspozíciókért. […] Információs bomba robban fel életünk kellős közepében, képek repeszeit

záporozva mindannyiunkra, és drasztikusan megváltozatja valamennyiünk világfelfogását és magánéleti viselkedését egyaránt." (Toffler, 1980, pp. 167–179)

Elemzésünknél induljunk ki a két fő szereplő jelenlegi helyzetéből:

Amerikai Egyesült Államok

A korábbi ipari forradalmakból győztesen került ki, ahogy a világháborúkból egyaránt.

Tervezési és szervezési ismeretei, az innovációk felkarolásának és menedzselésének kifinomult rendszere párosul a stratégiai gondolkodásmóddal. A katonai fejlesztésekből rutinszerűen képes polgári alkalmazásokat bevezetni a piacra. Globális hatalmi szerepét a II. világháború után tovább erősítette, élére állva a nemzetállamok érdekeit gyakran sértő globalizációnak. Ennek keretében előbb uralma alá vette az információipart (hír- és filmgyártás, reklámtevékenység stb.), majd globális termelési és szolgáltatási hálózatokat épített ki. Ezzel párhuzamosan az ENSZ transznacionális vállalatok nemzetközi szabályozási kezdeményezéseit blokkolta. Kiépítette a globális adatátviteli és szállítási hálózatait, melyeket felhasználva globális pénzügyi szolgáltatóipart működtet. Dominálja a jogi fejlődést a független média, a független igazságszolgáltatás, a független nemzeti jegybankok és a független civil szervezetekre vonatkozó szabályok előírásával, miközben ezen szabályok egy részét magára nézve nem tartja kötelezőnek. Kiépített egy új iparágat az adatipart, ennek hatékony felhasználásával a Földön elsőként képes átállni a digitális gazdaságra.

Katonai szervezete a világon a leghatékonyabb, melyet saját érdekei mentén nem fél alkalmazni. Szövetségi rendszere erős, bár a kibertérben az „Öt szem" országokkal (Nagy-Britannia, Kanada, Ausztrália és Új-Zéland) kivételes kapcsolatban áll. Az utóbbi évek téves háborúi azonban kikezdték a nemzetközi reputációját, azok pénzügyi, pszichés, valamint szociális-egészségügyi következményei még hosszú ideig fognak negatívan hatni.

Eladósodottságát fedezetlen pénzkibocsátással és más országok erőforrásainak bevonásával kezeli, a hitelminősítők rá nem alkalmazzák a szokásos elemzési módszereket.

A belső társadalmi feszültségekkel nem néz szembe, a Financial Times által is szorgalmazott új kapitalizmust nem képes bevezetni. A politikai rendszer a lobbi-csoportok által korrumpálódott. Felismerve, hogy a kutatás és fejlesztés emberi erőforrásai Ázsiába igyekeznek, képes megújulni, az agyelszívás új módszereit vezette be.

Kínai Népköztársaság

Évezrednyi történelme során talán most először vállal globális szerepet. Erőteljes modernizációt hajt végre, a saját viszonyaira adaptálva a megelőző ipari forradalmak tanulságait.

Modernizációját tőkefelhalmozással kezdte, olcsó munkaerejére támaszkodva jelentős exportoffenzívába kezdett. 2016. február elejére elérte, hogy a világ legnagyobb devizatartalékával, 3,23 ezer milliárd dolláros tartalékkal rendelkezett, 1,53 ezer milliárd dolláros külső adósság mellett, azonban ez utóbbinak túlnyomó része jüanban denominált külföldön kibocsátott kötvény volt. Mindeközben 2015 áprilisában 1,23 ezer milliárd dollárnyi amerikai államadósság volt a kezében. A legutóbbi gazdasági világválság óta Kína volt az USA legnagyobb hitelezője.

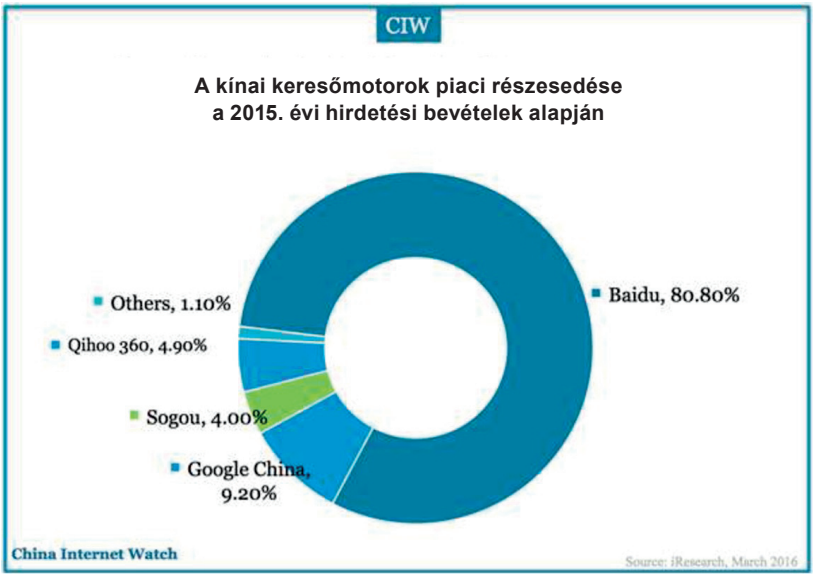
A sokszor alacsony hozzáadott értékű és jövedelmezőségű bérmunkákat is felvállalva importálta a termékelőállítási és munkaszervezési ismereteket, és átvéve a Japán példát, ezeket továbbfejlesztve hamarosan a legnagyobb gyártók konkurenciájaként jelentkezett. Jelentős haladást ért el a pénzügyek területén, de az Egyesült Államoktól eltanulta, hogy a katonai fejlesztéseket felhasználva, azokból hogyan lehet jövedelmező polgári termékeket és szolgáltatásokat előállítani.

Mindeközben hatékonyan védi belső piacait, és igyekszik elkerülni a 4. ipari forradalom sokkszerű, a nyugati világ által eddig figyelmen kívül hagyott, romboló hatásait. Elsőként kötött nemzetközi kibermegállapodásokat az Egyesült Államokkal és Oroszországgal.

Kínát nagyságrendje, potenciálja és az évezredeken nyugvó, sajátos gondolkodása emelte olyan szuperhatalommá, amely az Egyesült Államok mellett egyedül rendelkezik az állami szuverenitás teljességével.

Ebből a hirdetési árbevételek 10,55 milliárd dollárt értek el, amely az előző évhez viszonyítva 32,2%-os emelkedést jelentett.

A Baidu kínai vállalat továbbra is dominálja ezt a piacot, a hirdetési árbevételek több mint 80%-ának megszerzésével, melyet a Google China követ 9,2 %-kal.



(https://www.chinainternetwatch.com/17415/search-engine-2012-2018e (Utolsó letöltés: 2016.08.13.)

Annak ellenére, hogy a kibertérben a fragmentáció kimutatható, és a politikai, gazdasági versengés egyértelmű, **az új bipolaritás – ellentétben az előzőtől – a kooperációra** épül, nem a totális szembenállásra. Ennek elemzéséhez vegyünk egy mindennapi példát, amely jól mutatja a kínai-amerikai együttműködést:

Az iResearch szerint 2015-ben az összes kínai keresőmotor-szolgáltató cég éves árbevétele elérte a 12,48 milliárd dollárt, ez 34,7%-os emelkedést jelentett. Az ilyen, és hasonló – közös hasznot hozó – együttműködések száma jelentős, elég, ha az IBM együttműködésére utalunk számítógépek gyártásának átadásáról.

5.7. A kibertér orosz felfogása és szabályozása[1]

Internet felhasználók

Oroszország a világ legnagyobb országa: 11 időzónát fed le, kelet-nyugat irányban a két szélső pont között 8000 km a távolság. Össznépesség 146,5 millió,

1 Az elemzést Horváth Péter Oroszország szakértő, a Geopolitikai Tanács Közép-Ázsia Kutatóközpontjának volt vezetője készítette

73,7 százalékuk városlakó. A milliósnál nagyobb 13 nagyvárosban összesen 29,5 millióan. A keleti és északi országrészben a népsűrűség nullához közeli. Az ország földrajzi adottságai miatt is óriási jelentősége van az internetnek, mint az idő- és térbeli korlátoktól mentes kapcsolattartás eszközének.

A legtöbb internet felhasználó Közép-Oroszországban van (19,8 millió, melyből 7,3 millió Moszkvában), és minden hatodik orosz nyelvű felhasználó a Volga-vidéken (11 millió), vagy Északnyugat-Oroszországban él (10 millió).

Az internet az orosz üzleti élet és a mindennapok fontos részévé vált: az országosan több mint 80 millió internetes felhasználó közül 62 millióan naponta kapcsolódnak fel a hálózatra.

A legkedveltebb orosznyelvű kereső a Yandex. ru (a Google nagy riválisa a térségben) egyébként szépen olvassa a latin betűs kereséseket is.

Az orosznyelvű internetes domain hálózat, a „runet" felhasználóinak 54 százaléka nő. Az internetezők több mint fele 35 év alatti. A gemiusAudience kutatási projekt adatai azt mutatják, hogy minden harmadik orosz internet felhasználó a 25–34 éves korosztályba esik. Ötből egy runet felhasználó18 és 24 év közötti, illetve 35–44 éves, míg minden hatodik a 45–54 éves korcsoportba tartozik. Az orosz nyelvű weboldalak látogatói között a legkisebb csoport az 55 év feletti korosztály.

A runet közösség az iskolai végzettség szempontjából is változatos. Több mint egyharmaduk szakmunkás képesítésű, valamivel kevesebben rendelkeznek felsőfokú diplomával. Az orosz internet felhasználók több mint negyedének van középfokú végzettsége. FORRÁS http://www.gemius.hu/uegynoeksegi-hirek/az-orosz-internet-felhasznalokrol.html

(A gemiusAudience egy nemzetközi kutatási projekt, melyet a Gemius több mint 35 országban végez Európában, Észak-Afrikában és a Közel-Keleten. A kutatás célja, hogy az internet felhasználók száma és demográfiai profilja mellett azt is meghatározza, hogy milyen módon használják az internetet. A projektet a Gemius saját módszertana és az ICC / ESOMAR nemzetközi előírásainak megfelelően végzik.)

A digitális iparág (közösségi média, mobil, online videó és közösségi vásárlás) folyamatosan bővül a közép-kelet-európai régióban. Ezen belül a CCE régió online populációjának közel 40%-át az orosz, 16 százalékát a török felhasználók adják.

Az oroszországi internetes kábelhálózat térképét az alábbi helyen lehet megtalálni:

(https://yandex.ru/maps/?source=serp_navig&text=кабельная%20сеть%20интернета%20в%20россии&sll=41.903948%2C57.281988&sspn=70.136719%2C18.097794&ll=41.903948%2C57.281988&z=4&sctx=CAAAAAIAa9WuCWnPQkD%2FPuPCgeBLQJP8iF%2BxhuQ%2Faw2l9iLa3T8EAAAAAAECAxQAAAAAAAAAAAAAAAAAAA1QAAAAGs%2F38%2FAAAAAAAAAAA%3D)

Természetesen külön kábelrendszer köti össze a nagy oroszországi és nemzetközi IREX-eket (Inter-Exchange Carrier, nemzetközi szállítmányozási cégeket például Hamburgban, Amszterdamban, Frankfurtban).

Az Oroszországi Föderáció és az Amerikai Egyesült Államok közötti mélytengeri optikai kábelhálózat fejlesztése állandónak tekinthető folyamat. Közös beruházásban valósul meg az Alaszka felé vezető új vonal kiépítése. Részletesebben lásd: https://sg.hu/cikkek/115467/orosz-kemhajok-a-tengeralatti-internetkabeleknel

IT szolgáltatók

Az Oroszországi Föderációban az IT szolgáltatást biztosító vállalkozások száma több ezerre tehető – ezek nagyságrendje is rendkívül változatos. Van olyan szolgáltató, amely csupán egy-egy irodaházat, vagy néhány háztömböt lát el telefóniával és internettel, de országos méretű ellátást biztosító cégek is működnek (nagy telefontársaságok). A helytől és az egyes régiók fejlettségétől függően a hálózatot üvegszálas vagy rézdrótos vezetékekből építik fel – a műholdas megoldás Oroszországban is nagyon drága. A szolgáltatók gyakorlatilag mind hazai tulajdonú magánvállalkozások, az alkalmazottak is meghatározóan hazaiak.

A működési engedélyeket az Oroszországi Föderáció Hírközlési és Informatikai Minisztériuma adja ki. Egy átlagos szolgáltató tevékenységéhez az alábbi licenceket köteles megszerezni:

- adatforgalmazás hangszolgáltatás nélkül,
- hangos adatforgalmazás,
- helyi telefonszolgáltatás,
- távadat-szolgáltatás,
- felhasználói hálózat kiépítése és működtetése.

Ezeken felül be kell mutatnia
- az alkalmazott programok jogszerű használatát igazoló engedélyt,
- szerződést valamely biztonságtechnológiai céggel (pl.: Kaspersky, ESET)

valamint
- egy szolgáltató rendszert és eszközállományt biztosító céggel (például AddPac) kötött felhasználói jogosultsági szerződést.

Törvényi környezet

Az IT szektor működésének jogi környezetszabályozása Oroszországban is követő jellegű: a technológiai fejlődésből adódó, illetve a piaci versenyből következő kihívásokra próbál törvényhozási, politikai, állami válaszokat adni.

A rendkívül nagyszámú törvényhelyeket áttekintve kiemelendő két fontos jogszabály. Az első a ***2000.szeptember 9***-én életbe lépett ***„Az Oroszországi Föderáció Információbiztonsági doktrínája”***. A dokumentum alapvetése, hogy a kérdéskörben érvényes állami politikát mindenki megismerhesse. A biztonság fontos tényezőjének tartja a hazai fejlesztésű és gyártású IT eszközök elterjesztését, továbbá az érzékeny információk elleni támadások megakadályozását, az információs és kommunikációs eszközök védelmét. (FORRÁS http://www.femida.info/14/19002.htm)

Ezt az alapvető dokumentumot több alkalommal is aktualizálták, illetve kiegészítették – ezek sorában a legújabb a ***2013. július 24-én kiadott 1753. számú elnöki rendelet***, amely ***2020-ig terjedő időszakra*** határozza meg az Oroszországi Föderáció ***állami politikáját*** a nemzetközi információs biztonság témakörében.

A dokumentum célja, hogy előmozdítsa a nemzetközi információs biztonság ügyét, beleértve a jogi, szervezeti környezet korszerűsítését, továbbá a különböző országok közötti technológiai színvonal kiegyenlítését, az információs és kommunikációs technológiáknak a reálgazdaságba való általános bevezetését.

A nemzetközi információs biztonság fogalmán a globális infó-tér olyan állapotát értik, amelyben kizárható a személyiségi jogok, társadalmi és állami érdekek megsértése, valamint a kritikusan érzékeny nemzeti információs infrastruktúrák elleni jogszerűtlen és destruktív tevékenység.

A dokumentum a ***fenyegetettség*** négy területét különíti el:

- a katonai-politikai célú, agresszív, az állami szuverenitást támadó, az ország területi egységét veszélyeztető információs tevékenység
- terrortámadások érzékeny infrastruktúrák ellen, terrorista-toborzás
- közrend megsértése való felbujtás, nemzetiségi, faji, vallási ellenségeskedés szítása, rasszista és idegengyűlölő propaganda terjesztése, gyűlöletkeltés
- számítógépes információkhoz való jogtalan hozzáférés, ártalmas számítógép programok létrehozása, használata és terjesztése.

A nemzetközi információs biztonság kérdéskörében az Oroszországi Föderáció kezdeményező szerepet kíván vinni. Aktivitását kétoldalú, sokoldalú, regionális és globális szinteken fejti ki.

Kezdeményezi, hogy az ENSZ tagállamai – orosz javaslatra – fogadjanak el egy ***nemzetközi konvenciót*** az információs biztonság erősítéséről.

Javasolja ***rendszeres szakértői konzultációk*** megtartását

- a Sanghaji Együttműködés (https://en.wikipedia.org/wiki/Shanghai_Cooperation_Organisation),
- a Független Államok Közössége (https://hu.wikipedia.org/wiki/Független_Államok_Közössége),
- a Kollektív Biztonsági Szerződés Szervezete (u.ott), a BRICS (https://hu.wikipedia.org/wiki/BRICS),
- az Ázsiai-Csendes óceáni Gazdasági Együttműködés https://hu.wikipedia.org/wiki/Ázsiai_és_Csendes-óceáni_Gazdasági_Együttműködés),
- a Nyolcak, a Húszak Csoportjának tagállamai, további országok és nemzetközi szervezetek részvételével.

Szorgalmazza, hogy ***tegyék nemzetközivé az internet irányítását*** és ebbe vonják be az Nemzetközi Távközlési Uniót (*International Telecommunication Union, ITU, az ENSZ szakosított intézménye*).

A felvázolt feladatok sikeres elvégzése érdekében szakértői csoportot kell létrehozni, amely alkalmas az elképzelések elemzésére, tudományos és módszertani elemzésére.

Tovább kell erősíteni a Sanghaji Szerződés tagállamai által elfogadott ***Egyezményt***, amely a nemzetközi információs biztonság növelését célozza.

(A megállapodást Jekatyerinburgban, 2009. június 16-án fogadták el, életbe lépett 2012. január 5-én. FORRÁS: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf)

Az orosz fél szorgalmazza, hogy további országok is csatlakozzanak ehhez a megállapodáshoz. Az Oroszországi Föderáció javasolja, hogy nemzetközi egyezménnyel tiltsák be az ***információs fegyver*** alkalmazását és terjesztését.

Olyan nemzetközi programok kidolgozását és megvalósítását javasolja, amelyek hozzásegítenek a fejlett és feljövő országok között meglévő ***informatikai egyenlőtlenségek*** csökkentéséhez.

Oroszország kezdeményezőként is hozzá kíván járulni a ***globális információs hálózatok és rendszerek*** létrehozásához, amelynek alapja a nemzeti informatikai infrastruktúrák fejlesztése. (FORRÁS http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=178634;fld=134;dst=1000000001,0;rnd=0.880983740257514)

Figyelmet érdemel, hogy az ***2015-ik évi 683. számú elnöki rendelet***, amely az Oroszországi Föderáció nemzetbiztonsági stratégiáját tartalmazza, a II. bek. 21-22 pontjában külön is említést tesz az információs biztonságról (FORRÁS) http://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html).

Az információs tér működését meghatározó ***alapvető törvénynek tekinthető*** az (elfogadása óta számos alkalommal módosított) ***2006. július 14-én életbe lépett, 149-es számú „Szövetségi Törvény az információról, információs technológiáról és az információ védelméről”*** (FORRÁS http://rg.ru/2006/07/29/informacia-dok.html).

A 149-es számú törvényt az elmúlt néhány évben jelentős kiegészítésekkel ***módosították***. Ezek közül kiemelendők az alábbiak:

A 2012-ben elfogadott 139 sz. szövetségi törvény, amely ugyan alapvetően a gyermekek egészségét és fejlődését károsan befolyásoló információk elleni védelmet szolgáló korábbi jogszabály módosítását célozza, mégis – egy sor más vonatkozó törvény kiegészítéseként – az internet tartalmak szűréséről, a tilalmas tartalmakat közlő site-okat felsoroló ***Egységes Nyilvántartás*** létrehozásáról és a fekete listára került oldalak letiltásáról intézkedik. (FORRÁS http://rg.ru/2012/07/30/zakon-dok.html)

Az idézett törvénymódosítás egyebek mellett bevezeti a (6, 12, 16, 18 éves) ***korhatár feltüntetését*** minden olyan tartalom esetén, amelyhez gyerekek is

hozzáférhetnek. A törvény részletesen szabályozza a korhatáros tartalmak minősítésének módszereit is. Egyúttal intézkedik arról, hogy kiskorúak számára elérhető terekben számukra korlátozni kell az internet hozzáférést.

Lényegi változást jelent, hogy jogszabályban ***pontosítja az internet site, internet oldal, domain név, hálózati cím, internet site tulajdonosa, hosting provider fogalmakat.***

Előírja, hogy az Egységes Nyilvántartásban meg kell nevezni mindazon domain neveket, web oldalakat, szolgáltatókat, amelyek az orosz szövetségi törvények szerint tilalmas tartalmakat terjesztenek (gyermekpornográfia, tájékoztatás kábítószerek beszerzési helyeiről illetve előállításáról, öngyilkossági módok bemutatása, öngyilkosságra bíztatás, kiskorúak terhére elkövetett bűncselekmények ismertetése, továbbá minden olyan tartalom, amelynek terjesztését bíróság tiltja meg).

A nyilvántartásba vételről (a fekete listára való felkerülésről) a ***Roszkomnadzor*** illetékese dönt. Az intézmény a szövetségi Távközlési Minisztérium felügyelete alá tartozik, 2008 óta hivatalos neve: Távközlési, Információs Technológiai és Tömegtájékoztatási Szövetségi Felügyeleti Szolgálat. ld. később.

A tilalmi listára felkerült tartalmakat az üzemeltető, illetve a tulajdonos köteles haladéktalanul eltávolít(tat)ni, ellenkező esetben az oldalhoz való hozzáférést a szolgáltató blokkolja.

A nyilvántartásba vétel maximum 90 napon belül bíróságnál megtámadható.

A tiltólista 2012. november 1-től az ***eais.rkn.gov.ru*** nem nyilvános honlapon ismerhető meg az érintett szolgáltatók számára.

Megjegyzendő, hogy erre a törvényre hivatkozva 2012-ben nyolc, 2013-ban 3 esetben került a tiltási nyilvántartásba internetes tartalom, illetve weboldal.

2013-ban az orosz törvényhozás újabb kiegészítést fogadott el az 2008-as, 149. számú internet-törvényhez. (Megjelent a «Российская газета» című lap, № 6271 számában, 2013 december 30-án)

A ***398-as számmal jegyzett törvény*** a szélsőséges tartalmakat megjelentető site-ok azonnali, ***bírósági ítélet nélküli blokkolását*** teszi lehetővé. A Roszkomnadzor (Médiafelügyelet, Internetfelügyelet) a legfőbb ügyész utasítására köteles haladéktalanul kikapcsol(tat)ni azokat az internetszolgáltatókat, amelyek oldalain tömeges zavargásokra, a közrend megbontására vagy szélsőséges cselekményre szólítanak fel.

A törvény alapján 2014. március 13-án egyszerre három, független szerkesztőségi politikát folytató internetes portál elérhetőségét korlátozta a hatóság: a grani.ru, a kasparov.ru és a Jezsegynevnij zsurnal oldalait. Ugyancsak a feketelistára került Alekszej Navalnij ellenzéki személyiség blogja a Zsivoj zsurnal internetes lapon és az Echo Moszki rádió online változatán.

2014 végén a Facebook és a Vkontakte hálózat – a Médiafelügyelet követelésére – blokkolta a Navalnij támogatására szervezett felvonulásról szóló információt.

Oroszországi jogvédők ezt a törvénymódosítást is az internet nyílt cenzúrázása eszközének tekintik. Az orosz elnök emberjogi tanácsa szerint is a törvénymódosítás korlátozza az állampolgárok alkotmányos jogait és szabadságát.

2014-ben további, az internet működését befolyásoló jogszabályokat fogadott el az orosz törvényhozás. (FORRÁS https://hi-tech.mail.ru/review/internet_zakony_2014/)

Ezek egyike például ***megtiltja, hogy orosz állami intézmények honlapjait külföldi szolgáltatók kezeljék***. A jogszabály elfogadását átfogó felmérés előzte meg. Ebből kiderült, hogy a vizsgált kilencezer állami intézmény, illetve állami tulajdonú vállalat egyharmada külföldi (elsősorban Egyesült Államokbeli, továbbá németországi) szerverekről működtette honlapjait. Részletezve: a külhoni hostingok szolgáltatásait 1560 költségvetési, 1320 államhatalmi szerv, 720 önkormányzat és 350 stratégiai jelentőségű vállalat vette igénybe. A jogszabálytervezet vitája során orosz szakértők felhívták a figyelmet arra, hogy kizárólag oroszországi felhő alapú szolgáltatások használhatók, ám amennyiben ilyenek nem állnak rendelkezésre, akkor az állami intézmények számára tiltani kell a felhő alapú-számítástechnikai megoldások igénybevételét.

2015. szeptember 1-vel lépett életbe az a törvény, amely előírja, hogy az oroszországi állampolgárok ***személyes adatai*** kizárólag Oroszország területén tárolhatók. A törvény a 2006-ik évi 152. számú, a személyes adatokról szóló szövetségi törvényt módosítja.

A ***„blogger-törvény”*** (97 számú Szövetségi Törvény 2014. május 5.) (FORRÁS http://rg.ru/2014/05/07/informtech-dok.html) újabb kiegészítése a 2006-os, 149. számú első médiatörvénynek. Eszerint minden olyan site és/

vagy internetes oldal, közösségi háló tulajdonosa, vagy működtetője, amely nyílt tartalmat közöl és ***napi látogatottsága legalább 3000*** (és egy-egy csatlakozás időtartama meghaladja a 15 másodpercet), köteles betartani valamennyi, az internetre és általában a tömegtájékoztatási eszközökre érvényes törvényeket. Vagyis a bloggerek ***ugyanolyan elbírálás alá esnek, mint általában az internet-szolgáltatók***. A bloggerek kötelesek regisztráltatni magukat az internethatóságnál (Roszkomnadzor). A blogger-törvényt egyebek mellett a 2013. decemberi, volgográdi pályaudvari és trolibuszos robbantásos terrorcselekményekre hivatkozva vezették be. A média felügyelet egy felmérése szerint a bloggerek körében feltárt törvénysértések 91%-a trágár kifejezések használata és náci jelképek bemutatása, 6%-a kábítószer propagálása, 3% pedig szélsőséges cselekményekre való felbujtás.

A 2014-es internetes jogszabályalkotás során életbe lépett a ***„kalózkodás elleni törvény"***, amely a szerzői jog megsértésével közreadott tartalmak tilalmát és szankcionálását kiterjeszti az internetre is.

Hatályossá vált a ***spam-ellenes jogszabály***, amely a reklámtartalmak küldését a felhasználó előzetes, írásos hozzájárulásához köti. A nyilatkozattal megszerzett jogot a reklám-kibocsátó harmadik fél számára nem adhatja tovább. A jogszabály indoklásakor fontos szempont volt, hogy egy előzetes felmérés szerint a mobil-használók 76%-át zavarják a kéretlen reklámok.

A törvényhozás bevezette az ***anonim internetes pénzátutalás tilalmát, illetve korlátozását***. A jogszabály szerint természetes személyek naponta 60 ezer, havonta 200 ezer rubelt (cca. 1 millió HUF) utalhatnak át interneten, miután azonosították magukat mobil telefonszámmal, személyi igazolvány számmal és/vagy adószámmal, tb-számmal, nyugdíjbiztosítási számmal.

Felügyeleti hatóság

A hatóságot mai formájában 2008-ban hozták létre. A Távközlési Minisztérium irányítása alatt működő testület hivatalos neve: ***Távközlési, információs technológiai és tömegtájékoztatási szövetségi felügyelet (Roszkomnadzor).***

A Felügyelet ***szervezeti struktúrája***:

- Távközlési engedélyezési osztály
- Távközlési ellenőrzési és felügyeleti osztály
- IT felügyeleti osztály

- Személyes adatvédelmi jogok osztálya
- Média-engedélyezési osztály
- Média ellenőrzési és felügyeleti osztály
- Jogi osztály
- Szervezési osztály
- Igazgatási osztály

Feladat- és kompetenciaköre összetett. A hagyományos médiahatósági feladatkörökön (pl. frenkvenciakiosztás, médiafelügyelet) túl kifejezetten az IT szektorra vonatkozóan az alábbiakat lehet kiemelni:

- Egységes, automatizált információs rendszer létrehozása, amely tartalmazza mindazon domain neveket, honlapokat és hálózati címeket, amelyeken tiltott tartalmak jelentek meg (Egységes Nyilvántartási Rendszer, amit tiltó, vagy feketelistaként is említenek).
- A nyilvános hálózatok operátorainak nyilvántartásba vétele.
- Tartalom felügyeleti szervezet és szakértői csoport létrehozása, működtetése.
- A személyes adatokat kezelő operátorok nyilvántartásba vétele.
- Szolgáltató vállalkozások engedélyezése, bejegyzése.

FORRÁS http://rkn.gov.ru/about/

A szabályozás hatékonysága, új kihívások

Az állami szabályozás eddigi hatásairól készített összefoglaló (FORRÁS http://www.gazeta.ru/ tech/2016/01/03/8000057/legislative-control-of-internet-in-russia-2015-results.shtml) szerint az internet használók ***biztonságát az állami szabályozás nem növelte***. Azokat egyébként is a biztonsági szempontból érzékeny objektumok és vállalatok infrastruktúrájának védelmére vezették be.

A felhasználók számára a legnagyobb fenyegetést továbbra is az ***internetes bankokat támadó*** trójai vírusok, adatlopások jelentik, továbbá a zsarolóvírusok tömeges elterjedése.

Egyre veszélyesebb támadások érik a ***mobil-internetezőket***, különösen veszélyeztetettek a legelterjedtebbek: a Windows és az Android rendszereket alkalmazók – de várható, hogy már 2016-ban sorra kerülnek az Apple és a Linux operációs rendszerek is.

2014–2015-ben tömeges mértékben detektáltak olyan rosszindulatú programokat, amelyek a ***routereket támadták***, hasonló támadásnak vannak kitéve az internetes játékok, az okos órák, megfigyelő kamerák használói is. Ezek ellen vírusvédelemmel, de legfőképpen tudatos géphasználattal, az általános internetes műveltségi színvonal emelésével lehet tenni.

Prognosztizálható továbbá, hogy 2016- várhatóan tovább éleződik a Google és az orosz Yandex közötti ***konkurencia háború***.

IT szakma és politika

2015. december 21-én tartották meg az első IT szakmai konferenciát Oroszországban. (FORRÁS http://www.gazeta.ru/tech/2015/12/22/7985363/future_of_russian_it.shtml) Az ***„Internet gazdálkodás jövője"*** című fórumon megjelent ***Vlagyimir Putyin*** államfő is, aki az elé tárt javaslatok közül messzemenően támogatta a ***hazai programfejlesztést*** – kedvezményeket és állami megrendeléseket, nyílt protekcionizmust ígérve, természetesen WTO kompatibilis módon – továbbá megerősítette, hogy tovább kell szigorítani az Oroszországban működő ***külföldi IT cégek ellenőrzését***.

A fórum résztvevői kiemelték, hogy a hazai fejlesztések célja – az import kiváltásán túl – ***Oroszország „IT szuverenitásának"*** megőrzése. Külön hangsúlyt kapott, hogy a ***szakemberképzés*** során a hallgatók ne elsősorban a Cisco és a Microsoft termékeit, hanem az azokat kiváltó hazai eszközöket ismerjék meg.

Az internetes biztonság kérdéskörében elhangzott, hogy nem csupán a személyes adatokat, hanem a ***magáninformációkat*** is kizárólag hazai tárhelyeken legyen lehetséges elhelyezni. Ez utóbbin olyan adatokat értenek, amelyek birtokában egyes cégek – például a Google – keresőmotorjai irányított, kvázi személyre szabott reklámokat tudnak küldeni a felhasználóknak. A téma szakértői siettek leszögezni, hogy a külföldi tárhelyek tilalma nem a személyes adatok ellenőrzését, hanem az adatok kontroll nélküli felhasználásának megakadályozását célozza.

Az ágazat iránti kitüntetett politikai figyelem jeleként értékelhető, hogy Putyin elnök felajánlotta a 2015 februárjában létrehozott Internet fejlesztési Intézet vezetőjének, ***German Klimenko***-nak, hogy ***elnöki tanácsadói minőségben*** legyen ***az IT ágazat fejlesztésének felelőse***. Az 1966-os születésű

médiavállalkozó a leningrádi hadmérnöki főiskolán szerzett mérnök-programozó diplomát, ezt kiegészítette közgazdász képesítéssel. Tulajdonosa a Live-Internet és MediaMetrics internetes adatforgalom számlálóknak, valamint őt tartják a ***runet alapító atyjának***. (A runet az orosz nyelvű internetes portálok összessége, valamennyi kontinensen, beleértve az Antarktiszt is. Az angol (57,4%) után a legelterjedtebb nyelv egyébként az internet világában az orosz (5,9%). Az elnöki főtanácsadót kritikusai „putyinoid"-nak mondják, feltétlen lojalitása miatt.

Felfogása szerint Oroszország akkor jár el helyesen, ha az internet működését ***a kínai modell*** szerint szabályozza. Ennek lényege, hogy az állami (államhatalmi) intézmények és szervezetek teljesen függetlenedjenek a külföldi szolgáltatóktól. A Google oroszországi működését ahhoz a feltételhez kössék (szintén kínai mintára), hogy ha szükséges, az orosz állami megkeresésekre adják ki a kért forgalmi adatokat és tartalmakat. Ugyanakkor a kínai „Nagy Tűzfal" felépítését nem tartja követendő példának, a rendkívül magas költségek miatt (300-500 millió USD). Az elnöki főtanácsadó meggyőződése szerint végső soron Európa valamennyi állama követni fogja a kínai modellt: önálló, minden tekintetben hazai bázisra épülő állami internetet fognak létrehozni. (FORRÁS http://www.gazeta.ru/tech/2014/09/22 a6231973.shtml)

(Az elképzeléseket, a teljes körű nemzeti IT szuverenitásra való törekvést ugyanakkor célszerűnek látszik óvatosan kezelni. A jelenlegi oroszországi helyzet úgy fest, hogy a szektor egészében gyakorlatilag 100%-osan csak a világszerte bevált nagy operációs rendszereket használják (Windows, Linux, IOS). Az más kérdés, hogy szoftverek fejlesztésében az orosz szakemberek világszínvonalon teljesítenek, ebben nagyon erősek. A teljes számítógépeket is gyakorlatilag csak importból szerzik be. Igaz, az aktuális embargó rászorítja az oroszországi fejlesztőket az önállósulásra, ugyanakkor a lényegi alkatrészeket a kínai piacról kénytelenek beszerezni. Az import-kiváltás egyelőre siralmas állapotáról egy-egy – szűk nyilvánosságnak szánt – szakmai konferencián lehet tájékozódni.) (http://ittek.ru/download/Pshychenko.pdf)

Zárszó

A technikai fejlődéssel birtokba vett új terek sokáig az országok határait, szuverenitását tágították (pl. légtér). A nemzetállamok akarata alakította ki előbb a világtengerek nem part menti részeit, úgynevezett mindenki által szabadon használható (res communis omnium usus) területekké, de a világűr meghódításánál is ugyanez a folyamat játszódott le. Mivel mindkét tér a világóceánok, illetőleg a világűr is elsősorban a katonai szembenállás területei voltak, az összeütközések valószínűségének csökkentése érdekében hamar megszülettek azok a nemzetközi egyezmények, amelyek e közös területek használatát szabályozták. A szabályozásnál viszonylag könnyű dolga volt a nemzetközi jogászoknak, hiszen kevés nagyhatalom volt képes a világtengerek uralására, vagy annak idején csak a bipoláris szembenállás két vezető hatalma, az USA és a Szovjetunió tudott a világűrbe űrhajót felbocsátani. Időközben a technológiai helyzet megváltozott, egyre több ország képes már a világűrt elérni, illetőleg nem csak a nagyhatalmak lennének képesek a világóceánok egyre nagyobb szeletét valóságosan is birtokba venni, mint ahogyan a tengerfenék kiaknázásával kapcsolatos technikai verseny is egyre erőteljesebbé válik.

Más a helyzet a kibertérrel. A gépi memóriákban lévő adat- és információtömeg jelenleg meghatározott vállalkozások, államok, egyéb szervezetek vagy akár magánszemélyek rendelkezése alatt áll. Azok a kísérletek, amelyek egy egységes, res communis omnium usus, azaz mindenki által szabadon használható kiberteret tűztek ki célul, rendre elbuktak, vagy háttérbe szorították őket a profitszerzési szándékok. A közös kibertér fejlődése mégis elkerülhetetlen, bár magának az internet szabad használatának is vannak buktatói. Ahhoz, hogy megelőzzük az internet széthullását, vagy a sötét oldalának kiteljesedését, minél hamarabb meg kellene állapodni legalább a szabályozás alapelveiben.

Mindezen tevékenységek átgondolására leginkább az ENSZ lenne alkalmas lehetőség, de erre jelenleg sem kapacitása, sem politikai szándéka nincs az ENSZ-be tömörülő tagállamok összességének.

Felhasznált irodalom

Hivatkozás könyvre

ANCEL, Jacques (1936) Géopolitique. Librairie Delagrave, Paris. p. 109.

ARON, Raymond (1996) Paix et guerre entre les nations. Calmann-Lévy, Paris. 770. részlet

BARABÁSI, Albert-László (2003) Behálózva. Budapest, Libri. ISBN 978-963-310-971-7

DEFARGES, Philippe Moreau (1994) Bevezetés a geopolitikába, Introduction à la géopolitique, éd. du Seuil, Paris. p. 230.

DENARDIS, Laura (2014) The Global War for Internet Governance. New Haven and London, Yale University Press. ISBN 978 0 300 18 135 7

Dictionnaire de géopolitique, Flammarion, Paris, 1993. p. 1680

FOUCHER, Michel (1997) A geopolitika vége? La fin de la géopolitique? Réflexions géographiques sur la grammaire des puissances. Politique étrangère, Paris, 1997/1.

HALÁSZ, László (1985) Vége a Gutenberg-galaxisnak? Budapest, Gondolat. ISBN 963 281 509 2

HUNTINGTON, Samuel P. (2001) A civilizációk összecsapása és a világrend átalakulása. Budapest, Európa Könyvkiadó. 48-49 p. ISBN 963 07 7084 9

MATOLCSY, György (2015) Amerikai Birodalom – a jövő forgatókönyvei. Budapest, Pallas Athéné Geopolitikai Alapítvány. 285 p. ISBN 978 963 12 3814 3.

McLUHAN, Herbert Marshall (2001) A Gutenberg-galaxis. Budapest, Trezor Kiadó. ISBN 963 9088 55 2

PIKETTY, Thomas (2015) A tőke a 21. században. Budapest, Kossuth Kiadó. ISBN 978 963 09 8191 0

RATZEL, Friedrich (1923) Politische Geographie. Wien

ROSENGREN, Karl Erik (2004) Kommunikáció. Budapest, Tipotex Kiadó, ISBN 978-963-9548-93-0

SMITH, Anthony (1980) The Geopolitics of Information. New York, Oxford University Press. ISBN 0 19 520208 2

TOFFLER, Alvin (2001) A harmadik hullám. Bp., Typotex. ISBN 963 9326 21 6

TOFFLER, Alvin (1980) The Third Wave. United States and Canada, Bantam Books. ISBN 0 553 22 635 5

Hivatkozás könyvrészletre:

MÉSZÁROS, Rezső (2010) A globális kibertér. In: MÉSZÁROS R, NAGY G, NAGY E, BOROS L, PÁL V. A globális gazdaság földrajzi dimenziói. Budapest, Akadémiai Kiadó. pp. 349–361. ISBN 978 963 05 89 36 9. ISSN 2060-5536

MOLNÁR, Gusztáv (1999) Összefoglaló. In: CSIZMADIA Sándor, MOLNÁR Gusztáv, PATAKI Gábor Zsolt. Geopolitikai szöveggyűjtemény. Budapest, Stratégiai Védelmi Kutatóintézet pp. 13. ISBN 963 8117 68 0

Hivatkozás folyóiratcikkre:

BUSH, Vannevar (1945) Út az új gondolkodás felé. In: SUGÁR János (szerk.): Hypertext + Multimedia. Budapest, Artpool Füzetek, 1996/3. sz. http://www.artpool.hu/hypermedia/ (2010.02.12.)

DOUZET, Frederick (2014) La géopolitique pour comprendre le cyberespace. Hérodote, 152-153. 2014 1-2. pp. 3-21. ISBN 978 2 7071 7898 5

FOUCHER, Michel (1997) A geopolitika vége? La fin de la géopolitique? Réflexions géographiques sur la grammaire des puissances. Politique étrangère, Paris, 1997/1.

MÉSZÁROS, Rezső (2001) A kibertér társadalomföldrajzi megközelítése. Magyar Tudomány, 2001. július

PINTÉR, István (2009) A virtuális tér szerepe a vállalatirányításban. Geopolitikai Tanács Alapítvány Műhelytanulmányok, 2009/2. ISSN 1788-7895. ISBN 978-963-9816-28-2.

SZVETELSZKY, Zsuzsanna (2008) Pletyka, internet, hálózattudat. Szín – A Magyar Művelődési Intézet és Képzőművészeti Lektorátus folyóirata, 2008. évf. április. 13/2. pp. 20-23. ISSN-1416-6925

SZVETELSZKY, Zsuzsanna (2013) Térsebészet. In: VESZELSZKI Ágnes. A világhálóba keveredett ember. Budapest, ELTE Eötvös Kiadó. pp 78-82. ISBN

SZVETELSZKY, Zsuzsanna (2013) Tehetség és hálózat. In: SZÁVAI Ilona. Én ne lennék tehetséges? Budapest, Pont Kiadó. pp. 95-100. ISBN: 978-963-9957-61-9

ULFKOTTE, Udo (2014) Megvásárolt újságírók. Budapest, Patmos Records. ISBN 978 615 5526 04 6

WIESER, Dieter (1994) „Geopolitika" – egy vitatott fogalom reneszánsza. Aussenpolitik, 1994/4. szám

Hivatkozás elektronikus tartalomra/weboldalra:

LLOYD, Seth (2002) Computational Capacity of the Universe. *Cambridge, Massachusetts,* 2002. The American Physical Society. ISSN 0031-9007_02_88(23)_237901. p.237901-1 (https://scholar.google.com/scholar_lookup?author=S.+Lloyd&title=Computational+capacity+of+the+universe&publication_year=2002&journal=Phys.+Rev.+Lett.&volume=88)

TÓTH, Máté (2004) A könyvtáros szakma szerepváltása a digitális korban – trendek a hazai és nemzetközi könyvtárügyben. Tudományos és Műszaki Tájékoztatás, 51. évf., 2004/1. sz., 16-29 o. http://tmt.omikk.bme.hu/show_news.html?id=3486&issue_id=447 (2010.02.11.)

http://world-statistics.org/index-res.php?code=IP.PAT.RESD?name=Patent%20applications,%20residents#top-result

http://news.mediaspecs.be/sites/default/files/Global%20Digital%20Landscape%202015%20-%20Insight%20Slides.pdf

Köszönetnyilvánítás

Nevük felsorolásával köszönöm meg mindazoknak, akik hozzájárultak még a kutatás sikeréhez, a tanulmánykötet elkészítéséhez:

Arany Imre
Horváth Péter
Kiss Erika Gabriella
Kramarics Istvánné
Mészáros Lajosné
Szabó Barbara
Sz. Bátkay Katalin
Sztanó Zsuzsanna

illetve külön köszönet illeti a Pallas Athéné Geopolitikai Alapítvány döntéshozóit, akik támogatásukkal lehetővé tették a virtuális térrel kapcsolatos kutatást, valamint köszönet illeti Frédérick Douzet asszonyt, hogy hozzájárult cikkének a jelen tanulmánykötet előszavaként való megjelenéséhez.

Kiadja: Geopolitikai Tanács Közhasznú Alapítvány
www.cgeopol.hu
Felelős kiadó: Dr. Pintér István
Borítóterv, tipográfia és tördelés: Layout Factory Grafikai Stúdió, Budapest
Nyomdai munkák: Perc Print Digitális Nyomdai Műhely, Budapest
Készült 50 példányban

ISBN 978-963-9816-34-3
ISSN 1788-7895