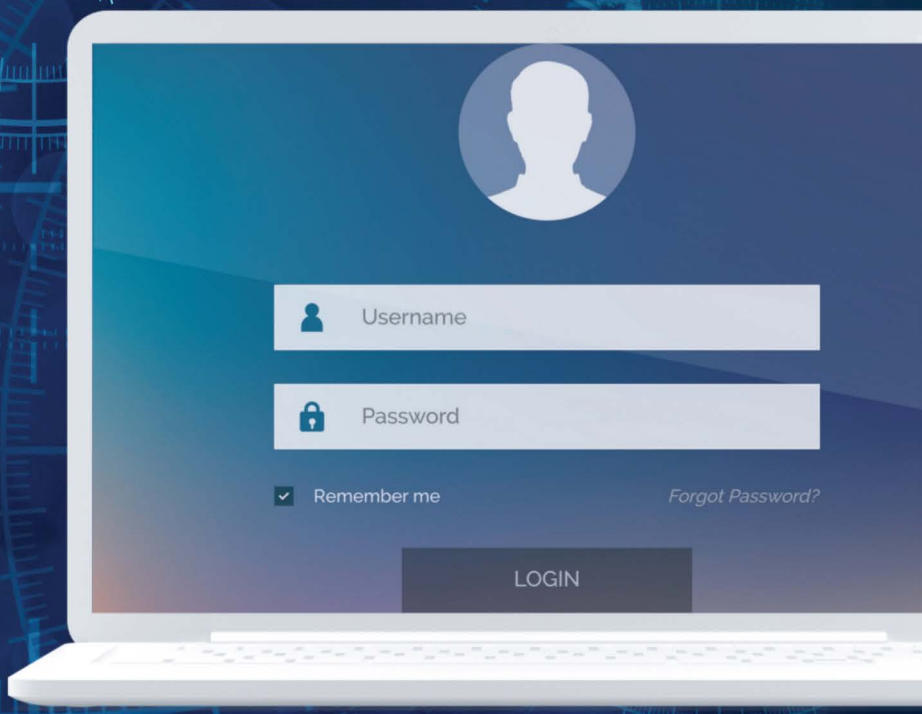
DIGITÁLIS BIZTONSÁGPOLITIKA A KIBERTÉRBEN

Szerkesztette: Babos Tibor



MATE

DIGITÁLIS BIZTONSÁGPOLITIKA A KIBERTÉRBEN

A kötet összeállításában közreműködött és a kiadást támogatta
a Hunexpert Magyar Szakértői Rendszer Kft.

DIGITÁLIS BIZTONSÁGPOLITIKA A KIBERTÉRBEN

Tanulmánykötet

Szerkesztette:
Babos Tibor

Magyar Agrár- és Élettudományi Egyetem
Gödöllő, 2021

Szerzők:
Babos Tibor, Beregi Alexandra Lilla, Csutak Zsolt, Drabancz Áron,
El-Meouch Nedim Márton, Hegyi Henrietta, Paráda István

Szerkesztő:
Babos Tibor

Lektorok:
Babos Tibor, Jobbágy László, Varga Dóra

Kiadja a Magyar Agrár- és Élettudományi Egyetem
Cím: 2100 Gödöllő, Páter Károly utca 1. Telefon: +36-28/522-000
Honlap: https://www.uni-mate.hu
Felelős kiadó: Prof. Dr. Gyuricza Csaba PhD, rektor

Kézirat-előkészítés és korrektúra:
Hunexpert Magyar Szakértői Rendszer Kft.

Tördelés/lapterv:
Szalai Norbert

Készült a Szent István Egyetem Kiadó és Üzemeltető Kft. nyomdájában
Cím: 2100 Gödöllő, Páter Károly utca 1.
Felelős vezető: Borbély László

A kiadvány a *Digital Security Policy in the Cyber Space* című
angol nyelvű tanulmánykötet magyar nyelvű változata

ISBN 978-963-269-974-5 (nyomtatott)
ISBN 978-963-269-975-2 (PDF)

TARTALOMJEGYZÉK

ELŐSZÓ

„Digitális", „biztonság", „politika" – napjaink politikai, társadalmi, gazdasági, technológiai vagy nemzetközi kapcsolataiban használt gyakori szavak. Jelentésük ugyan magától értetődőnek tűnik, azonban a három szó viszonyrendszerére vagy azok korrelációjára vonatkozó rendszerelmélet, összehasonlító elemzés, kutatási projekt mindezidáig nem látott napvilágot a világon sehol. Kutatók és egyszerű érdeklődők nap mint nap tapasztalhatják, hogy a világ vezető tisztségviselői, szakértői, kutatói másként értelmezik a digitális biztonságpolitikát, eltérően rangsorolják annak elemeit. Az értékeléseket, érveléseket, álláspontokat gyakran radikálisan befolyásolják a politikai, gazdasági, kulturális, történelmi, földrajzi, vallási hovatartozásból vagy körülményekből fakadó tényezők. A digitális biztonságpolitika alapdilemmája is tulajdonképpen ebben rejlik: közös nevezők, definíciók hiányában nemcsak a problémamegközelítés, hanem annak megoldását elősegíteni hivatott kutatások, tárgyalások, konferenciák eredményei is különbözőek, kimenetelük többesélyes. Mindezt a digitalizáció hihetetlen gyors fejlődési sebessége tovább bonyolítja. Jóllehet a digitalizáció számos problémára megoldást jelentett az elmúlt években, ma már látjuk, jótékony hatása mellett számtalan kérdést, dilemmát, sőt veszélyt is rejt magában.

A *Digitális biztonságpolitika* kutatási projekt, konferencia és az annak nyomán született *Digitális biztonságpolitika a kibertérben* című könyv e különbözőségek csökkentéséhez, az eltérő álláspontok közelítéséhez, s a fogalmak közös nevezőre hozásához járul hozzá. A világon egyedülálló módon, hiszen ilyen címmel hasonló kutatási projektet még sehol sem jegyeztek fel. Jelen könyv ezt az egyedülálló tudományos és szakmai teljesítményt dokumentálja. E sorok jegyében ajánlom a *Digitális biztonságpolitika* kutatási projektet, konferenciát és az annak nyomán, Egyetemünk gondozásában most kiadott könyvet minden olyan érdeklődő, kutató számára, akik a téma aktuális fejleményei tekintetében naprakész ismeretekre kívánnak szert tenni. Bízom abban, hogy a *Digitális biztonságpolitika a kibertérben* című kötet kiadását még sok további tanulmánykötet is követi, hiszen a téma dinamikus fejlődése ezt egyébként is indokolja.

Prof. Dr. Gyuricza Csaba rektor
Magyar Agrár- és Élettudományi Egyetem

KÖSZÖNETNYILVÁNÍTÁS

A főszerkesztő, a szerkesztő, a kiadó, valamint a szerzők ezúton is köszönetüket fejezik ki az alább felsorolt szervezeteknek azért, hogy szakmai tudásukkal, hozzáértésükkel, emberi erőforrásukkal hozzájárultak a *Digitális biztonságpolitika* kutatási projekt, konferencia megvalósulásához, valamint az annak nyomán szerkesztett, jelen könyv megjelenéséhez. E kutatási projekt a Digitális Jólét Nonprofit Kft., kiemelten Jobbágy László ügyvezető; a Doktoranduszok Országos Szövetsége; a Hunexpert Magyar Szakértői Rendszer Kft.; a Magyar Agrár- és Élettudományi Egyetem és a Szent István Biztonságkutató Központ; a Magyar Atlanti Tanács; valamint az Országos Tudományos Diákköri Tanács odaadó támogatása nélkül nem valósulhatott volna meg.

Babos Tibor

A *Digitális biztonságpolitika* kutatási projekt háttere és követelményrendszere

„Messze jövendővel komolyan vess öszve jelenkort"[1]
Kölcsey

Helyzet

Napjaink nemzetközi kapcsolatai tempójára, időbeli korlátjaira és egyben kilátásaira jelentős hatással van a globalizáció és a belőle kinőtt átfogó digitális, technológiai forradalom. A digitális, technológiai forradalom széleskörű, szerteágazó, sokrétű, ugyanakkor nagy sebességű változásokat indukált a társadalom egészében, gyökeresen alakította át a politikai, közigazgatási, gazdasági, ipari, mezőgazdasági, oktatási, tudományos, egészségügyi, közlekedési, energetikai, diplomáciai, nemzetbiztonsági és katonai rendszereket.

A mai értelemben vett digitalizáció, számítástechnika és internet a második világháborús katonai rendszerekben kezdte meg fejlődését, majd a hidegháború katonai tömbjeiben kapott új lendületet, s az ötvenes évekre már a teljesen elszabadult fegyverkezési verseny nukleáris és hagyományos *high tech* fegyverrendszerek műszaki vezérlőberendezéseiben teljesedett ki. Az informatika ma éppúgy jelen van a fejlett világ katonai szervezeteiben, mint a feltörekvő országok haderőiben. Az Egyesült Államok, Franciaország, Nagy-Britannia vagy Németország katonai rendszereinek vezetése, irányítása, híradása, logisztikája, utánpótlás-szervezése vagy hadiipari fejlesztései éppúgy digitális platformokon történnek, mint Kínában, Indiában, Brazíliában vagy Oroszországban.

A katonai, hadiipari szektorból kiszabadulva a digitalizáció és az informatikai forradalom mára feltartóztathatatlanná vált, áthatja a világ társadalmi rendszerének egészét. Gyökeresen alakítja át a politikai, közigazgatási, gazdasági, ipari, mezőgazdasági, oktatási, tudományos, egészségügyi, közlekedési, logisztikai, energetikai, diplomáciai, nemzetbiztonsági és katonai rendszereket. Nagy biztonsággal állapítható meg, hogy a biztonság is digitalizálódott, s e folyamat a történelem globális korszakváltásaként értelmezhető, ami hosszú távon determinálja az emberiség fejlődésének alternatíváit. Ebből következően alapvető kérdésként vetődik fel: a nemzeti (nemzeti biztonsági, katonai és nemzetbiztonsági) stratégiák milyen módon kezelik az informatikai forradalmat és az azzal együtt felgyorsuló információs, technológiai haladást, elzárkóznak-e tőle, adaptálódnak-e hozzá, vagy élére állnak és a maguk malmára hajtják az abban rejlő lehetőségeket.

1 Kölcsey Ferenc: Huszt. 1831. dec. 29, Kölcsey Ferenc összes művei, Országos Széchenyi Könyvtár, Budapest, 2019

Probléma

E folyamat teljesen új fejlődési dimenziót nyitott az emberiség előtt: az információ és a kommunikáció globalizációja, a tudás széles tömegek előtti gyors elérhetősége; a sebesség növekedése és a távolságok relatív csökkenése; a kultúrák, szokások, nyelvek univerzálódása; a piacok világszintű összekapcsolódása következtében alapjaiban változik meg az emberek napi rutinja, és sorra dőlnek meg a korábbi tudományos tételek. A műszaki, technológiai robbanás ma feltartóztathatatlannak és behatárolhatatlannak látszik. A klaszszikus rend dinamikus átrendeződése következtében egyfelől hallatlanul fokozódik a politikai, gazdasági, piaci és technológiai szabadverseny, másfelől a nemzeti, állami, kulturális és vallási központok közötti rivalizálás, ami egyúttal katonai erőgenerálást is maga után von. A gazdasági dimenzióváltás, a termelés, a fogyasztás és a szolgáltatások új struktúrái, a nemzetközi pénzügyek integrálódása, a nyersanyagok utáni fokozott kereslet és a létszükségletek iránti hajsza egyre erőteljesebben és radikálisabban alakítja a nemzetközi rendet, ahol a fegyveres erők szerepe növekvő tendenciát mutat. A világ „összezsugorodása" következtében a fejlettségbéli különbségek, az érdekellentétek élesebben rajzolódnak ki.[2] E világban a fejlett technológián alapuló katonai képességek fontossága ugyan fokozatosan, de mind határozottabban tért hódít.

Nagy biztonsággal állapítható meg: e folyamat a történelem globális korszakváltásaként értelmezhető, és még hosszú távon determinálja az emberiség fejlődésének alternatíváit. A digitális, technológiai forradalom számos jótékony eredménye mellett mostoha fejleményekkel is számolni kell. A széleskörű, vagy célzott kibertámadások közérdeket szolgáló hálózatok, azok kritikus elemei ellen; a közösségi rendszerek feltörése, személyes adatok lopása és az azokkal való visszaélések, manipulációk és lejáratások; a kommunikációs rendszerek ellehetetlenítése, befolyásolása ma is direkt fenyegetést jelentenek államok, szervezetek és egyének számára egyaránt. A mesterséges intelligenciában, az űrkutatásban, a génkutatásokban, vagy a nanotechnológiában rejlő lehetőségek és veszélyek beláthatatlanok.[3] A műszaki, informatikai, vagy digitális találmányok új dimenziót nyitottak a katonai, haditechnikai és hadiipari szektorban is. A technológiai és informatikai alapú rendszereink térnyerése, azok megváltozott tartalma, ugyanakkor sérülékenysége, új biztonsági követelményeknek való megfeleltetést és más viselkedési normákat tesznek szükségessé. Az ebből adódó folyamatos és nagy iramú megfelelési kényszert sokan nem képesek követni, az alkalmazkodni, vagy versenyképtelen rendszerek gyakrabban és gyorsabban omlanak össze, maradnak le, rekesztődnek ki, s válnak a folyamat ellenzőivé.

2 Tibor Babos: "The Five Central Pillars of European Security", NATO Public Diplomacy Division Brussels, Strategic and Defense Research Institute Budapest, NATO School Oberammergau and Chartapress Budapest, 6 October 2007

3 Babos Tibor: „A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái", Hadtudomány, 2018. évi elektronikus lapszám, Budapest, 2018

Célrendszer

Mindebből következően alapvető kérdésként vetődik fel: a nemzeti (nemzeti biztonsági, katonai és nemzetbiztonsági) stratégiák milyen módon kezelik a digitális, technológiai forradalmat és az azzal együtt felgyorsuló információs haladást, elzárkóznak-e tőle, adaptálódnak-e hozzá, vagy élére állnak és a maguk malmára hajtják az abban rejlő lehetőségeket. Tekintettel arra, hogy a digitális átalakulás lehengerlő, áthatja a fejlett világ társadalmi rendszerének egészét, hazánknak nemcsak kapcsolódnia kell, hanem célszerű vezető szerepre törnie e folyamatban annál is inkább, mert Magyarország nemzetközi összehasonlításban is magasan pozícionált a tudományos, technológiai, informatikai és matematikai felkészültség, szürkeállomány terén; a magyarok vívmányai, tudományos elismerései vitathatatlanok világszerte évszázadok óta.

„Messze jövendővel komolyan vess öszve jelenkort" írja Kölcsey 1831-ben a reformkor idején, amikor az ország fejlődése új lendületet kapott. A 19. század elejére a fejlődésben Nyugat-Európa mintaadó államaihoz, Angliához, Franciaországhoz és a Habsburg Birodalomhoz képest lemaradt magyar társadalomban nemzeti és újítási folyamatok indultak meg. A korszak idején számtalan politikai, gazdasági, szociális és kulturális vívmány született, köztük különösen említésre méltó a magyar nyelv oktatása, a nemzeti összetartozást kifejező művészeti alkotások, a polgári átalakulás útjában álló akadályok elhárítása, valamint nem utolsó sorban az önálló modern ipar és technológia megteremtése. E vívmányok aztán az öntudatra ébredő magyar nemzet újkori történelmének alappilléreivé váltak, s elvezettek a modern, polgári Magyarország létrejöttéhez. Korunkat jellemző informatikai forradalom révén hazánknak a reformkorhoz fogható körülmények között kell megvalósítania nemzeti törekvéseit és megvédenie évezredes értékeit. Fontos ezért, hogy az aktuális biztonsági folyamatokat, kihívásokat és a nemzetközi folyamatok trendjeit helyesen vegyük számba, és megfelelő következtetések levonásával sikeres politikát folytassunk regionális és nemzetközi viszonylatban egyaránt.[4]

Tézis

A Magyar Kormány Digitális Jólét Program, a Magyar Atlanti Tanács, a Doktoranduszok Országos Szövetsége, az Országos Tudományos Diákkori Tanács és a Magyar Agrár- és Élettudományi Egyetem Biztonságkutató Központja által, *Digitális biztonságpolitika* címmel meghirdetett nyílt kutatási projekt és konferencia célja, hogy fiatal magyar tudósoknak lehetőséget biztosítson „biztonság" és „digitalizáció" kulcsszavak tárgyában folytatott kutatások folytatására. A *Digitális biztonságpolitika* kutatási projekt és konferencia égisze alatt (1) tanulmányírásra; (2) konferencián való részvételre és prezentációra; valamint (3) szerkesztett és lektorált könyvben történő publikációra pályázhatnak magyar fiatal tudósok. Az arra érdemes jeles dolgozatok szerzői díjazásra és a magyar biztonsági tanulmányok vérkeringésébe való bekapcsolódásra számíthattak.

4 Babos Tibor: „A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái", Hadtudomány, 2018. évi elektronikus lapszám, Budapest, 2018

A pályamunkákban az aktuális biztonsági fenyegetések, kihívások és a digitalizáció kapcsolatrendszerét, folyamatait, trendjeit helyesen körüljáró, a nemzeti (nemzeti biztonsági, katonai és nemzetbiztonsági) stratégiák kialakításában, regionális és nemzetközi viszonylatban hasznosítható eredmények ismertetését várták a pályázat kiírói. A pályázatok beérkezési határideje 2020. április 30. napja volt.

Következtetés

A *Digitális biztonságpolitika* címmel 2020-ban megkezdett kutatási projekt előrehaladását, valamint a szerkesztett és lektorált könyv megjelentetését a COVID-19 globális járvány nagyban befolyásolta, kitolta. Ezzel együtt számos tanulságot, egyben eredményt is biztosított a pályázat kiírói számára. Ezek közül talán a legfontosabb, hogy az emberiség biztonsága váratlanul, akár gyökeresen is megváltozhat, amellyel szemben az emberiség a világtörténelemben először lépett fel – többé-kevésbé – egységesen és közösen, és ez a fellépés alapvetően az emberek fizikai kontaktusának korlátozását jelentette, amelyben a *digitális biztonságpolitika* kulcsfontosságúvá vált. Ez a könyv, e körülmények közepette született elsőként, hazai és világviszonylatban egyaránt. Az alapítók szándéka, hogy e téma és e tudományos kutatási kezdeményezés ne álljon meg az első konferenciánál és az első kötetnél.

Babos Tibor

A digitális biztonságpolitika védelem- és katonapolitikai összefüggései

„A fény ára kevesebb, mint a sötétség költsége."[1]
Arthur C. Nielsen

Rezümé

A digitális átalakulás feltartóztathatatlan, áthatja a fejlett világ társadalmi rendszerének egészét. Hazánknak nemcsak kapcsolódnia kell ahhoz, hanem célszerű vezető szerepre törnie e folyamatban. A tanulmány röviden összefoglalja a Digitális Jólét Program (DJP) katonai vetületeit, kapcsolódásait; vázolja a Zrínyi 2026 Honvédelmi és Haderő-fejlesztési Program irányait; javaslatokat tesz DJP-hez kapcsolható katonai rendszerekkel szemben támasztott követelmények meghatározására; valamint általános következtetéseket fogalmaz meg a biztonság-, védelem- és katonapolitika DJP-ben történő megjelenítése tárgyában.

Resume

The digital transformation is irresistible, penetrates the political, economic and social system of the developed world as a whole. Due to its high standard scientific capacities, Hungary should take a leading position in this global process. The study discusses the relevant security, defense and military aspects of the Digital Welfare Program (DWP), makes recommendations for defining requirements for military systems linked to the DWP, as well as offers general conclusions on the issue of security, defense and military policy in the DWP.

Vezetői összefoglaló

Az informatikai forradalom gyökeresen alakítja át a politikai, közigazgatási, gazdasági, ipari, mezőgazdasági, oktatási, tudományos, egészségügyi, közlekedési, logisztikai, energetikai, diplomáciai, nemzetbiztonsági és katonai rendszereket. Nagy biztonsággal állapítható meg: e folyamat a történelem globális korszakváltásaként értelmezhető és hosszú távon determinálja az emberiség fejlődésének alternatíváit. Ebből következően alapvető kérdésként vetődik fel: a nemzeti (nemzeti biztonsági, katonai és nemzetbiztonsági) stratégiák milyen módon kezelik az informatikai forradalmat és az azzal együtt felgyorsuló információs, technológiai haladást,

1 Arthur C. Nielsen, Colorado State University, Denver,
online: http://social.colostate.edu/2015/06/19/the-price-of-light-is-less-than-the-cost-of-darkness/ (2019. július 5.)

elzárkóznak-e tőle, adaptálódnak-e hozzá, vagy élére állnak és a maguk malmára hajtják az abban rejlő lehetőségeket. Tekintettel arra, hogy a digitális átalakulás feltartóztathatatlan, áthatja a fejlett világ társadalmi rendszerének egészét, hazánknak nemcsak kapcsolódnia kell, hanem célszerű vezető szerepre törnie e folyamatban annál is inkább, mert Magyarország nemzetközi összehasonlításban is magasan pozícionált a tudományos, technológiai, informatikai és matematikai felkészültség, szürkeállomány terén, a magyarok vívmányai, tudományos elismerései vitathatatlanok világszerte. Ennek tükrében e tanulmány a biztonsági fenyegetések és informatika hatásmechanizmusának bemutatása után röviden összefoglalja a DJP és a DJP 2.0 katonai vetületeit, kapcsolódásait; vázolja a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program nyílt forrásból megismerhető elemeit, irányait; javaslatokat tesz a DJP-hez és a DJP 2.0-hoz kapcsolható katonai rendszerekkel szemben támasztott követelmények meghatározására; valamint általános következtetéseket fogalmaz meg a biztonság-, védelem- és katonapolitika DJP-ben történő megjelenítése tárgyában.

Bevezetés

Az informatikai forradalom átfogó és nagyiramú változásokat indukált a társadalom egészében, gyökeresen alakította át a politikai, közigazgatási, gazdasági, ipari, mezőgazdasági, oktatási, tudományos, egészségügyi, közlekedési, logisztikai, energetikai, diplomáciai, nemzetbiztonsági és katonai rendszereket. Nagy biztonsággal állapítható meg: e folyamat a történelem globális korszakváltásaként értelmezhető és hosszú távon determinálja az emberiség fejlődésének alternatíváit. Ebből következően alapvető kérdésként vetődik fel: a nemzeti (nemzeti biztonsági, katonai és nemzetbiztonsági) stratégiák milyen módon kezelik az informatikai forradalmat és az azzal együtt felgyorsuló információs, technológiai haladást, elzárkóznak-e tőle, adaptálódnak-e hozzá, vagy élére állnak és a maguk malmára hajtják az abban rejlő lehetőségeket.[2] Tekintettel arra, hogy a digitális átalakulás feltartóztathatatlan, áthatja a fejlett világ társadalmi rendszerének egészét, hazánknak nem csak kapcsolódnia, hanem célszerű vezető szerepre törnie e folyamatban annál is inkább, mert Magyarország nemzetközi összehasonlításban is magasan pozícionált a tudományos, technológiai, informatikai és matematikai felkészültség, szürkeállomány terén, a magyarok vívmányai, tudományos elismerései vitathatatlanok világszerte.

A Digitális Jólét Program (DJP) egyik legfontosabb feladata éppen annak támogatása, hogy Magyarország állami rendszerei, közigazgatása, vállalkozásai és minden polgára, a digitalizáció és az informatikai forradalom nyertese lehessen. A Program – ezt felismerve – kívánja felkészíteni Magyarország polgárait, gazdasági szereplőit, állami rendszereit e globális átalakulásra. Középtávú célként jelölhető ki, hogy Magyarország, a digitalizáció nyújtotta lehetőségekbe terelve tudományos, technológiai, ipari, oktatási és egyéb rendszereit, egy évtizeden belül a világ élvonalába kerüljön.[3]

2 Tibor Babos, The Five Central Pillars of European Security, NATO Public Diplomacy Division, Brussels, Strategic and Defense Research Center, Budapest, NATO School, Oberammergau, 2008, pp. 69-92.

3 2012/2015. (XII. 29.) Korm. határozat az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (In-ternetKon) eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról, Netjogtár, online: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A15H2012.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (2018. január 10.)

A Kormány szándékai szerint az egymásra épülő, egymást kiegészítő kormányzati infokommunikációs programokat a magyar társadalom és a magyar nemzetgazdaság digitális fejlesztését célzó, a Kormány 2012/2015. (XII. 29.) határozatával elfogadott DJP keretében kell összehangolni. A DJP célkitűzéseinek megvalósítása a Nemzeti Infokommunikációs Stratégiával (NIS) összhangban, a Digitális Nemzet Fejlesztési Programban (DNFP) elért, illetve megvalósítás alatt álló eredményekre építve tervezett. A 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról (DJP 2.0), azaz a Digitális Jólét Program kibővítéséről, annak 2017–2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről.[4]

Tekintettel arra, hogy a politikai, közigazgatási, gazdasági, ipari, mezőgazdasági, oktatási, tudományos, egészségügyi, közlekedési, energetikai és más polgári rendszerek mellett a digitalizáció és informatika nagyban hat a védelmi, katonai és nemzetbiztonsági felépítményekre is, e tanulmány tézise, hogy a biztonsági, honvédelmi, katonai és nemzetbiztonsági megfontolások részét kell képezniük a Digitális Jólét Programnak és annak 2.0 verziójának. Pontosabban fogalmazva: a DJP-ben és a DJP 2.0-ban ki kell alakítani a honvédelmi, katonai és nemzetbiztonsági ágazatot azért, mert (1) a biztonsági folyamatok közvetlenül befolyásolják a digitális jólétet; (2) a honvédelmi, a katonai és a nemzetbiztonsági rendszereknek támogatniuk kell azt; (3) a katonai rendszerek maguk is alkalmaznak és fejlesztenek informatikai, digitális- és hálózatalapú képességeket; s mert (4) a honvédelmi, nemzetbiztonsági szektor egészének kapcsolatban kell állnia az ország legnagyobb szabású digitális fejlesztési projektjével, elkerülendő az attól való leszakadást vagy izolációt. A DJP megvalósításának egyébiránt is a biztonsági körülmények, fenyegetések szakszerű, folyamatos vizsgálatán, valamint védelmi, katonai és nemzetbiztonsági oltalmazás alatt kell állnia.

A fentiek tükrében e tanulmány a biztonsági fenyegetések és informatika hatásmechanizmusának bemutatása után röviden összefoglalja a DJP és a DJP 2.0 katonai vetületeit, kapcsolódásait; vázolja a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program nyílt forrásból megismerhető elemeit, irányait; javaslatokat tesz a DJP-hez és a DJP 2.0-hoz kapcsolható katonai rendszerekkel szemben támasztott követelmények meghatározására; valamint általános következtetéseket fogalmaz meg a biztonság-, védelem- és katonapolitika DJP-ben történő megjelenítése tárgyában.

A biztonság átalakulásának digitális vonatkozásai

„Messze jövendővel komolyan vess öszve jelenkort”[5] írja Kölcsey 1831-ben a reformkor idején, amikor az ország fejlődése új lendületet kapott. A 19. század elejére a fejlődésben Nyugat-Európa mintaadó államaihoz, Angliához, Franciaországhoz és a Habsburg Birodalomhoz

4 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelen-téséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munka-terve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről, Net-jogtár, online: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A17H1456.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (2018. január 18.)

5 Kölcsey Ferenc: Huszt, Cseke, 1831. dec. 29, Kölcsey Ferenc összes művei, Országos Széchenyi Könyvtár, Budapest, online: http://mek.oszk.hu/06300/06367/html/01.htm#120 (2015. október 12.)

képest lemaradt magyar társadalomban nemzeti és újítási folyamatok indultak meg. A korszak idején számtalan politikai, gazdasági, szociális és kulturális vívmány született, köztük különösen említésre méltó a magyar nyelv oktatása, a nemzeti összetartozást kifejező művészeti alkotások, a polgári átalakulás útjában álló akadályok elhárítása, valamint nem utolsó sorban az önálló modern ipar és technológia megteremtése.[6] E vívmányok aztán az öntudatra ébredő magyar nemzet újkori történelmének alappilléreivé váltak, s elvezettek a modern, polgári Magyarország létrejöttéhez. Korunkat jellemző informatikai forradalom révén hazánknak a reformkorhoz fogható körülmények között kell megvalósítania nemzeti törekvéseit és megvédenie évezredes értékeit. Fontos ezért, hogy az aktuális biztonsági folyamatokat, kihívásokat és a nemzetközi folyamatok trendjeit helyesen vegyük számba és megfelelő következtetések levonásával sikeres politikát folytassunk regionális és nemzetközi viszonylatban egyaránt.

A nyolcvanas évek végén a kelet–nyugati szembenállás megszűnésével gyökeresen új globális stratégiai helyzet alakult ki. A közép- és kelet-európai államok sorban szakítottak a szocializmus gyakorlatával, a központosított államrenddel, s deklarálták, hogy a nyugat és annak társadalmi rendszere felé fordulnak. E történések széleskörű dezintegrációs, ugyanakkor integrációs tendenciákat idéztek elő. A Kelet-Európában végbemenő események radikálisan megváltoztatták a világ politikai arculatát, s az annak hatására meginduló változások még ma is meghatározók a kontinensen. A jelenlegi újszerű, a korábbinál sokrétűbb és instabilabb helyzetben a biztonságot befolyásoló tényezők, veszélyforrások, kockázatok is más hangsúlyt kaptak, újakkal bővültek.[7] Előtérbe kerültek a biztonság egyéb alkotóelemei: a gazdasági, a pénzügyi, a társadalmi, a kulturális, a vallási, a környezeti, a közbiztonsági, vagy a migrációs problémák mellett dominánsan jelentkeznek a technológiai és informatikai kockázatok.

Földünk biztonságát még mindig az átfogó történelmi korszakváltás következményeiből adódó átmenetiség, illetve a dinamikus restruktúrálódás, a piaci és politikai konkurenciaharc, a regionalizáció, lokalizáció és a nacionalizmus jellemzi, miközben a digitális forradalom és annak kiteljesedése meghatározó történelmi jelenséggé lép elő. Míg a nyolcvanas évek óta a második világháborúban kialakult hidegháborús rend szétporladása egyre inkább dinamikáját veszti, addig az új globális hatalmi centrumok súlyközéppontjai átalakulnak és újradefiniálódnak Ázsiában, Észak-Amerikában és Európában. E folyamatban az amerikai és a nyugat-európai gazdasági potenciál ugyan továbbra is meghatározó, azonban már egyértelműen nem domináns. A hatalmi központok kialakulása és sikere a digitális, informatikai, információs rendszerek minél aktívabb, céltudatosabb és szélesebb felhasználásán múlik.

Ezzel párhuzamosan mind a globális, mind pedig az európai biztonsági kihívások átfogó és nagyléptékű mutációt is produkálnak. Ma egyre makulátlanabbul és erélyesebben juthatnak kifejezésre a nemzetállamokhoz nem minden esetben köthető, viszont transznacionális karakterisztikát öltő fenyegetettségek. Az olyan háborús küszöb alatti rizikófaktorok, mint a nacionalizmus; a szeparatizmus; az extrémizmus; a gazdasági, technológiai, társadalmi és kulturális aránytalanságok; a fejlődési perspektívák divergenciái; az etnikai és vallási kontrasztok; a territoriális integritás és a nemzeti, etnikai önrendelkezés közötti ellentmondások; valamint

6 Gergely András: A polgári átalakulás programja, A reformkor, Rubicon, Történelmi folyóirat, 1996/10. Kormányfők, 1996/4-5., Államtörténet, 1996/1-2. Ezer év, Budapest

7 Tibor Babos, The Five Central Pillars of European Security, NATO Public Diplomacy Division, Brussels, Strategic and Defense Research Center, Budapest, NATO School, Oberammergau, 2008, pp. 69-92.

a tömegpusztító fegyverek proliferációja; a terrorizmus, a nemzetközi szervezett bűnözés; a pénzmosás; a kábítószer-, fegyver-, és emberkereskedelem; a migráció; a környezetszennyezés; az ipari és az ember által okozott egyéb mesterséges katasztrófák vagy a járványok gyűrűzésének a mai országhatárok már egyértelműen nem szabnak gátat. Természetüket tekintve korunk biztonsági kockázati tényezői térben kisebb kiterjedésűek, azonban sokrétűbbek, szerteágazóbbak, s egyben dinamikusabbak is; hatásukat tekintve könnyen akár globális méreteket is ölthetnek; időben pedig szinte behatárolhatatlanok.[8]

A globális stratégiai javakat megcélzó nemzeti gazdasági, politikai és katonai stratégiák esetleges konfrontációja a XXI. században is potenciális biztonsági veszélytényező. Míg a fejlett világban a globális centrumok közötti verseny egyre dinamikusabban fokozódik, addig a bizonytalansággal és átmeneti viszonyokkal küszködő térségekben a biztonsági devianciák folyamatos halmozódása tapasztalható. A túlélésért folytatott harc a gazdasági fejlettség különböző szintjein elhelyezkedő országok között, a jóléttől tulajdonképpen függetlenül zajlik. A fejlett országok éppúgy rivalizálnak egymással, mint a fejletlenek vagy a fejletlenek a fejlettekkel és fordítva. Leegyszerűsítve: éppúgy több kell annak, akinek kevés van, mint aki sokkal rendelkezik. A globális stratégiai javak többsége azonban ma még véges. Az informatika adta platformokat azonban minden állami és nem állami entitás használja, fejleszti, ezért a digitális terek nagyban összeolvadnak, ezáltal képezve globális egységet, egyben sokrétűséget.

A globalizáció, a digitalizáció, az információ és a médiák által befolyásolt társadalmi és kulturális értékek súlyos identitászavarokat okoznak makro- és mikroközösségi szinten egyaránt. A tradicionális nemzeti jellemvonások, öntudatok, szabályok és egyéb értékek új értelmezést kapnak, s e sokrétű folyamatban a nemzeti stratégiai célok is merőben átalakulóban vannak. Ennek egyik legfőbb oka, hogy a nyitottabb határok, a szabad információáramlás és az információ globálissá válása következtében a nemzetközi kapcsolatok „nemzeti", „(nemzet)állami" és „nemzetközi" vizsgálati kategóriái, szintjei merőben átértékelődnek.[9]

A globalizáció hatására univerzálódó biztonsági kihívások nagyban összemossák a „kül- és belbiztonság-politikák" közötti különbséget. E folyamatban az államközpontú intézmények és szabályok feloldódnak és teret engednek a globális kapcsolati rendszerek és szereplők diktálta törvényeknek. A kockázati tényezők egyetemessé válása folytán egyfelől élénkülnek a közös biztonságpolitikai fellépést szorgalmazó viták, másfelől a nemzetállamok magasabb, a nemzetközi biztonsági intézményrendszerek szintjére emelik érdekeik érvényesítését, amely tendencia a nemzetközi intézményrendszer felelősségének növekedésével jár. E folyamatban az állam mint a „nemzetközi kapcsolatok egyik tényezője" szerepe és kompetenciája átformálódik. Ma az államok a posztinternacionális dinamizmus időszakában működnek, amely a határokat sokkal átjárhatóbbá, az intézményeket kevésbé hatékonnyá és a politikai erőt zavarosabbá teszi. Az állami intézmények ugyan továbbra is fontosak maradnak, azok azonban kisebb hatékonysággal, kevesebb forrással és csökkenő legitimációval funkcionálnak. Tekintettel azonban arra, hogy a nemzetközi szervezetek presztízs- és legitimációvesztése rohamosabban megy végbe, mint az államoké, a nemzeti szereplők ereje relatíve gyarapszik.[10]

8 Tibor Babos, The Five Central Pillars of European Security, NATO Public Diplomacy Division, Brussels, Strategic and Defense Research Center, Budapest, NATO School, Oberammergau, 2008, pp. 69-92.
9 Ibid.
10 Ibid.

A globalizáció és modernizáció útjában még mindig számos, elsősorban kulturális, vallási és nacionalista bástya áll. Kérdés, hogy az olyan erősen zárt, tradicionális jelszavak mentén szerveződő közösségek, mint például az iszlám társadalmak, vagy korunk diktatúrái képesek lesznek-e konfliktusmentesen ellenállni e komplex, és többszintű folyamatnak, vagy konfrontálnak vele. Minthogy maga az iszlám sem homogén, valószínű, hogy a konfliktusok az extrémitások, vagyis egyfelől a túlzottan zárt, fundamentalista diktatúrák, valamint a nyitott, liberalizált társadalmak közötti törésvonalak mentén törnek fel. E két ellentétes irányú erő minden bizonnyal mindaddig konfrontálódik egymással, amíg a kontrasztok ki nem egyenlítik, vagy megfelelőképpen le nem rontják egymást.[11] A digitális hálózatok e konfrontáció nyílt színterei. Miközben az internet óriási kulturális hatást gyakorol a zárt társadalmakra, addig a fundamentális rendszerek mind gyakrabban használják e rendszert támadásaik érdekében.

A legnagyobb veszély ma talán a radikalizmus és a technológia kontrasztjában rejlik. Az egyenlőtlen társadalmi, gazdasági alapok és az aránytalan erőforrások következtében fokozódó konfrontációkockázatot a kulturális, civilizációs, vallási, etnikai retorikák és politikai érdekek tovább élezik. E komplex társadalmi polarizáció aztán kölcsönhatásba kerül(het) a hidegháború örökségeként megmaradt katonai potenciállal, amely folyamatban a szinte összemérhetetlen technológiai kontrasztok és a tömegpusztító fegyverekhez való relatíve könnyű hozzáférés meghatározó szerepet játszanak. Ehhez ok-okozati összefüggésként kapcsolódik a további rohamtempójú és széles spektrumú tudományos-technológiai fejlődés, amelynek során a gazdagok még inkább gazdagabbá és fejlettebbé válnak, a szegények pedig relatíve még inkább a perifériára sodródnak. Az, hogy ezek a kontrasztok miképpen és mikor egyenlítik ki egymást, ma még beláthatatlan.

Az aszimmetrikus biztonsági kockázati tényezők, úgymint a tömegpusztító fegyverek alkalmazása, azok célba juttathatósága és/vagy a terrorizmus által okozható csapás napjainkban nagyobb valószínűségű fenyegetettséget jelent a fejlett országokra nézve. A hidegháború utáni évek zavaros biztonsági környezetében a tömegpusztító fegyverek és más pusztító technológiák ellenőrizetlenül hagyása és proliferációja következtében ma a világ stratégiai erőegyensúlya átstrukturálódik. A fejlett világgal opponáló országok, nemzetek és nem állami szereplők a nemzetközi érdekérvényesítés „szabályszerű" eszközei hiányában, vagy azok helyett aszimmetrikus kellékeket ragadnak, amelyek relatíve kis forrásigényűek, ugyanakkor hatásukat tekintve akár egyetemesek is lehetnek. Azok a fejlett hatalmak, ahol kifejlesztették e technológiákat, mára potenciális célponttá váltak. Miután növekszik annak lehetősége, hogy a harmadik világ bizonyos politikai erői az egymás közötti vagy a fejlett világgal szembeni konfliktusai során a hadviselés „piszkos" eszközeihez nyúljanak, a nukleáris, vegyi és biológiai technológiákban, a génmanipulációban, a tömegpusztító fegyverek hordozóeszközeiben, a számítógépek tömeges felhasználásában rejlő szerteágazó veszélyforrások, a technológiák illetéktelenekhez kerülése jelenti napjaink talán a legkönnyebben bekövetkezhető fenyegetését.

A globalizáció egyfajta reakciós tényezője, vagy inkább selejtterméke a terrorizmus. A terrorizmus soha többé nem tekinthető belpolitikai problémának, tudniillik a terrorizmus direkt fenyegetést jelent a nemzetközi biztonságra. Az egyenlőtlenség, a szegénység, a diktatúrák

11 Ibid.

expanziós becsvágya és az ehhez kapcsolódó kulturális gyökerek táptalajul szolgálnak a terrorizmus burjánzásának. A terrorizmus mint az egyetemes fenyegetés, a támadások skálája, a globális veszteségek minőségi és mennyiségi mutatói, valamint a transznacionális, professzionális, mobil és minden gátlást és határt nélkülöző terrorszervezetek által nyilvánul meg, amelyek minden egyes nemzetállam biztonságára potenciális veszélyt jelentenek.

A kultúrák szempontjából a globalizáció, a digitalizáció és az informatikai fejlődés jövőjét illető kérdés úgy fogalmazódik meg, hogy az egyes nemzetek, országok, föderációk, államközösségek, régiók, szövetségek és szervezetek mindegyike képes lesz-e annak érdekében mozgósítani forrásait, hogy konfliktusmentesen kapcsolódjon be e folyamatba, vagy, hogy átalakuljon, esetleg megszűnjön? És ha nem, mely(ek) lesz(nek) az(ok) amely(ek) nem lesz(nek) képes(ek)? Mikor? És milyen áron?

A „globális közös terek" „kibertere"

A 2010. november 19–20-án, Lisszabonban megrendezett NATO-csúcsértekezleten Anders Fogh Rasmussen főtitkár bejelentette: az állam és kormányfők elfogadták az új stratégiai koncepciót, amely egy erősebb, hatékonyabb, ugyanakkor a globális szereplők és folyamatok irányába nyitottabb, együttműködőbb Szövetséget vizionál. A NATO-vezetők hitet tettek amellett, hogy a NATO-képességeket úgy alakítják a jövőben, hogy azok megbízhatóbb védelmet nyújtsanak korunk modern kihívásaival szemben. A ballisztikus rakétavédelem, a hibrid fenyegetések elleni küzdelem, az informatikai rendszerek védelme, valamint az elektronikus hadviselés kiemelt figyelmet kap a Szövetség jövőbeni képességfejlesztésében.[1] A stratégiai koncepció előkészítésében aktívan közreműködő Szövetséges Transzformációs Parancsnokság (Allied Command Transformation – ACT) a modern kihívások alaposabb vizsgálata céljából indította el az ún. „globális közös terek" (Global Commons) projektet, amely tulajdonképpen azon földrajzi és virtuális dimenziókban rejlő lehetőségeket vizsgálja, amelyek nem köthetők egy adott országhoz, régióhoz, viszont meghatározóak a NATO egésze és tagországai biztonsága szempontjából. Ezek a közös dimenziók alapvetően a tengerek és óceánok; a légtér; a világűr, és a kibertér.

A „Globális közös terek" címmel indított ACT-tanulmány[2] azon földrajzi és virtuális terekben rejlő biztonsági kihívásokat és hatalmi kontroll-lehetőségeket vizsgálja, amelyek nem köthetők egy adott nemzethez, országhoz vagy régióhoz, viszont meghatározó fontossággal bírnak a NATO egésze és tagországai szempontjából. A közös tengerek és óceánok; a légtér; a világűr és a kibertér olyan, egymással összekapcsolt, ugyanakkor egymást át is fedő, illetve egymástól függő terek, amelyek behálózzák a földkerekséget. Mivel lehetővé teszik az információk, áruk, szolgáltatások és az emberiség számára fontos egyéb termékek áramlását, valamint az ember mozgását, mindenki használja azokat.[3] A globalizálódó világban a közös terek stratégiai jelen-

1 NATO Summit paves way for renewed Alliance, NATO HQ, 20 Nov. 2010, online: http://www.nato.int/cps/en/SID-A807E092-E5343B66/natolive/news_68877.htm (2010. december 1.)

2 The Global Commons Initiative, The Global Commons Homepage, Allied Command Transformation, NATO, online: http://www.act.nato.int/globalcommons (2010.december 1.)

3 Protecting the Global Commons, Security and Defence Agenda, Atlantic Council, Brussels, 2010 November

tősége fokozatosan nő, nemcsak a jóhiszemű, hanem a rosszhiszemű felhasználók számára.[4] A biztonság kutatásában élenjáró szervezetek – köztük a NATO – figyelmét az a felismerés vezeti e téren, hogy a dimenziók egyikén, vagy akár többjükön relatív kis anyagi ráfordítással és innovációval, stratégiai károkat lehet okozni. Annak érdekében, hogy a NATO és annak tagállamai képesek legyenek e kihívások kezelésére, komoly politikai, diplomáciai és katonai lépéseket kell tenniük a külső és belső szabályozás terén egyaránt. E feladat azért is sürgető, mert a probléma kétélű: egyfelől a fokozódó globalizáció és technológiai forradalom miatt gyorsan, nehezen követhetően változnak a biztonsági körülmények, ezért a késlekedés később csak jelentős többletráfordítással behozható, stratégiai hátránnyá nőhet. Másfelől, az Egyesült Államok és nyugati szövetségesei által definiált – és egyébként eddig dominált – globális közös terek adta lehetőségeket mind gyakrabban használják ki azok a rosszhiszemű, rendszerint nem állami szereplők, amelyek károkat vagy akár direkt csapást mérhetnek a nyugati világra.

A négy dimenzió jelentősége katonai szempontból számottevő, hiszen a legfelsőbb parancsnokságoktól egészen a legkisebb alakulatokig, folyamatosan használják azokat a manőverek – de legfőképpen a vezetés, irányítás, összeköttetés – alkalmával.[5] A Szövetség a műveletek során például aktívan használja a csapatok és hadianyagok szállítására a világtengereket és légteret, vezetésirányításra, felderítésre, navigációra a légteret és világűrt vagy a vezetésirányítás fenntartására és kommunikációra a kiberteret. Tekintettel arra, hogy a NATO katonai alakulatainak nemcsak az a feladata, hogy saját magukat védelmezzék, hanem a tagországok érdekeit is – ideértve azok kereskedelmét, kutatásait vagy távközlését –, mindezen felül készen kell állniuk a katonai feladat-végrehajtásra a négy dimenzió bármelyikében. Ez természetesen jelentős felderítő, stratégiai elemző, tervező, vezetési, képességfejlesztő, logisztikai és műveleti előkészítő tevékenységet követel a globális terekre vonatkozóan.

A négy dimenzió vonatkozásában egyértelműen megállapítható, hogy sok szempontból közös jegyekkel rendelkeznek, ezért össze is kapcsolódnak, átfedik egymást, más szempontból viszont számos sajátos tulajdonságuk van. Ebből kifolyólag általános és specifikus szempontból egyaránt vizsgálni kell őket.[6] A biztonság szempontjából a globális dimenziók közül a kibertér kapja a legnagyobb figyelmet, hiszen ezeket az emberiség az utóbbi néhány évtizedben „kreálta", s ezért nem áll rendelkezésre elegendő nemzetközi jogi vagy történelmi tapasztalat annak szabályozására, kezelésére. Eltérően a tengerektől és a légtérről, a kibertér nem írható körül egyértelműen, mert nem rendelkezik tisztán definiálható határokkal. A technológiai fejlődés ezek esetében nem egy behatárolt térben történik, mitöbb, sokkal inkább az a jellemző rá, hogy a technológia tökéletesedésével a kibertérben rejlő lehetőségek, távlatok is dinamikusan bővülnek. A globális közös terek jellemvonásai, a bennük rejlő törvényszerűségek megismerése nemcsak azért fontos, mert mindennapi életünkben állandóan használjuk őket, hanem elsősorban azért, mert a szemben álló felek stratégiai előnyöket érhetnek el vagy veszteségeket szenvedhetnek rajtuk.

4 Scott Jasper: Securing Freedon int he Global Commons, Stanford University Press, California, USA, 3.o.

5 Linton Wells II: Maneuver in the Global Commons – The Cyber Dimension, SIGNAL Magazine, December 2010, online: http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2472&zoneid=306 (2011. január 25.)

6 Tara Murphy, Security Challenges in the 21st Century Global Commons, Yale Journal of International Affairs, Vo-lume 5, Issue 2 - Spring/Summer 2010, Spotlight on Security, July 20, 2010, online: http://yalejournal.org/2010/07/security-challenges-in-the-21st-century-global-commons/ (2010. december 9.)

A kibertér bizonyos szempontból a legegyedibb dimenzió az összes közül, hiszen nem köthető és nem is jellemezhető csak fizikai vagy földrajzi fogalmakkal. Ugyanakkor a kibertér nagyban függ fizikai eszközöktől, technológiáktól, számítógépektől, szerverektől, terminálóktól, kábelektől, antennáktól, műholdaktól, amelyek már nem virtuálisak, hanem birtoklásuk és helyük is meghatározható.[7] Mihelyst egy információ útjára indul a mesterségesen kialakított csatornákon át, adott tartózkodási helyének meghatározása rendkívül bonyolulttá válik. Egy adott számítógépről indított információ szerverek, jeltovábbítótornyok, optikai kábelek, műholdak sokaságán keresztül jut el rendeltetési helyére. Az adathalmaz ez esetben nem a legrövidebb úton halad, hanem útját alapvetően a hálózatok szabad és olcsóbb kapacitásai határozzák meg. Az adott információ eközben egyfelől haladhat a földi optikai vagy más kábeleken, a légtérben elektronikai jelcsoportként, a tengerekbe lefektetett rugalmas optikai kábeleken vagy műholdas rendszereken a világűrben. Ez a típusú információforgalom már ma is több milliószor megy végbe óránként a világban, miközben mennyisége és minősége hatványozottan fejlődik. Egyértelműen prognosztizálható: a kibertér rendszerei nagyobbá, gyorsabbá és komplexebbé válnak az idő előrehaladtával.

A kibertér sebezhetőségét pontosan annak komplexitása adja, amelynek – ma ismert – elsődleges támadói a hackerek. Egészen az elmúlt évekig bezárólag a támadások főleg a szoftverekre irányultak, vagyis a hackerek a programokat és a virtuális rendszereket támadták. Ez azonban erőteljesen változik. Eltérően a többi dimenziótól a kibertér információbázisa és technológiai infrastruktúrája túlnyomó részt civil és kereskedelmi szereplők tulajdonában van.[8] A kibertér ezért elsősorban nem államoktól vagy kormányoktól függ, s a különböző rendszerek biztonságát sem azok garantálják elsősorban. Erről maguk a civil cégek gondoskodnak. A helyzetet tovább bonyolítja, hogy a tulajdonosok gazdasági szereplők, így a piac szabályai szerint tevékenykednek, és erős gazdasági konkurenciaharcot folytatnak egymással.[9] Ilyen körülmények közt a kibertér szolgáltatóinak sokkal inkább az az érdeke, hogy ellenálljanak a külső korlátozásoknak, kibújjanak az állami és nemzetközi szabályzók alól, s a szabályok által előírt biztonságot háttérbe szorítsák. Ez természetesen nagyobb szabadságot, kreatívabb fejlesztéseket, s nem utolsó sorban olcsóbb fenntartást biztosít számukra. Pontosabban: a külső szabályzókból fakadó kötelezettségek szigorú betartása helyett saját biztonságukra és fejlesztésekre költik az összegeket. Amennyiben ez a paradox helyzet így marad, az államok – nemzetközi jog által biztosított – kontrollszerepe folyamatosan gyengül.

A kiberteret jellemző extrémitások, szabályozatlanságok és veszélyek egyik legjobb példája a 2010 őszén kirobbant Wikileaks-botrány. Mint ismert, az internetes szolgáltató és támogatói arra szakosodtak, hogy bizalmas vagy akár szigorúan titkos információkat tegyenek közre függetlenül attól, hogy azok egyéni, cég, vagy kormányzati forrásból származnak. Mivel e tevékenység súlyos károkat és érdeksérelmet eredményezett számos civil cégnek és államnak, nagyszabású ellenkampányba kezdtek a sértettek. Jelenleg nagy intenzitású és szerteágazó hackertámadás, kormányzati felderítő művelet, rendőrségi eljárás, diplomáciai koordináló tevékenység, valamint

7 Ron Deibert: Toward a Cyber Security Strategy, Vanguard, Canada, online: http://www.vanguardcanada.com/CyberArmsRaceDeibert (2011. január 28.)

8 The National Strategy to Secure Cyberspace, The White House Washington, February 2003, online: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (2010. december 17.)

9 Ziad I. Akir: Space Security: Possible Issues & Potential Solutions Space Journal Issue 6 2004

gazdasági-pénzügyi ellehetetlenítés folyik a wikileaks.com ellen.[10] Valószínűsíthető, hogy az állami érdekeket ért durva Wikileaks-támadás apropóul szolgál az állami védekezőmechanizmusok megszilárdításához, köztük a titkosszolgálati informatikai képességek fejlesztéséhez.

Katonai szempontból a 2007 májusában, Észtország ellen észlelt kibertámadás és a 2008 nyarán kirobban orosz–grúz konfliktus szolgáltatja a legutóbbi tanulságot. Az Észtország ellen indított informatikai támadást ma az elemzők a hadtörténelem első nagyszabású, igazi, országok között zajló „kiberháborújának" nevezik. A Tallin elleni kiber-haditerv egy ún. DDOS-támadás volt, amely az informatikai rendszerek túlterhelését és ezáltal működésképtelenségét idézte elő. A célpontok között az észt parlament, kormányhivatalok, minisztériumok, bankok, telefontársaságok és médiacégek szerverei voltak. Egybehangzó szakértői vélemények szerint a célpontok kiválasztása, a támadások szervezettsége, egységessége, hadműveleti ütemezése és ereje messze túlmutat azon, amit egyszerű hackercsoportok vagy akár a szervezett alvilág képes lenne végrehajtani. Az észt informatikai hálózatoknak ugyanis a normális adatforgalom ezerszeresét kellett volna kezelniük, amire természetesen nem voltak képesek.[11] Mivel Észtország kérte a NATO Tanács összehívását, az incidens kivizsgálására széleskörű nemzetközi összefogás jött létre. Ennek ellenére nem voltak képesek igazolni, hogy a támadások honnan indultak, és pontosan mely állam állt a háttérben. A célpontokat ellehetetlenítő adatfolyamok ugyanis vírusokkal voltak fertőzve, és a világ különböző helyein telepített ideiglenes szerverekről érkeztek. Csak gyanítható, hogy mindemögött orosz kományhivatalok álltak valójában.

Az orosz–grúz konfliktus kiberdimenziója ennél világosabb képet mutat. Moszkva rádióelektronikai felderítő szervei, szorosan az orosz hadvezetéssel, összehangolt csapást mértek a grúz civil és kormányzati kiberrendszerek ellen, aminek következtében a civil nyílt és a minősített kormányzati informatikai hálózatok is összeomlottak.[12] Ez esetben nemcsak a virtuális rendszereket támadták, hanem a fizikai infrastruktúrát is. Mindez tulajdonképpen hosszú időre lebénította a grúz kormányzat teljes egészének védelmi képességét. Túlzás nélkül kimondható, hogy a fent említett hasonló helyzetek még az olyan államok védelmi rendszereit is tönkre teheti, mint a NATO vezető hatalmaié, nem beszélve arról, ha ezeket konkrét fegyveres cselekmények is követik.

A NATO informatikai rendszerei elleni folyamatos támadásokra válaszul a Szövetség 2009-ben kiadta a kibervédelemre vonatkozó koncepcióját, amely komplexen leírja a virtuális és fizikai infrastruktúrák védelmét, valamint szól azon területekről is, amelyeket a NATO érdekövezetébe sorol.[13] A NATO informatikai rendszereit ért támadások mellett azonban a technológiai fejlődés nyomása is nagyban inspirálta a döntéshozókat. A NATO vezetése már évekkel ezelőtt felismerte, hogy az ún. digitalizált had- és műveleti vezetésre való áttérés ma már alapkövetelmény, amelynek alapvetéseit és védelmét a legmagasabb

10 Láthatatlan seregek vívják a WikiLeaks-háborút, origo.hu, online: http://www.origo.hu/nagyvilag/20101209-wikileaks-julian-assange-internetes-haboru.html (2010. december 16.)

11 Ian Traynor, Russia accused of unleashing cyberwar to disable Estonia, The Guardian, 17 May 2007, online: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (2010. december 16.)

12 Gadi Evron, Internet Attacks Against Georgian Websites, CircleID Internet Infrastructure, Aug 11, 2008, online: http://www.circleid.com/posts/88116_internet_attacks_georgia/ (2010. december 16.)

13 Evgeny Morozov, The Fog of Cyberwar, NATO military strategists are waking up to the threat from online attacks, Newsweek, April 18, 2009, online: http://www.newsweek.com/2009/04/17/the-fog-of-cyberwar.html# (2010. december 16.)

szintű koncepcionális dokumentumoknak is tartalmazniuk kell.[14] A Szövetség tehát egy „föntről lefelé" elvet követő szabályzómechanizmussal foglalta koncepcióba a stratégiai elveket és sztenderdeket, ugyanakkor a gyakorlati munka során a döntéshozó, felelős szervek és végrehajtók vonatkozásában pedig operatív, ellentétes irányú, „alulról felfelé" munkamódszerre épít.[15] Mindebben az emberi tényezőt tartja a legfontosabbnak, hiszen minden kibertámadás, és azok kivédése mögött is, elsősorban emberi tevékenység áll. A védelem szempontjából tehát mindennél fontosabb a NATO-felhasználók, rendszerfenntartók és -gazdák képzése, felkészítése.

Nemzetközi kitekintés

A NATO és az Egyesült Államok

A NATO először az 1999-es koszovói bombázás során szembesült a kiberhadviselés eszközeivel. A katonai beavatkozás 1999. március 24-én indult Slobodan Milosevic csapatai ellen. A támadást követően szerbiai hackerek megtámadták a NATO weboldalait. A folyamatos túlterheléses támadásoknak (Distributed Denial of Service – DDoS) köszönhetően több alkalommal hosszú időre elérhetetlenné vált a NATO honlapja. A támadásokért felelős Fekete Kéz elnevezésű szerb hackercsoport mindezek mellett több kormányzati oldalra helyezte el politikai üzeneteit, és több alkalommal megpróbáltak betörni a NATO parancsnoki szervereibe, nagyrészt sikertelenül, tekintve, hogy bár a légierő számítógépes hálózatába sikeresen bejutottak, azonban titkos információkhoz nem fértek hozzá. A Belgrádban található kínai nagykövetség bombázásának hatására csatlakoztak kínai, majd később orosz hackerek is, akik szintén túlterheléses támadásokkal és deface-technikával szabotálták mind a NATO, mind pedig az amerikai nagykövetségek weblapjait. A „From Russia With Love" elnevezésű orosz hackercsoport volt a zászlóshajója a NATO elleni támadásoknak, statisztikák szerint legalább 14 katonai és állami weboldalt törtek fel szerb hackerekkel együtt az 1999-es balkáni háború alatt. Nagyrészt a koszovói beavatkozást követő kiberincidensek segítették hozzá a döntéshozókat ahhoz, hogy felismerjék a kiberbiztonság fontosságát. Ennek eredményeképpen a 2002-es prágai csúcstalálkozó alkalmával elindították a NATO kibervédelmi programját, melynek részét képezte a Számítógépes Incidenskezelő Képesség kialakítása is. A képesség mögött álló Technikai Központ képes érzékelni a NATO rendszereibe történő behatolásokat. Ezzel kezdetét vette az Észak-atlanti Szerződés Szervezetének felkészülése a kiberhadviselésre.[16]

Napjainkban a NATO, az Egyesült Államok koncepció- és stratégiafejlesztési rendszeréhez igazodva, annak mintájára komplex rendszerként kezeli a digitalizációt és a kiberteret, egyfelől alkalmazza, épít rá saját és fejleszti rendszereiben, másfelől mint – a globális közös

14 Rex B. Hughes: NATO and Cyber Defence, What steps have been taken by NATO against the threat of cyber at-tacks? What needs to be done to prevent them in the future? Mission Accomplished? Ap: 2009nr1/4, online: http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf (2011. január 28.)

15 Rex B. Hughes, Mission Accomplished? NATO and Cyber Defence, 2009 1/4 online: http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf (2010. december 16.)

16 Szentgáli Gergely: A NATO kibervédelmi politikájának fejlődése, Nemzet és biztonság, Budapest, online: http://uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf (2017. december 28.)

terek egyike – létének és hadszíntereinek egyikeként tekint rá[17] a doktrinális rendszerek vonatkozásában NNEC DJTS stb. Ugyan önálló kibererőket a Szövetség még nem hozott létre, rendelkezik egy ún. Kiber-védelmi Kiválósági Központtal (NATO Cooperative Cyber Defence Centre of Excellence – NATO CCD COE). A Tallinnban 2010-ben alapított szervezet egyszerre funkcionál úgy, mint a NATO által akkreditált tudásközpont, kutatóintézet, kiképző és oktatási bázis, valamint gyakorlóközpont. E nemzetközi katonai szervezet interdiszciplináris alkalmazott kutatásokat folytat, valamint oktatási kurrikulumokat, kiképzéseket, gyakorlatokat kezdeményez és fogad be. Állományát tekintve a szervezet nemzetközi szakértőkből, tudósokból, jogászokból, stratégiai tervezőkből és katonákból áll, akik közösen folytatnak kiber- és technológia-jellegű kutatásokat a NATO és tagországai katonai, kormányzati, közigazgatási és ipari érdekei mentén. A tagság nyitott minden szövetséges állam előtt. A jelenleg aktívan résztvevő országok: az Amerikai Egyesült Államok, Csehország, az Egyesült Királyság, Észtország, Franciaország, Görögország, Hollandia, Lengyelország, Lettország, Litvánia, Magyarország, Németország, Olaszország, Spanyolország, Szlovákia és Törökország. Ausztria és Finnország, mint nem NATO partnerországok együttműködési partnerséget írt alá.[18]

Kína

A kínai gazdasági csoda és az annak nyomán rögzülő komplex hatalmi expanzió mára klisévé vált. Kína, kétséget kizárólag a világ politikai, gazdasági élvonalába került az elmúlt alig negyed században, s mára egyetlen másik hatalom sem hagyhatja figyelmen kívül Peking érdekeit, s e bővülő expanziót. A kínai csoda és imperializmus azonban nem állt meg, és az ország globális hatalmi terjeszkedésében a kibertér nem egy elhanyagolt portfólió.[19]

Az Internet Live Stats mérései szerint Kínában 721 434 547 internetfelhasználó volt 2016-ban, ami az 1 382 323 332 lélekszámú kínai lakosság 52,2%-a. Ez a világ 3 424 971 237 összes internetfelhasználójának 21,1%-a.[20] Ez annál is inkább megdöbbentő adat, mert alig egy évtizede az internet egésze a kínai központi kormányzás által cenzúrázott hálózat volt. Ma Kína rendelkezik a legstrukturáltabb és legnagyobb állami informatikai rendszerrel Ázsiában.[21] Ebbéli pozícióját tartva és fejlesztve, Kína nemzetközi viszonylatban és abszolút értelemben is jelentős fejlesztéseket eszközöl az informatikában, s napjainkban nemcsak mint felhasználó, hanem mint fejlesztő is jelen van a digitális piacon.

A világ legnépesebb államaként és földünk egyik legnagyobb digitális rendszerével rendelkező ázsiai hatalomként idejekorán felismerte a kibertér veszélyeit és az abban rejlő lehetőségeket, ideértve annak katonai felhasználását. A kínai biztonsági és katonai rendszerek

17 Babos Tibor: "Globális közös terek a NATO-ban", Nemzet és Biztonság, Stratégiai és Védelmi Kutató Központ, Budapest, 2011. április, On-line: http://www.nemzetesbiztonsag.hu/cikkek/babos_tibor-___globalis_kozos_terek____a_nato_ban.pdf

18 History, Structure, NATO Cooperative Cyber Defence Centre of Excellence, online: http://www.ccdcoe.org./history.html (2018. január 10.)

19 Mikk Raud, China and Cyber: Attitudes, Strategies, Orgainaztion, NATO Cooperative Cyber Defence Centre of Excellence, online: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (2017.augusztus 27.)

20 Internet Live Stats, online: http://www.internetlivestats.com/internet-users/china/ (2018. január 25.)

21 Desmond Ball, China's Cyber Warfare Capabilities, online: https://indianstrategicknowledgeonline.com/web/china%20cyber.pdf (2017. december 20.)

közvetlen megjelenését, aktivitásuk növekedését a világhálón egyértelműen detektálják a nemzetközi internetes mérések. Ezt azt igazolja, hogy Kína világviszonylatban is számottevő eszközparkot hozott létre, és szakembergárdát mozgósított a digitális átalakulás érdekében. A kínai Kormányzat azonban nem tekinti önálló témának a digitális forradalmat, ezért önálló kiberszervezeteket vagy ilyen jellegű hierarchiákat nem hozott létre mindezidáig. A bonyolult kínai államigazgatási struktúrák és ismert koncepcionális dokumentumok inkább arra engednek következtetni, hogy a kormányzati portfóliók mindegyikét és az állam minden szegmensét alakítják át egyszerre és teszik képessé az informatika befogadására, kezelésére.[22]

Hszi Csin-ping (Xi Jinping), a Kínai Népköztársaság elnöke 2016-ban személyes felügyelete alatt hozta létre a Központi Internet-biztonsági és az Információvezetési Csoportot, amelynek fő feladatául szabta Kína kiberstratégiájának elkészítését. Ez is egyértelműen azt bizonyítja, hogy a digitalizációt és informatikát Peking a társadalmi fejlődés természetes velejárójának tekinti, ezért nem különíti el sem a kormányzás, sem a Kínai Kommunista Párt ideológiájától. E rendkívül érdekes szemléletből számos következtetés levonható:

- a világ legnagyobb nemzeti internetközössége központi kormányzás alatt áll;
- a közösség méretére tekintettel e kormányzás direkt módon hat az internethálózat egészére, befolyásolja azt;
- Kína ezzel nemcsak, hogy részévé, hanem domináns szereplőjévé is vált az online világnak, s mivel az internet a nyugati értékek és kultúra mentén kezdett el feltöltődni, közvetlen információs kaput is jelent számára, miközben Kína maga is sok területen adaptálódott a nyugathoz;
- mindez fordítva nem igaz, hiszen Kínából szinte semmi nem jelenik meg nyugaton a világhálón;
- alkalmazkodva az internet adta lehetőségeihez, Kína számtalan területen jutott többletinformációhoz és kapcsolati tőkéhez.[23]

Kihasználva ezen körülményeket, Kína tudatosan bővítette ilyen jellegű nemzetbiztonsági és katonai képességeit is. Bizonyított tény, hogy a pekingi kormány utasítására a kínai haderő, kínai magánvállalatok és magánszemélyek aktív informatikai és információs tevékenységet folytatnak a nyugati hatalmak és a szomszédállamok irányába. Ezen műveletek célrendszerét a tudományos kutatások, technológiai titkok, az ipari fejlesztések, kormányzati rendszerek, minősített információk képezik. Peking ezzel egyértelműen mutatja, hogy éppúgy, mint az elmúlt 30-40 évben, kész jogellenesen és agresszívan is technológia és know how lopására, hogy megragadja a stratégiai kezdeményezést és direkt gazdasági, politikai vagy katonai előnyre tegyen szert. A kínai információs tevékenység sikerét mi sem bizonyítja jobban, mint a komplett amerikai F-35-ös vadász- és bombázórepülőgép fegyverrendszer-ellopása, ami az Egyesült Államok legdrágább hadiipari fejlesztése volt.[24]

22 Mikk Raud, China and Cyber: Attitudes, Strategies, Orgainaztion, NATO Cooperative Cyber Defence Centre of Excellence, online: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (2018. január 26.)

23 Mikk Raud, China and Cyber: Attitudes, Strategies, Orgainaztion, NATO Cooperative Cyber Defence Centre of Excellence, online: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (2018. január 13.)

24 Mikk Raud, China and Cyber: Attitudes, Strategies, Orgainaztion, NATO Cooperative Cyber Defence Centre of Excellence, online: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (2018. január 6.)

Oroszország

A kiberhadviselést Oroszország teljesen eltérően értelmezi és kezeli, mint a nyugati szövetségesek. A téma nem új elemként, hanem az orosz stratégiai teoretikusok általános és hagyományos koncepcióiba illeszkedik, mint új lehetőség és hadviselési tér. A Kreml stratégái szerint Oroszországot az Egyesült Államok által dominált és terjeszkedő NATO geostratégiai nyomás alatt tartja, és éppúgy, mint minden más területen, az informatikai rendszereken és hálózatokon keresztül is fenyegeti az ország biztonságát. Az információs teret Oroszország alapvetően állandónak és végtelennek tekinti. Az internet, az információk szabad áramlása, az adatokhoz való nyílt hozzáférés, Moszkva számára egyszerre fenyegetés és lehetőség, amit ki kell aknázni. Ezzel együtt a Kreml relatíve sokkal kevésbé ambicionálja az olyan nagyarányú kiberfejlesztéseket, mint amit az amerikai hadvezetés eszközöl, viszont a téma tudáshátterébe és humántámogatásába komoly tőkét invesztál.

Az orosz katonai szakírók nem használják sem a „digitális", sem a „kiber" szót a katonai rendszerek vonatkozásában. A koncepcionális dokumentumokban sokkal inkább az ún. „információs rendszerek" és „információs hadviselés" jelenik meg, ami egy általános keretként szolgál a számítógépes rendszerek, informatika, elektronikus hadviselés, információs műveletek és pszichológiai hadviselés témákhoz. Ebből kifolyólag a kiber és az informatika inkább egyfajta eszköz, mint önálló stratégiai dogma Oroszország számára. Eszköz- és térjellegéből adódóan, és illeszkedve az információs rendszer koncepcióba a hadvezetés egyre nagyobb hangsúlyt fektet a témára a hagyományos műveletek során. A mai kiberműveleteket tanulmányozó számos szakíró felvetette azt is, hogy a komplex információs műveleti képesség kialakítása akár már rövidtávon is felkerülhet Oroszország stratégiai elrettentő képességei közé.

Jóllehet a Vörös Hadsereg meglehetősen elmaradottnak tekinthető az informatikai fejlesztések tekintetében, hiszen mindezidáig a digitalizálás csak a hagyományosan high tech űr-, rakéta-, repülőgép-, haditengerészeti és tűzvezetési rendszerekben van jelen, a haderő doktrinálisan és strukturálisan egyaránt nélkülözte az információs kor alapvető vívmányait is. Ennek egyik fő oka, hogy a globális hálózatok adta fenyegetésektől védeni akarták a katonai rendszereket. A 2008 augusztusában kirobbant orosz–grúz konfliktus műveleti tapasztalatai ugyanakkor egyértelműen arra utalnak, hogy a Vörös Hadsereg kibertámadó és -elhárító képességei létrejöttek és sikeresen működnek. A Vörös Hadsereg kiberképességei az orosz–ukrán válságban debütáltak világszínvonalon, amikor egyértelművé vált, hogy magas színvonalú eszközparkkal, kiváló eljárásrenddel és műveleti készséggel voltak képesek uralni a kiberhadszínteret és elrettenteni az ellenséget támogató külső erőket is.

A nemzetközi kibereseményekvizsgálata során született megállapítások mindegyike igazolja, hogy közvetlenül vagy közvetve Oroszország szinte minden jelentős esetben jelen volt és saját érdekeinek megfelelően zárta a cselekményt. A katonai műveletek információs támogatásán túl az orosz információs képességek nap mint nap felvillannak, legyen az kiberbűnözés; elektronikus banki rendszerek, tranzakciók; hírközlő csatornák és médiák vagy informatikai támadások bizonyos állami, közigazgatási rendszerek ellen.

A DJP és a DJP 2.0 katonai kapcsolódásai

A mai értelemben vett digitalizáció, számítástechnika és internet a második világháborús katonai rendszerekben kezdte meg fejlődését, majd a hidegháború katonai tömbjeiben kapott új lendületet, s az ötvenes évekre már a teljesen elszabadult fegyverkezési verseny nukleáris és hagyományos *high tech* fegyverrendszerek műszaki vezérlőberendezéseiben teljesedett ki. Az informatika ma éppúgy jelen van a fejlett világ katonai szervezeteiben, mint a feltörekvő országok haderejében. Az Egyesült Államok, Franciaország, Nagy-Britannia vagy Németország katonai rendszereinek vezetése, irányítása, híradása, logisztikája, utánpótlás-szervezése, vagy hadiipari fejlesztései éppúgy digitális platformokon történnek, mint Kínában, Indiában, Brazíliában vagy Oroszországban.

A DJP és DJP 2.0 szempontjából ez azt jelenti, hogy a magyar védelmi, nemzetbiztonsági és katonai rendszereket az alábbi négy követelménynek kell megfeleltetni: (1) be kell ágyazódniuk a mindenkori magyar digitális rendszerbe; (2) – szövetségesi és uniós tagságunkból adódóan – biztosítani kell a hazai védelmi, katonai és hadiipari rendszerek NATO- és EU-kapcsolódását, -interoperabilitását; (3) a békeidőben kialakított katonai informatikai rendszernek arra is képesnek kell lenniük, hogy bármilyen, a békeállapottól eltérő jogrendben, önállóan is képesek legyenek – korlátozásokkal – az ország vezetését, irányítását és a közigazgatás működését biztosítani.

A DJP által rövidtávon kitűzött általános feladatokhoz igazodva az alábbi honvédelmi, katonai és nemzetbiztonsági célrendszer meghatározása indokolt:

- A magyar honvédelmi, nemzetbiztonsági és katonai rendszerek egésze – ideértve az eszközparkot, az azt üzemelő személyi állományt és eljárásrendet – lépjen egyet előre a digitális felkészültség terén.
- Minden honvédelmi, katonai és nemzetbiztonsági alrendszer, amely informatikán, technológián alapszik vagy kapcsolódik ahhoz, a digitalizáció fontosságát időben felismerve növelje verseny-, védelmi és műveleti képességét.
- A honvédelmi, katonai és nemzetbiztonsági informatikai, digitális és hálózatalapú rendszerek kialakítása egy egymásra épülő, egymással kapcsolatban lévő és egymást kiegészítő, szükség esetén redundáns rendszerként is funkcionáló egységet képezzen, hogy a történelmi léptékű digitális átalakulás nyerteseként nagyot lépjen előre a nemzetközi katonai és kiberhadszíntéren, ezzel is biztosítva Magyarország védelmét és nemzeti érdekeinek megvalósítását.
- Mindezzel együtt a katonai informatikai rendszerek fejlesztését úgy kell megvalósítani, hogy azok védve legyenek a polgári és civil platformok támadásaival szemben, bármikor leválaszthatók legyenek azoktól és bármikor, önállóan is képesek legyenek működni, hogy az ország vezetését békétől elérő állapotokban is folyamatosan lehetővé tegyék.

A 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017–2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről szóló kormányzati célok megvalósításához igazodva (a Korm. határozat felépítését követve) az alábbi honvédelmi, katonai és nemzetbiztonsági területek kapcsolódása javasolt:[25]

25 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelen-téséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munka-terve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről, Net-jogtár, online: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A17H1456.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (2018. február 1.)

- (Preambulum) a Kormány a Digitális Jólét Program 2.0 végrehajtása során megteremtett széleskörű társadalmi párbeszéd fórumaiba, szakmai, társadalmi, érdekképviseleti és tudományos szervezetek közreműködésébe és együttműködésébe be kell vonni a honvédelmi és nemzetbiztonsági szervezeteket (Honvédelmi Minisztérium, Magyar Honvédség, Katonai Nemzetbiztonsági Szolgálat);
- a nemzeti fejlesztési miniszter által bemutatott, *Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentése* című dokumentum (NIS Monitoring jelentés) honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, katonai nemzetbiztonsági és hadiipari vonatkozások);
- a Digitális Jólét Programjával kapcsolatos kormányzati feladatok összehangolásáért és megvalósításáért felelős miniszterelnöki biztos által számára bemutatott, *Digitális Jólét Program 2.0* című stratégiai dokumentum honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, katonai nemzetbiztonsági és hadiipari vonatkozások);
- a Szupergyors Internet Program (SZIP) keretében zajló fejlesztések, a Nemzeti Távközlési Gerinchálózattal (NTG) kapcsolatos fejlesztések, a Nemzeti Információs Infrastruktúra Fejlesztési (NIIF) Program továbbfejlesztése, a magyarországi hírközlési szolgáltatók önerős digitális hálózatfejlesztési beruházásai, valamint a szupergyors internetelérés sebességének megfelelő ütemű emelését célzó program honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, hadműveleti, vezetési és irányítási, katonai nemzetbiztonsági és hadiipari vonatkozások);
- a mobil távközlés új technológiai megoldása, az 5G hálózati és alkalmazásfejlesztések, és a vezető nélküli gépjárművek elterjesztése, honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (hadműveleti, vezetési és irányítási, haditechnikai és hadiipari vonatkozások);
- szakmai, tudományos és érdekképviseleti szervezetek részvételével megalakuló Magyarországi 5G Koalíció, valamint Magyarország 5G Stratégiája és akcióterve honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (hadműveleti, vezetési és irányítási, haditechnikai és hadiipari vonatkozások);
- a digitális felkészültség és kompetenciák, a digitálisan felkészült munkavállalók szakirányú honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, hadkiegészítési, hadműveleti, vezetési és irányítási és hadiipari vonatkozások);
- a Digitális Munkaerő Program végrehajtásának honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, hadkiegészítési, a HM irányítása alatt álló hadiipari cégvonatkozások);
- nemzetgazdasági szempontból kiemelten fontos mikro-, kis- és középvállalkozások számára indítandó, a mikrovállalkozások digitális felkészültségének javítását célzó átfogó program honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, hadkiegészítési, hadműveleti és a HM irányítása alatt álló hadiipari cégvonatkozások);

- a nemzetgazdasági ágazatok digitalizációját támogató egységes módszertani kézikönyv és mérési, minősítési rendszer kidolgozása, valamint a Digitális Szolgáltatás Kereskedelem-fejlesztési Stratégia honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, hadkiegészítési, és a HM irányítása alatt álló hadiipari cégvonatkozások);
- Magyarország Digitális Agrár Stratégiájának és a stratégia végrehajtását támogató intézkedések honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (katonai és műveleti térképek komplex digitális tartalmai, fóliarendszerei);
- a digitális eszközök és technológiák szerepe az egészségmegőrzésben, a betegségek megelőzése a gyógyászati tevékenységben, illetve az egészségipar digitális innovációs tevékenysége érdekében elrendelt Magyarország Digitális Egészségipar-fejlesztési Stratégiája, valamint az Idősügyi Infokommunikációs Modellprogram honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (katonai egészségügy, Honvédkórház, NATO Egészségügyi Kiválósági Központ);
- a digitális technológiák alkalmazásának felgyorsítása érdekében elrendelt Magyarország Digitális Sport Stratégiája honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (műveleti, kiképzési, képzési, katonaisport- (Honvédelmi Sportszövetség), versenysport-vonatkozások);
- a digitális közigazgatási szolgáltatások hatékony támogatása, az állampolgárok és a vállalkozások ügyintézése érdekében elrendelt, a közigazgatás digitalizációjával kapcsolatos feladatok átfogó nyomon követése és koordinációja, illetve a közigazgatásban dolgozók számára egységes referenciakeret, tananyagok és oktatási keretrendszer honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, hadkiegészítési, hadműveleti, vezetési és irányítási és hadiipari vonatkozások);
- a hazai informatikai mikro-, kis- és középvállalkozások, szellemi műhelyek innovációs tevékenységének és termékfejlesztésének támogatását szolgáló intézkedések honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi és technológiai kutatások, hadiipari vonatkozások);
- a nemzeti kulturális örökség részét képező közgyűjteményi kulturális kincsek egységes szemléletű digitális fejlesztése, a digitalizált kulturális értékek akadálymentes hozzáférhetővé tétele a köznevelés és az oktatás számára, illetve a polgárok digitális kulturális tartalmak iránti érdeklődésének élénkítése célkitűzések honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (hadtörténelem, történeti levéltár (Hadtörténeti Intézet és Múzeum), honvéd-hagyományőrzés);
- a polgárok, a vállalkozások és a közintézmények, valamint a magyarországi digitális hálózatok kiberbiztonsága honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (Honvédelmi Minisztérium, Magyar Honvédség, a HM felügyelete alatt működő hadiipari cégek, Katonai Nemzetbiztonsági Szolgálat);

- a Nemzeti Kiberbiztonsági Stratégia felülvizsgálata, valamint az annak nyomán elkészítendő tételes feladat- és felelősmegjelölést is tartalmazó intézkedési terv honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (Honvédelmi Minisztérium, Magyar Honvédség, a HM felügyelete alatt működő hadiipari cégek, Katonai Nemzetbiztonsági Szolgálat);
- a Digitális Jólét Program 2.0 kapcsán felmerülő információbiztonsági szempontok érvényesítésének honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (Honvédelmi Minisztérium, Magyar Honvédség, a HM felügyelete alatt működő hadiipari cégek, Katonai Nemzetbiztonsági Szolgálat);
- a digitális ökoszisztéma működését és fejlődését szolgáló hálózati kutatások és azok eredményeinek közvetlen hasznosítása a közigazgatás fejlesztésében, az oktatásban és képzésben honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (Honvédelmi Minisztérium, Magyar Honvédség, a HM felügyelete alatt működő hadiipari cégek, Katonai Nemzetbiztonsági Szolgálat);
- a helyi, települési és térségi közösségek digitális fejlesztési programjainak, illetve az Okos Város (Smart City) fejlesztések nyomán indított Okos Város munkacsoport, illetve Okos Város és Okos Térség közigazgatási mintaprojekt honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (Honvédelmi Minisztérium, Magyar Honvédség, védelmi igazgatás, a HM felügyelete alatt működő hadiipari cégek, Katonai Nemzetbiztonsági Szolgálat);
- a digitalizációval együtt járó társadalmi, élettani és környezeti hatások felmérése, a kedvezőtlen hatások enyhítése érdekében elrendelt kutatások, valamint a digitalizáció nyomán megjelenő káros társadalmi hatások kezelése, illetve a jogrendszerben való szankcionálása honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (Honvédelmi Minisztérium, Magyar Honvédség, védelmi igazgatás, a HM felügyelete alatt működő hadiipari cégek, Katonai Nemzetbiztonsági Szolgálat).

Digitális, informatikai és hálózatalapú katonai célrendszerek

Az Alaptörvényben, továbbá a honvédelemről és a Magyar Honvédségről (MH), valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvényben (Hvt.) meghatározottak szerint az MH-nak, honvédelmi feladatai ellátása érdekében külső fegyveres támadás elhárítására békeidőszakban felkészített erőkkel, eszközökkel és képességekkel kell rendelkeznie. Ebből következik, hogy az MH-nak már békeidőszakban ki kell építenie és működtetnie kell a vezetéshez és irányításhoz szükséges saját üzemeltetésű híradó, informatikai és információvédelmi rendszereket. A Hvt. egyes rendelkezéseinek végrehajtásáról 290/2011. (XII. 22.) Korm. rendelet (Hvt. vhr) értelmében az MH vezetési és irányítási feladatai érdekében MH Kormányzati Célú Elkülönült Hírközlő Hálózatot (MH KCEHH) üzemeltet, melynek fejlesztéséért és működtetésért a honvédelmi miniszter a felelős. A kormányzati célú hálózatokról szóló 346/2010. (XII. 28) Korm. rendelet 2. melléklete elkülönült hírközlő hálózatként nevesíti a honvédelemért felelős miniszter által működtetett Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatot.

Az MH KCEHH az alábbi fő feladatok biztosítására kötelezett:

- A Hvt. vhr értelmében a MH KCEHH a Honvédség vezetési és irányítási feladatai érdekében üzemeltet állandó és tábori telepítésű híradó, informatikai és információvédelmi rendszert.
- A Hvt. vhr 15.§ (1), bekezdése alapján a Honvédség Műveleti Vezetési Rendszere speciális működési feltételeit akkor kell biztosítani, ha a döntéshozatal feltételei, az irányítási és vezetési rendszer működése béke időszaki rendben nem biztosítható, vagy a béke időszaki vezetési objektum veszélyeztetettsége olyan mértékű, hogy az irányítás és vezetés feltételei nem biztosíthatók (ilyen esetben a Honvédség stratégiai és műveleti szintű vezetési elemei a béke időszaki objektumtól eltérő helyen működnek, ahol szintúgy biztosítani kell az irányítás és vezetés biztonsági feltételeit).
- A Hvt. vhr 15.§ (2), bekezdése alapján a Honvédség Műveleti Vezetési Rendszere speciális működésének infokommunikációs támogatását a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának rendszerei, továbbá bérelt rendszerek biztosítják.
- A jogszabályban meghatározottakra figyelemmel az MH KCEHH alaprendeltetése, hogy magas rendelkezésre állással biztosítsa az MH alaprendeltetéséből adódó honvédelemi feladatainak végrehajtása érdekében a Honvédség vezetésének és irányításának, ezen belül az MH Műveleti Vezetési Rendszerének infokommunikációs támogatását béke, és különleges jogrend időszakában egyaránt.

Az MH KCEHH stratégiai irányítása három szinten, az alábbiak szerint érvényesül:

- Honvédelmi Miniszter: a Hvt. vhr 2.§ (2) 17. pontja alapján a Honvédelmi Miniszter felelős az MH KCEHH fejlesztéséért, működtetéséért, megállapítja a Honvédség feladatainak teljesítése szempontjából fontos híradó, informatikai és információvédelmi szolgáltatások működőképességének biztosítása érdekében szükséges együttműködési feladatokat;
- Honvéd Vezérkar Főnök (HVKF):
  - A Hvt. vhr 11.§ (1) 2. 3. pontja értelmében a HVKF felelős az ország fegyveres védelmi tervének, a Honvédség különleges jogrend bevezetéséhez kapcsolódó feladatrendszerének, továbbá a készenlét fenntartása és fokozása rendjének előkészítéséért, végrehajtásáért és annak ellenőrzéséért, valamint az ország területének légvédelmi készenléti erőkkel való oltalmazásáért.
  - A Hvt. vhr 11.§ (1) 6. pontja értelmében irányítja a híradó, informatikai és információvédelmi stratégia és szolgáltatási rendszer kialakítását, az MH KCEHH, valamint a MH VIR tervezését, fejlesztését, a szolgáltatások folyamatos biztosítását, üzemeltetését és fenntartását.
  - A Hvt. vhr 11.§ (1) 7. pontja értelmében felelős a Honvédség Műveleti Vezetési Rendszere működtetéséért, működési feltételei biztosításával kapcsolatos feladatok végrehajtásáért, az ehhez szükséges infrastruktúra és infokommunikációs rendszer üzemeltetéséért.
  - A Hvt. vhr 11.§ (1) 8. pontja alapján közreműködik a Honvédség feladatainak teljesítése szempontjából fontos közlekedési hálózat, a híradó, az informatikai és az információvédelmi szolgáltatások, a légi, sugárfigyelő, jelző- és riasztási rendszerek, valamint az energetikai hálózatok elemei közül a létfontosságú rendszerek és létesítmények védelmében.

- HVK Híradó, Informatikai és Információvédelmi Csoportfőnök: a HM SZMSZ alapján a honvédelmi minisztertől átruházott jogkörben ellátja az MH KCEHH hálózatgazdai feladatait.

A Digitális Jólét Programhoz kapcsolható katonai szempontok

A DJP-hez kapcsolódó fejlesztések országos kiterjedésűek és relatíve nagy léptékűek, ezért nemzetbiztonsági és gazdaságossági szempontból egyaránt indokolt a fejlesztés alatt álló digitális infrastruktúrák megnyitása és elérhetővé tétele a honvédelmi és katonai rendszerek irányába. Ez irányú pozitív vezetői döntés esetén létre kell hozni a DJP védelmi, katonai és nemzetbiztonsági szegmensét, blokkját. Ezzel már a fejlesztések tervezésénél és megvalósításánál is érvényesítésre kerülhetnének az MH távközlő hálózatokkal és infokommunikációs rendszerekkel kapcsolatos követelményei is. A közcélú és kormányzati vezetékes és vezeték nélküli hálózatokat magába foglaló digitális infrastruktúrával kapcsolatos katonai követelményeket az alábbiak mentén javasolt meghatározni:

- biztosítson magas rendelkezésre állást, illetve ennek érdekében robosztus, szövevényes, redundáns kialakítású legyen;
- biztosítsa az adatok bizalmasságát, sértetlenségét és időbeni továbbítását;
- biztosítsa a meghibásodások, a hálózatokban keletkezett incidensek, biztonsági események azonnali észlelését, illetve az azokra történő gyors reagálás lehetőségét az azonnali intézkedések megtétele, a meghibásodások behatárolása, elhárítása, a biztonsági események bekövetkezése esetén a keletkezett károk minimalizálása és a szükséges ellenintézkedések megtétele érdekében;
- biztosítsa a hálózatok, rendszerek, szolgáltatások és alkalmazások MH általi használatát;
- biztosítsa az MH részére a hálózatokhoz történő csatlakozást valamennyi hozzáférési ponton, illetve – külön egyeztetések alapján – hozzáférési pontok kerüljenek kiépítésre az MH által meghatározott helyszíneken;
- a vezetékes, főként optikai átviteli utak kerüljenek végződtetésre valamennyi használatban lévő HM-vagyonkezelésű létesítményben (vezetési objektumok, laktanyák, lő- és gyakorlóterek stb.);
- optikai kábeles átviteli utak kerüljenek kiépítésre valamennyi járási székhelyre;
- a vezeték nélküli hálózatok (közcélú mobil, EDR) országos lefedettséget, illetve a beszédkommunikáció mellett minél nagyobb átviteli sebességű adatforgalmat biztosítsanak;
- kapjon támogatást a katonai célra is alkalmazható, legalább Európát lefedő magyar (esetleg V4) távközlési műhold pályára állításának és üzemeltetésének projektje;
- a digitális infrastruktúráról – annak valós idejű változásait, meghibásodásait tükröző – központi adatbázis kerüljön létrehozásra, melyhez való online hozzáférés – főként különleges jogrend szerinti időszakban – az MH részére biztosított legyen;
- indokolt esetben, illetve különleges jogrend szerinti időszakban, legyen lehetőség a szolgáltatások igénybevételének MH általi priorizálására, a prioritásra jogosult felhasználói kör meghatározására, illetve adott esetben a nyilvános felhasználók forgalomból történő kizárására;

- a kormányzati és közcélú informatikai rendszerekben tárolt – műveleti, logisztikai és hadkiegészítési szempontból releváns – adatokhoz előre definiált jogok és felhasználási célok alapján legyen online hozzáférése az MH kijelölt szervezeteinek, pl. elektromos- és gázelosztó központok, víznyerő kutak, vegyi üzemek, logisztikai központok elhelyezkedése, hidak teherbírása, szélessége, a kórházakba beérkezett betegek, sérültek száma, kórházak, orvosi rendelők, polgármesteri hivatalok dolgozóinak lakcíme, a népesség-nyilvántartás hadkiegészítési szempontból fontos adatai, útlezárások, forgalmi akadályok, aktuális rendezvények stb.;
- az MH kijelölt szervezetei legyenek képesek a katasztrófavédelmi, a mentési, a határ- és rendvédelmi szervezetek informatikai szolgáltatásait igénybe venni, azokból aktuális információkat nyerni és oda adatokat küldeni.

Fenti követelményeket Magyarország nemzetközi kötelezettség-vállalásából adódó, illetve az ország védelmével kapcsolatos feladatai indokolják, mely feladatok végrehajtása érdekében elengedhetetlen a Műveleti Vezetési Rendszerhez, a katonai vezetési és irányítási, légi és egyéb fegyverirányítási rendszerek folyamatos és megbízható működéséhez szükséges digitális infrastruktúra fenti követelmények szerinti kialakítása és működtetése.

Magyar védelemi és hadiipari fejlesztések – *Zrínyi 2026*

Zrínyi 2026 néven az elmúlt huszonhat év legnagyobb honvédelmi és haderő-fejlesztési programját indította el 2017 januárjától a Magyar Honvédség. A 1298/2017. (VI. 2.) Korm. határozat a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról úgy fogalmaz, hogy a Kormány megtárgyalta a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Programot, és jóváhagyta annak fő irányait, és egyetért azzal, hogy a Programot – Magyarország biztonsági helyzetére és a Magyar Honvédség fejlesztési igényeire tekintettel – a Nemzetbiztonsági Kabinet 2017. február 1-jei ülésén meghatározott prioritási sorrendben kell megvalósítani. A Program részét képező feladatok végrehajtása érdekében felhívta a honvédelmi minisztert az egyes elemeinek megvalósításáról szóló további Kormány-előterjesztések összeállítására és a Kormány részére történő benyújtására.[26] A Kormány döntése értelmében a honvédelmi kiadások és a hosszú távú tervezés feltételeinek megteremtését szolgáló költségvetési források biztosításáról szóló 1273/2016. (VI. 7.) Korm. határozatban foglaltaknak megfelelően, a támogatási főösszeg GDP-arányának 0,1 százalékpontos növelésére vonatkozó előírás szerint, valamint egyéb többletek (közte haditechnikai eszközök felújítására 5.000,0 millió forint) miatt 72.048,7 millió forinttal növelésre került a 2017. évi eredeti támogatási főösszeghez képest.[27]

A komplex haderőfejlesztési terv részleteit magasan minősített dokumentumok képezik, jóllehet sajtóértesülésekből következtetni lehet rá, hogy lényege az erősen elavult Szovjetunió-gyártotta eszközök leváltása és korszerű, NATO-kompatibilis és -interoperábilis haditechnika beszerzése, valamint informatikai, digitális és hálózatalapú fejlesztések véghezvitele

26 1298/2017. (VI. 2.) Korm. határozat, a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról, Magyar Közlöny, Budapest, online: http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK17081.pdf (2017. december 29.)

27 http://www.parlament.hu/irom40/15381/adatok/fejezetek/13.pdf (2018. február 2.)

tíz éven belül. Ennek megfelelően átgondolt tervezésre és jól ütemezett, precíz kivitelezésre van szükség, hiszen ez esetben nem egyszeri többletforrásról és annak felhasználásáról van szó, hanem a fokozatosság elvén működő átfogó haditechnikai és hadiipari fejlesztési folyamatról. Összhangban nemzeti célkitűzéseinkkel és szövetségesi kötelezettségvállalásainkkal a *Zrínyi 2026* jelenleg körvonalazódó fő pillérei az alábbiak: szállítórepülőgép-, helikopter-, légvédelmirendszer-beszerzések; fegyverzet-, lőszer-, terepjárószállító-gépjármű-; valamint vezetési, irányítási, híradó-, informatikai és kibervédelmi rendszerfejlesztések.[28] Az előző, a *DJP katonai relevanciái*ról szóló fejezetben részletezett jogi, szakmai szabályzók és a stratégiai irányítási rendszerrel szemben támasztott további fontos követelmény, hogy szolgálja és biztosítsa a katonai high tech fegyverrendszerek és a hadiipar fejlesztését.

A katonai műszaki, haditechnikai, vezetési, irányítási, híradástechnikai és kommunikációs, felderítési rendszerek fejlesztései elképzelhetetlenek a ma rendelkezésre álló modern informatikai platformok igénybevétele, alkalmazása nélkül. Ezért a *Zrínyi 2026* haderőfejlesztési célkitűzései között szerepeltetni szükséges azt, hogy az MH már rövidtávon térjen át és zárkózzon fel a világ informatikai, digitális és hálózatalapú, ezen keresztül pedig a technológiai élvonalába a katonai rendszerek tekintetében. Mivel a küszöbön álló modernizáció védelempolitikai célrendszere és forrástámogatottsága is jelentősnek mondható, fontos, hogy e fejlesztések a súlypontok helyes meghatározásával, a források megtérülés-számításával valósuljanak meg úgy, hogy a honvédelem egészét új pályára, digitális platformra lehessen állítani. Ez csak úgy valósulhat meg, hogy a piacon rendelkezésre álló *high tech* rendszerekhez és a civil közigazgatás által használt infrastruktúrákhoz kacsolódnak a védelmi, katonai és nemzetbiztonsági rendszerek úgy, hogy szükség esetén bármikor leválaszthatók és önállóan is működtethetők legyenek, korlátozott mértékben átvéve a megtámadott, megsérült, vagy rongált kormányzati hálózatok funkcióit a kormány speciális működésének infokommunikációs támogatása érdekében.

28 Draveczki-Ury Ádám: Zrínyi 2026, Az átfogó fejlesztések időszaka következik, Magyar Honvéd 2017. január, Zrí-nyi Kiadó, Budapest, online: http://www.honvedelem.hu/cikk/61339 (2017. december 22.)

A DJP-hez és a DJP 2.0-hoz illeszthető potenciális katonai fejlesztési irányok

A fentiek tükrében az alábbi konkrét honvédelmi, katonai és haditechnikai fejlesztési irányok kitűzése indokolt a DJP és a DJP 2.0 keretében:

- digitális dominanciájú magyar részvétel a nemzetközi hadiipari munkamegosztásban;
- az 5G technológiára épülő katonai, műveleti, vezetési és irányítási, hírközlési, hadiipari és haditechnikai fejlesztések előnyben részesítése;
- precíziós fegyverek (kézifegyverek, önvezérlő fegyverrendszerek, bombák, rakétarendszerek) fejlesztése;
- intelligens katonai felszerelés-fejlesztés, egyéni és alegység-felszerelésrendszer (intelligens ruha), szenzorrendszer (egyéni és relatív helymeghatározás, valós idejű biofiziológiai állapotmérés, videokamera-rendszer, digitális audiokommunikáció, hőmérséklet-, páratartalom-, vegyi- és sugárzóanyag-mérés stb.);
- önvezérlő katonai járművek (tehergépjárművek, páncélozott járművek, páncélozott szállítójárművek, harcjárművek, repülőgépek [szállító, felderítő, zavaró], helikopterek);
- digitális alapú katonai térkép és fóliarendszer, valamint navigációs rendszer létrehozása;
- a magyar űrprogram nagyarányú digitális és hálózatalapú fejlesztése, magyar műhold fejlesztése és pályára állítása;
- komplex digitális és hálózatalapú vezetési, irányítási, katonai hírközlő és kommunikációs rendszer fejlesztése;
- a honvédelem rendszerében szolgálatot teljesítő katonák és polgári foglalkoztatottak átfogó felkészítése digitális kompetenciákkal (tanfolyamok);
- a katonai képzési, kiképzési rendszer kiegészítése digitális és hálózatalapú képességekkel;
- a védelmi igazgatási, katonai igazgatási rendszer kiegészítése digitális képességekkel;
- a hadkiegészítési, személyi nyilvántartási rendszerek kiegészítése valós idejű digitális és hálózatalapú platformmal;
- a katonai logisztika és hadtáp (fegyver, lőszer, hadianyag, felszerelés, ruházat, üzemanyag stb.) nyilvántartási rendszerének átállítása valós idejű digitális és hálózatalapú platformra;
- a Honvédelmi Minisztérium irányítása alatt működő cégek, hadiipari vállalkozások komplett vállalatirányítási és fejlesztési rendszereinek átállása digitális és hálózatalapú platformra.

Következtetések

A politikai, közigazgatási, gazdasági, ipari, mezőgazdasági, oktatási, tudományos, egészségügyi, közlekedési, energetikai és más polgári rendszerek mellett a digitalizáció és informatika nagyban hat a védelmi, nemzetbiztonsági és katonai felépítményekre is. A DJP és a DJP 2.0 szempontjából ez azt jelenti, hogy a magyar honvédelmi, katonai és nemzetbiztonsági rendszereket az alábbi négy fő követelménynek kell megfeleltetni: (1) ágyazódjanak be a teljes magyar digitális és hálózatalapú rendszerbe; (2) – az ország szövetségesi és uniós tagságából adódóan – biztosítsák a hazai védelmi, katonai és hadipari rendszerek NATO- és EU-kapcsolódását, -interoperabilitását; (3) a békeidőben kialakított katonai informatikai, digitális és hálózatalapú rendszerek legyenek képesek bármilyen, a békeállapottól eltérő jogrendben önállóan is működni, korlátozásokkal biztosítani az ország vezetését, irányítását és a közigazgatás zavartalan működését. A DJP és a DJP 2.0 tervezése és végrehajtása szempontjából ez azt feltételezi, hogy a biztonsági, honvédelmi, katonai és nemzetbiztonsági megfontolások részét kell képezniük a DJP-nek, vagyis a DJP-ben ki kell alakítani a honvédelmi, katonai és nemzetbiztonsági szakágazatot, blokkot. A honvédelmi, katonai és nemzetbiztonsági szakágazat elemezné és értékelné a biztonsági kihívásokat, szaktudásával, képességeivel és eszközeivel támogatná és oltalmazná a Programot, valamint saját maguk informatikai, digitális és hálózatalapú képességfejlesztéseit is e komplex rendszer keretében végeznék, megnyitva a DJP más szegmensei előtt is az idekapcsolódás lehetőségét, ezáltal is megteremtve a hazai digitális és informatikai rendszerek, hálózatok egymással való kompatibilitását és interoperabilitását.

Irodalomjegyzék

1. 2012/2015. (XII. 29.) Korm. határozat az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (InternetKon) eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról, Netjogtár, online: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A15H2012.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (2017. szeptember 4.)
2. 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről, Netjogtár, online: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A17H1456.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (2017. szeptember 4.)
3. 1298/2017. (VI. 2.) Korm. határozat, a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról, Magyar Közlöny, Budapest, online: http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK17081.pdf (2017. december 28.), online: http://www.parlament.hu/irom40/15381/adatok/fejezetek/13.pdf (2018. december 22.)

4. Babos Tibor: Globális közös terek a NATO-ban, Nemzet és Biztonság, Stratégiai és Védelmi Kutató Központ, Budapest, 2011. április, On-line: http://www.nemzetesbiztonsag.hu/cikkek/babos_tibor-___globalis_kozos_terek____a_nato_ban.pdf
5. Tibor Babos, The Five Central Pillars of European Security, NATO Public Diplomacy Division, Brussels, Strategic and Defense Research Center, Budapest, NATO School, Oberammergau, 2008
6. Desmond Ball, China's Cyber Warfare Capabilities, online: https://indianstrategicknowledgeonline.com/web/china%20cyber.pdf (2017. augusztus 27.)
7. Draveczki-Ury Ádám: Zrínyi 2026, Az átfogó fejlesztések időszaka következik, Magyar Honvéd 2017. január, Zrínyi Kiadó, Budapest, online: http://www.honvedelem.hu/cikk/61339
8. Internet Live Stats, online: http://www.internetlivestats.com/internet-users/china/ (2018. január 27.)
9. History, Structure, NATO Cooperative Cyber Defence Centre of Excellence, online: http://www.ccdcoe.org./history.html (2018. január 19.)
10. Mikk Raud, China and Cyber: Attitudes, Strategies, Orgainaztion, NATO Cooperative Cyber Defence Centre of Excellence, online: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (2018. január 30.)
11. Szentgáli Gergely: A NATO kíbervédelmi politikájának fejlődése, Nemzet és biztonság, Budapest, online: http://uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf (2018. január 28.)

Beregi Alexandra Lilla

A Magyar Honvédség digitalizációja a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program tükrében

Rezümé

A tanulmány célja, hogy a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Programmal összhangban bemutassa azokat képességfejlesztéseket és beszerzéseket, ajánlásokat, amelyek hozzájárulnak a honvédelem digitalizációjához. Megállapítható, hogy a Zrínyi 2026 célkitűzéseinek megvalósulása, valamint a digitális platformok azonos súllyal és intenzitással való kezelése esetén a honvédelem egésze digitális platformra állítható, amely azt eredményezné, hogy a piaci *high-tech* rendszerek és a közigazgatás által használt infrastruktúrákhoz igénybe vett védelmi, katonai, nemzetbiztonsági rendszerek önállóan, leválasztva is működhetnének a Kormány infokommunikációs támogatása érdekében.

Resume

The aim of the study is to presentthe the developments, procurements and recommendations of the Zrínyi 2026 Defense and Effective's development Program to reach the digitalization of the Hungarian defense system. It is a fact that if we will be able to reach the aims of the Zrínyi 2026 and use the digital platforms in balance (10 is recommended in the publication) whole of the Defense system could stand in a digital platform. It could mean that the defense, army and security systems would work with the other governmental systems and even alone to support the infocommunication of the Hungarian Government.

Vezetői összefoglaló

A tanulmány célja, hogy a Zrínyi 2026 programmal összhangban bemutassa azokat képességfejlesztéseket és beszerzéseket, ajánlásokat amelyek hozzájárulnak a honvédelem digitalizációjához. A dolgozat tézise, hogy a honvédelmi, katonai és nemzetbiztonsági rendszerek hazai digitális hálózatba való beágyazódása szükséges annak érdekében, hogy a békeidőben megfelelően működő katonai informatikai, digitális és hálózatalapú rendszerek képesek legyenek önállóan működtetni a közigazgatást, fenntartani az ország vezetését a békétől eltérő különleges jogrendben is.

„Nincs elavultabb, mint a tegnapi modern."
Csukás István

Bevezetés

Napjaink legmeghatározóbb biztonságpolitikai kihívásai (1) a globalizáció; (2) a digitalizáció; (3) a globális felmelegedés (4) és a nyersanyagforrások kimerülése.[1] Az Európát érintő biztonságpolitikai trendek meghatározzák Magyarország biztonságpolitikai kihívásait, törekvéseit és céljait. A dolgozat a fenti trendek közül a digitalizációt, mint biztonságpolitikai kihívást mutatja be azért, mert a digitalizáció fokozottabban jelenik meg a mai modern világban és ezáltal hatással van Európa, valamint Magyarország biztonságára is.

A digitalizáció fejlődésével a kibertérben elkövetett támadások számának és a cselekmények minőségének, sikerességének növekedésével kell számolnunk. Az emberiség technológiai szintje rohamos fejlődésének következményeként új kihívások jelennek meg, amelyek meghatározzák hazánk biztonságát.

A digitalizáció következtében minden elérhetőbbé válik a társadalom tagjai részére. A kibertérben elkövetett kibertámadások sok esetben visszafordíthatatlan politikai vagy gazdasági károkat eredményeznek. Magyarországnak rendelkeznie kell azzal a képességgel, hogy a kibertérbeli fenyegetéseket felismerje és kezelje, a kiberbiztonságot kiépítse, a kritikus információs infrastruktúra zavartalan működését biztosítsa, a támadásokat elhárítsa és a kibervédelmi feladatokat megfelelően elvégezze. A digitalizáció térhódítása azonban nemcsak a virtuális térben zajlik, hanem befolyásolja az alábbi 4 műveleti teret is: (1) szárazföld; (2) tenger; (3) levegő; (4) világűr.

A szerző szerint annak érdekében, hogy valamennyi műveleti területen országunk a digitalizáció következtében kialakult új biztonsági kihívások ismeretével és ezek leküzdéséhez szükséges képességekkel rendelkezzen, a honvédségnek új szemléletű, digitális platformra szükséges átállnia.

A digitális robbanás időszakában az új biztonsági kihívásokkal való sikeres fellépés érdekében elengedhetetlen a hadsereg modernizációja, amelyet a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program (a továbbiakban: Zrínyi 2026) keretében a Honvédelmi Minisztérium (a továbbiakban: HM) a Magyar Honvédséggel (a továbbiakban: MH) karöltve 2017-ben kezdett el megvalósítani.[2]

A Zrínyi 2026 célkitűzési között szerepel az MH áttérése és felzárkózása az informatikai, digitális és hálózatalapú katonai rendszerekhez. A fejlesztések megvalósulásának következtében a honvédelem egésze digitális platformra lenne állítható, amely azt eredményezné, hogy a piaci high-tech rendszerek és a közigazgatás által használt infrastruktúrákhoz igénybe vett védelmi, katonai, nemzetbiztonsági rendszerek önállóan, leválasztva is működhetnének a Kormány infokommunikációs támogatása érdekében.[3]

A dolgozat tézise, hogy a honvédelmi, katonai és nemzetbiztonsági rendszerek hazai digitális hálózatba való beágyazódása szükséges annak érdekében, hogy a békeidőben megfelelően működő katonai informatikai, digitális és hálózatalapú rendszerek képesek legyenek önállóan

1 Babos Tibor: A biztonság globális és európai összefüggései. Hadtudomány, Budapest, 2019/4. Online: http://real.mtak.hu/105840/1/016-029_Babos.pdf (Letöltve:2020. 02. 12.).

2 A Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról szóló 1298/2017. (VI. 2.) Korm. határozat.

3 Babos Tibor: A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái. Hadtudomány, Budapest, 2018. Online: http://real.mtak.hu/82604/1/2018ebabos2.pdf (Letöltve:2020. 01. 26.).

működtetni a közigazgatást, fenntartani az ország vezetését a békétől eltérő különleges jogrendben is.[4]

A Zrínyi 2026 fejlesztési és modernizációs törekvéseinek összehangolása elengedhetetlen az MH teljes körű digitalizációjával. A tézis igazolása érdekében a dolgozat első fejezete bemutatja azokat a haderőfejlesztési és digitális platformokat, amelyek mentén a Zrínyi 2026 hosszútávon lefekteti az MH digitalizációja és modernizációja érdekében tett cél- és eszközrendszerét, majd a második fejezetben, a teljesség igénye nélkül nemzetközi példák bemutatásával ajánlásokat fogalmaz meg a honvédség teljes körű digitális platformra helyezése érdekében.

A Zrínyi 2026 a digitalizáció jegyében

A Zrínyi 2026 bemutatása és célrendszere

A honvédség digitalizációjához elengedhetetlen az elavult képességek és technikák fejlesztése. Az MH szárazföldi és légierős eszközei, képességei modernizációra szorulnak. A fentiek érdekében a Zrínyi 2026 meghatározza azokat a modernizációs, honvédelmi és haderőfejlesztési képességeket és tevékenységeket, amelyek hozzájárulnak a honvédség teljes körű digitalizációjához.

A dolgozat első fejezete a következő kérdésekre keresi a választ:

- Melyek azok a platformok, amelyek mentén a Zrínyi 2026 meghatározza a modernizációs, honvédelmi és haderőfejlesztési tevékenységeit? Mik a célok?
- Mely beszerzések és képességfejlesztések valósultak meg a légierő és a szárazföldi erők modernizálása érdekében? Mik a további célok?

2017 januárjában vette kezdetét a Zrínyi 2026 haderőfejlesztési és modernizációs program,[5] amelynek célja, hogy biztosítsa a honvédség számára a mai kornak és kihívásoknak megfelelő technikai eszközöket, képességeket és személyi feltételeket. Egy hadseregnek folyamatos felkészülésre, képességekre és fejlett technikai eszközökre van szüksége ahhoz, hogy eredményesen helytálljon honvédelmi feladatainak végrehajtásában, megvédje a hazát – a szövetségesi együttműködés mellett – a nemzeti önerő képességének fenntartásával és fejlesztésével oly módon, hogy az állampolgárok hazafiasságra való nevelése, a haza védelmében való részvétele is megvalósuljon.

A Zrínyi 2026 az elmúlt 25 év legnagyobb és legátfogóbb haderőfejlesztési programja. A program részét képezi (1) a növekvő költségvetés az MH átfogó fejlesztése és modernizációja érdekében (2) a biztos életpálya a kiszámíthatóság, tervezhetőség és biztonság megteremtése érdekében (3) a honvédelmi program a biztos utánpótlásért az Önkéntes Területvédelmi Tartalék, az Önkéntes Honvédelmi Előképzés és a Honvédelmi Sportszövetség létrehozásával (4) az Önkéntes Tartalékos Rendszer kiépítése a sorkatonai szolgálat és az általános hadkötelezettség hiánypótlásaként (5) a katonacsaládok pénzbeli és természetbeni támogatása (6) a honvédelmi táborok országos szintű kiépítése a honvédség feladatainak ismerete céljából

4 uo.

5 A Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról szóló 1298/2017. (VI. 2.) Korm. határozat.

(7) a honvédelmi ösztöndíjprogram a középfokú és felsőoktatásban résztvevők számára (8) a fiatalok a honvédségért, honvédelmi nevelési program népszerűsítése a Honvéd Kadét Program keretében (9) a korszerű kiképzés az MH képességeinek megőrzése és fejlesztése okán a személyi állomány továbbképzésével, a korszerű haditechnikai eszközök alkalmazhatósága érdekében (10) az I. és II. világháborús hősök előtti tisztelgés a Katonahősök Emlékezete Program és a Magyar Katona Áldozatvállalása a Nagy Háborúban Program keretein belül (11) haderőfejlesztés a digitalizáció útján.[6]

A Zrínyi 2026 több pilléren nyugszik, ezek közül a leghangsúlyosabb a haderőfejlesztés, a hadsereg modernizációja, a képességek korszerűsítése, fejlesztése és digitalizációja. A fejlesztési és modernizációs program egyaránt átfogja a szárazföldi haderőnem és a légierő területét. A program keretein belül azonban modernizáción megy keresztül a logisztikai, a katonai-egészségügyi és a vezetési rendszer egésze is.[7]

A haderőfejlesztés célja a katonák egyéni harcászati felszerelésének megújítása, a helikopterflotta, a tüzér- és páncéltörőtüzér- képességek modernizálása, a honvédség merev és forgószárnyas légiszállítóképességének korszerűsítése, a radarok modernizálása, a légvédelmi rakétaegységek megújítása, a honvédség híradó-informatikai és tábori vezetési rendszerének modernizációja, valamint a különleges műveleti képességek továbbfejlesztése és a hibrid hadviselésen belül a kibervédelem fejlesztése korunk új biztonsági kockázatainak eredményes leküzdése érdekében. A komplex haderőfejlesztés a missziós feladatok és a katonai műveletek végrehajtását, valamint a katasztrófavédelmi helyzetek szakszerű kezelését, esetlegesen a polgári segítségnyújtást szolgálják.[8]

Az MH törekvése, hogy a NATO ajánlásaival összhangban 2024-ig a védelmi költségvetés legalább 20%-át fejlesztésekre és modernizálásra fordítsa. A Zrínyi 2026 kapcsán már megkezdődött a katonák egyéni felszerelésének és ruházatának megújítása. Továbbá RÁBA H sorozatú, különféle kialakítású terepjáró tehergépjárműveket, személygépkocsikat és speciális gépjárműveket is beszerzett a honvédség. A Mi-17-es szállító és a Mi-24-es harci helikopterek nagy javításokon estek át, lezajlott a Jak-52-es kiképző repülőgépek új Zlin típusú gyakorló és felderítő gépekre történő lecserélése, továbbá 16 db Airbus H145M helikopter beszerzése is már megvalósult. Az Airbus H145M helikopterek 2021-re légi mentési feladatok ellátásának is megfelelnek. A védelmi ipar fejlesztésének keretében 100 moduláris, modern autóbusz gyártása is megtörtént.[9] Továbbá megvalósult a vállról indítható páncéltörő képesség fejlesztése és a tüzéroptikai eszközök, valamint a Leopard 2A4 harckocsik beszerzése is. Utóbbiak nem új harckocsik, hanem korszerűsített és felújított eszközök, amelyek használata során felkészülhetnek a katonák a 2023 és 2025 között beszerzésre kerülő új Leopard 2A7-es nyugati csúcstechnológia alkalmazására. Beszerzés alatt állnak az önjáró lövegek, a légvédelmi rakétarendszer, a légvédelmi rakéták és tervben van a Gripen szoftverek megújítása is.[10]

---

6 Zrínyi 2026 honvédelmi és haderőfejlesztési program, A haza védelmében. Honvedelem.hu, Budapest. Online: https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf (Letöltve:2020.01.24.).

7 A haza védelme, a nemzet szolgálata. Honvedelem.hu, Budapest, 2019. Online: https://honvedelem.hu/files/files/116159/honvedseg_kiadvany_165x235mm_v2_6_.pdf (Letöltve:2020.02.14.).

8 uo.

9 Draveczki-Ury Ádám: Zrínyi 2026. Honvedelem.hu, Budapest, 2017.01.16. Online: https://honvedelem.hu/cikk/zrinyi-2026/ (Letöltve:2020.01.27.).

10 A járványról és a haderőfejlesztésről is beszélt a honvédelmi miniszter. Honvedelem.hu; Budapest, 2020. 12.05. Online:https://honvedelem.hu/hirek/a-jarvanyrol-es-a-haderofejlesztesrol-is-beszelt-a-honvedelmi-miniszter.html (Letöltve: 2021.02.27.).

Az MH kecskeméti légibázisán a Zrínyi 2026 keretében a felújítások részét képezi a kifutópálya, a fénytechnikai eszközök, az üzemi területek és az infrastruktúra fejlesztése is. A harckocsi- és önjárótüzér-, valamint helikopterképesség megteremtéséhez szükséges Tatán és Szolnokon az infrastrukturális fejlesztések megkezdése, továbbá az érintett laktanyák, mint Hódmezővásárhely esetében az épületek korszerűsítése.[11]

A 2 db Airbus A319 csapatszállító repülőgép vonatkozásában a MEDEVAC-képesség alkalmazhatóságának feltételei, valamint az A319-esek és a 2 db Dassault Falcon 7X futárgép kapcsán az önvédelmi képességek kerültek kialakítására. Ezekkel a képességekkel olyan logisztikai műveletek is végrehajthatók, mint a személy- és utánpótlás-szállítás, amelyek sikeres elsajátítása érdekében Bren 2-es típusú gépkarabélyokkal felfegyverzett különleges műveletei erők kiképzése is megtörtént.[12]

A légierő képességének modernizálása

A légierő képességeink megújítása, a légi szállítás mint katonai képesség megtartása stratégiai fontosságú az MH számára. A katonák felkészítése, kiképzése a műveleti és missziós feladatokra, a külszolgálathoz szükséges felszerelés és eszközök szállítása, utánpótlása és a humanitárius, katasztrófaelhárítási tevékenységben való részvétel a gépek megújításával, modernizálásával és új típusú digitális műszerekkel felszerelt helikopterek beszerzésével érhető el. A légiszállító képesség súlyos baleset, természeti katasztrófa, terrortámadás, vagy fegyveres konfliktus következtében, illetve tömeges baleset esetén szállításra is bevethető képesség.

A légierő képességének modernizálása érdekében elsőkörben 2019 novemberében érkeztek meg Szolnokra a Zrínyi 2026 keretében beszerzett Airbus H145M könnyűhelikopterek. Az MH a helikopterekhez logisztikai programot is biztosít, amely által a pilóták kiképzése már megtörtént, és az új gépek ellátása is biztosított. A helikopterek fegyverzete tartalmazza a 20 milliméteres gépágyút, és a nem irányított rakétákat, de lézeres irányítású páncéltörő rakétákkal is felszerelhetők.[13] 2020 júniusában további 3 db Airbus H145M típusú helikopter érkezett meg az MH 86. Szolnok Helikopter Bázisra. Az újonnan beszerzett helikopterek közül kettő már rendelkezik kutató-mentő felszereltséggel is.[14] 2020 decemberére összesen 16 db H145M Airbus érkezett meg Szolnokra.[15]

A honvédség előre tervezetten összesen 20 db Airbus H145M típusú helikopter beszerzését hajtja végre 2021-ig. A korszerű, modern felszereléssel, digitalizált műszerekkel és digitális, hálózati alapú fegyverekkel felszerelhető helikopterek használatát a szolnoki helikopterbázison tudják elsajátítani a magyar katonák. A nagy teljesítményű kamerával és elektronikus védelmi rendszerrel ellátott könnyű, többcélú helikopterek egyben rendelkeznek a kiképzőhelikopter,

11 Zrínyi 2026 honvédelmi és haderőfejlesztési program, A haza védelmében. Honvedelem.hu, Budapest. Online:https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf (Letöltve:2020. 01. 24.).

12 Irán támadást intézett két amerikai bázis ellen Irakban. Hirtv.hu, Budapest, 2020.01.08. Online: https://hirtv.hu/hirtvkulfold/iran-ballisztikus-raketakkal-tamadott-meg-amerikai-celpontokat-irakban-2492968 (Letöltve:2020. 01. 31.).

13 Már a szolnoki bázison vannak a honvédség első új helikopterei. Honvedelem.hu, Budapest, 2019.11.19. Online: https://honvedelem.hu/cikk/mar-a-szolnoki-bazison-vannak-a-honvedseg-elso-uj-helikopterei/ (Letöltve: 2020. 01. 25.).

14 Tovább gyarapodó légi képesség. Honvedelem.hu, Budapest, 2020. 06. 22. Online: https://honvedelem.hu/media/aktualis-videok/tovabb-gyarapodo-legi-kepesseg.html (Letöltve: 2021. 02. 27.).

15 Újabb helikopterek érkeztek. Honvedelem.hu, Budapest, 2020. 12. 10. Online: https://honvedelem.hu/hirek/ujabb-helikopterek-erkeztek.html (Letöltve: 2021. 02. 27.).

a kutató-mentő helikopter és a fegyveres-tűztámogató helikopter valamennyi tulajdonságával.[16] A H145M típusú gépeken túl további 16 db Airbus H225M közepes katonai helikopter beszerzése van folyamatban. A francia gyártású gépek 2023-2024-ben szintén a Zrínyi 2026 keretében érkeznek meg Magyarországra.[17]

A légierő képességének fejlesztése érdekében a Zrínyi 2026 által sugárhajtású kiképző repülőgépek kerülnek beszerzésre, amely beszerzés hozzájárul a pilótaképzés fejlesztéséhez. Ezenkívül a Gripenek fegyverzeti rendszerének modernizálása, MISTRAL M2 kis hatótávolságú rakéták fejlesztése és további kis-közepes hatótávolságú rakétakomplexumok beszerzése is tervben van. Az ország légterének ellenőrzése céljából az állandó telepítésű radarok légtérellenőrzési funkciójának kiegészítésére réskitöltő és mobil háromdimenziós radarállomások beszerzése, valamint a katonai repülőterek korszerűsítése is várható a programon belül.[18]

Az új Airbus H145M és H225M típusú helikopterek, valamint a sugárhajtású kiképző repülőgépek beszerzésével, továbbá a Gripenek modernizálásával és a MISTRAL M2 rakéták fejlesztésével új dimenzióba került a honvédség légierő-képességének modernizálása és ezen keresztül megnyílt az út a légierő-képességek digitalizációja előtt. A fejezetben bemutatott eredmények és megfogalmazott célok mind egy-egy lépéssel közelebb hozzák a honvédség teljes körű digitális platformra történő átállítását.

A szárazföldi erők modernizálása

A honvédségnek rendelkeznie kell azzal az elrettentő erővel és azokkal a katonai képességekkel, amelyek birtokában képes hatékonyan fellépni a biztonságot fenyegető veszélyekkel szemben. Ehhez szükséges a légierő fejlesztése mellett a honvédség szárazföldi erőinek modernizálása is, ezért a Zrínyi 2026 keretében sor kerül az MH szárazföldi képességeinek fejlesztésére és digitalizációjára is.

A katonák egyéni harcászati felszerelésének modernizálása – új, korszerű, a hazai gyártású eszközöket előnyben részesítve – már kezdetét vette. Az egyéni harcászati felszerelés békeidőben a napi munkavégzéshez és a kiképzési feladatok végrehajtásához szükséges eszközöket tartalmazza, háborúban pedig a feladatellátás biztosítása mellett növeli a katonák túlélőképességét. A haderőfejlesztési programon belül elindult a Digitális Katona Program, amelynek célja a katonák felszerelésének teljes körű digitalizációja.[19]

A szárazföldi erők modernizálása érdekében strukturális átalakításokat is megvalósítanak. Ennek keretében kerül sor a háromdandáros fejlesztésre, amely a nehéz, közepes és könnyű lövészdandár-szervezet létrehozását jelenti. A háromdandáros fejlesztés elemei összhangban állnak majd a szövetségesi elvárásokkal is, ezáltal a NATO követelményrendszere mellett az országvédelmi feladatok is megvalósulhatnak. A dandárok modern felszerelésének és

16 Révész Béla: Csúcstechnika a levegőben. Honvedelem.hu, Budapest, 2019.11.18. Online: https://honvedelem.hu/galeriak/csucstechnika-a-levegoben/ (Letöltve:2020. 01. 25.).

17 Baranyai Gábor: Megérkeztek a honvédség új helikopterei a német gyárból. Magyarnemzet.hu, 2019. 11.19. Online: https://magyarnemzet.hu/belfold/megerkeztek-a-honvedseg-uj-helikopterei-a-nemet-gyarbol-7505657/ (Letöltve: 2020. 01. 25.).

18 Zrínyi 2026 honvédelmi és haderőfejlesztési program, A haza védelmében. Honvedelem.hu, Budapest. Online:https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf (Letöltve:2020. 01. 24.).

19 Katonás Infotér. Honvedelem.hu, Budapest, 2019.10.16. Online: https://honvedelem.hu/hirek/hazai-hirek/katonas-infoter.html (Letöltve:2020. 01. 27.).

fegyverzetének beszerzése szintén a Zrínyi 2026 által lesz biztosítva. A koncepció megvalósításával párhuzamosan kerül kialakításra a dandárok korszerű katonai vezetési, irányítási és kommunikációs rendszerének telepítése, amely lehetővé teszi az információk és a vezetés új platformra helyezését.[20]

A tüzér- és páncéltörőtüzér-képesség fejlesztése és modernizálása érdekében új eszközök, valamint a hordozóplatformok és kiegészítő eszközök beszerzése és a honvédség műszaki csapatainak felzárkóztatása, a műszaki eszközök korszerűsítése, a közepes lánctalpas úszó gépjárművek és a hadihidak modernizálása szintén a hazai védelmi ipar bevonásával jön létre.

A világot és egyben Európát érintő új biztonsági kihívások közül a digitalizációs és hálózati rendszerek szempontjából kiemelt figyelmet szükséges fordítani a kibertámadásokra és a kibervédelemre. A hibrid hadviselés elleni küzdelemmel szemben a honvédség egy olyan kibervédelmi rendszer létrehozását tervezi, amely ellenáll a vezetési és irányítási rendszerekbe történő külső fél behatolásainak és képes felfedni a hálózat elleni támadásra utaló tevékenységet. A kibertérben jelentkező fenyegetések elhárításához naprakész oktatásra van szükség a katonák számára, ennek érdekében 2019 júniusában került átadásra Szentendrén a Magyar Honvédség Kiber Képzési Központja.[21]

Az új és modernizált eszközök szakszerű elhelyezéséhez elengedhetetlen a korszerű logisztikai, elhelyezési és tárolási rendszer, amely a laktanyarekonstrukciós program keretében valósul meg. A haderőfejlesztési program tervei között szerepel továbbá egy olyan tábori kórház felállítása, és az ehhez szükséges eszközök beszerzése, amely a harctéren az életmentésen túl sebészeti beavatkozásokra és diagnosztikai vizsgálatokra is alkalmas.[22]

A szárazföldi erők modernizálása érdekében 2020 decemberére megérkezett Tatára a 12 db Leopard 2A4 lízingelt harckocsi[23], amelyet további 44 db Leopard 2A7+ nehéz harckocsi, 24 db PzH 2000 önjáró löveg, és EJDER Yalcin típusú, „Multipurpose" Páncélozott Többcélú Moduláris Harcjárművek beszerzése követ.[24]

A hazai kézifegyverek további gyártása, a katonák egyéni harcászati felszerelésének fejlesztése, a kiberképesség fejlesztésének folytatása és az új eszközök fogadásához szükséges infrastrukturális feltételek megteremtése tervezett.

A Zrínyi 2026 tehát mind a légierő mind a szárazföldi erők modernizálása által hozzájárul ahhoz, hogy a honvédség rövid, majd hosszútávon áttérjen az informatikai, digitális és hálózatalapú katonai rendszerek teljes körű alkalmazására. Mindez alátámasztja a tézist, amely alapján a fejlesztések megvalósulásának következtében a honvédelem egésze digitális platformra állítható át, ezzel biztosítva azt, hogy a védelmi, katonai, nemzetbiztonsági rendszerek

20 Zrínyi 2026 honvédelmi és haderőfejlesztési program, A haza védelmében. Honvedelem.hu, Budapest. Online: https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf (Letöltve:2020. 01. 24.).

21 Átadták a Magyar Honvédség Kiber Képzési Központját. Kormany.hu, Budapest, 2019. 06. 13. Online https://2015-2019.kormany.hu/hu/honvedelmi-miniszterium/hirek/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat (Letöltve:2020. 02. 13.).

22 Zrínyi 2026 honvédelmi és haderőfejlesztési program, A haza védelmében. Honvedelem.hu, Budapest. Online: https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf (Letöltve:2020. 01. 24.).

23 Aki már huszonöt éve ismeri a „nagymacskákat". Honvedelem.hu, Budapest. Online: https://honvedelem.hu/hirek/aki-mar-huszonot-eve-ismeri-a-nagymacskakat.html (Letöltve: 2021. 02. 27.).

24 A haza védelme, a nemzet szolgálata. Honvedelem.hu, Budapest, 2019. Online: https://honvedelem.hu/files/files/116159/honvedseg_kiadvany_165x235mm_v2_6_.pdf (Letöltve:2020. 02. 14.).

önállóan, más rendszerektől leválasztva is képesek legyenek működtetni a közigazgatást, fenntartani az ország vezetését békeidőben és a békétől eltérő különleges jogrendben is.

A Magyar Honvédség digitalizációja

Napjainkban a korábbitól lényegesen eltérő, új hadviselés korának küszöbén állunk. Az új hadviseléshez az MH-nak is szükséges alkalmazkodnia a digitális transzformáció útján.

A következő fejezetben a szerző arra törekszik, hogy a tézis igazolása érdekében legtöbbször a nemzetközi példák bemutatásával megvizsgálja, elemezze és előrevetítse a honvédség teljes körű digitalizációját. Ennek érdekében a továbbiakban 10 ajánlás kerül bemutatásra.

A második fejezet arra keresi a választ, hogy milyen súllyal és intenzitással jelennek meg az alábbi platformok a honvédség digitalizációja érdekében:

1. A nemzetközi hadiiparban való magyar részvétel.
2. Az 5G technológia alkalmazása a katonai, műveleti, vezetési- és irányítási, hírközlési, hadiipari és haditechnikai fejlesztések terén.
3. Okos fegyverek fejlesztése, különös tekintettel a kézifegyverek, önvezérlő fegyverrendszerek, bombák, rakétarendszerek digitalizációjára.
4. Intelligens katonai felszerelés fejlesztése különös tekintettel az intelligens ruha és digitális szenzorrendszer kialakítására, digitális katonai térkép és navigációs rendszer fejlesztése.
5. Önvezérlő katonai járművek: tehergépjárművek, páncélozott járművek, páncélozott szállítójárművek, harcjárművek, repülőgépek, helikopterek modernizálása, digitális műszerekkel való felszerelése, mesterséges intelligencia a harctéren.
6. A katonák és civilek átfogó felkészítése digitális kompetenciákkal, képzések és tanfolyamok biztosítása a digitális eszközök ismeretének és szakszerű felhasználásának céljából.
7. A katonai kiképzési és oktatási rendszer, a védelmi igazgatási, a katonai igazgatási rendszer digitális- és hálózatalapú képességekkel való kiegészítése.
8. A személyi nyilvántartási rendszerek, a katonai logisztika és hadtáp nyilvántartási rendszer kiegészítése és átállítása digitális és hálózatalapú platformra.
9. A magyar űrprogram digitális fejlesztése, magyar műhold fejlesztése és pályára állítása.
10. A komplex hálózatalapú és digitalizált vezetési, irányítási, katonai hírközlő és kommunikációs rendszer fejlesztése.[25]

A nemzetközi hadiiparban való magyar részvétel

A hazai védelmi ipar fellendülése érdekében a HM, az Innovációs és Technológiai Minisztérium és a nemzeti védelmi ipari és védelmi célú fejlesztésekért, valamint a haderő-modernizáció koordinálásáért felelős kormánybiztos együttesen felel. Azonban a Kormány védelmi ipari fejlesztéseibe az ütemesebb és eredményesebb fejlődés érdekében a kis- és középvállalkozások, valamint a start up cégek bevonása is szükséges lehet. Kiemelt cél a hazai védelmi ipar

25 Babos Tibor: A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái. Hadtudomány, Budapest, 2018. 143-144. o. Online: http://real.mtak.hu/82604/1/2018ebabos2.pdf (Letöltve:2020. 01. 26.).

fejlesztése és a világ élvonalába tartozó befektetők Magyarországra vonzása, mint például az Airbus, amely a világ vezető repülés- és űrtechnikai vállalatának egyike. Az Airbus magyarországi tervei közt az alkatrészgyártáson túl a légi ipari klaszter létrehozása is szerepel.[26]

A Zrínyi 2026 keretein belül a HM és az MH megkezdte a haderő felfegyverzését 20 db Airbus H145M és további 16 db H225M helikopter beszerzésének kezdeményezésével, a német Krauss-Maffei Wegmann céggel kötött szerződés kapcsán 44 db Leopard 2 A7+ harckocsi, valamint 24 db PzH 2000 önjáró löveg beszerzése tervezett. A magyar fegyvergyártás fellendítése érdekében a P-07, P-09 típusú pisztolyok, a Bren 2 típusú gépkarabélyok és a Scorpion Evo 3 géppisztolyok előállítására tervezetten Kiskunfélegyházán kerül sor.[27]

Az 5G technológia

Az 5G mobilhálózatra való átállással egy technológiai korszakváltás veszi kezdetét a világban. Az 5G hálózat jóval gyorsabb lesz, mint a jelenlegi 4G mobilhálózat, ezzel lehetővé téve a gyorsabb adatátvitelt és a reakcióidők csökkentését. Az 5G-re való átállás hasznosítható lesz az autóiparban, a közlekedésben, a feldolgozóiparban, a mezőgazdaságban, az egészségügyben, az energiagazdálkodásban, a kereskedelemben, a szórakoztatóiparban és a médiában. Az 5G által minimálisra csökkentett reakcióidő és szinte valós idejű kommunikáció hozzájárul az intelligens közlekedés, az önvezető gépjárművek és az e-egészségügy létrehozásához és/vagy fejlődéséhez.[28]

Az 5G hálózat kiépítésében történő állami szerepvállalás kapcsán Magyarország vezető szerepet tölthetne be az európai fejlesztésekben, valamint a hálózat kiépítése is gyorsabban, a párhuzamosságokat elkerülve történne, a piaci szektorral karöltve. Az új hálózat kiépítését az Egyesült-Államok mellett Nagy-Britannia, Németország, Svájc, Kína, Dél-Korea és Ausztrália is szorgalmazza.[29]

A honvédség szempontjából a digitális műszerek 5G hálózathoz való csatlakozásával nemcsak a harctéren való alkalmazhatóságot, hanem a képzést és kiképzést is fejleszthetnénk. Az 5G technológiai alkalmazása a katonai, műveleti, vezetési- és irányítási, hírközlési, hadiipari és haditechnikai fejlesztések terén biztosítja a honvédség digitális platformra állítását.

Az okos fegyverek fejlesztése

Az okos fegyverek hadsereg számára történő fejlesztését és tömeges gyártását 2019-ben kezdte meg az Amerikai Egyesült Államok. Az elképzelés alapján a jövő kézi fegyverei külön operációs rendszerrel rendelkeznek. Az új technológiájú kézi fegyverek megváltoztatják a

26 Védelmi ipar ágazati koncepciója. Hmarzenal.hu, Budapest, 2018. Online: http://www.hmarzenal.hu/vedelmi-ipar/vedelmi-ipar-agazati-koncepcioja.pdf (Letöltve:2020. 02. 13.).

27 Bencze Áron: Digitális ugrásra készül a Magyar Honvédség. Innoteka.hu, Budapest, 2019. 05. 03. Online: https://www.innoteka.hu/cikk/digitalis_ugrasra_keszul_a_magyar_honvedseg.1909.html (Letöltve:2020. 01. 31.).

28 5GK-Magyarországi 5G Koalíció. Digitalisjoletprogram.hu, Budapest. Online: https://digitalisjoletprogram.hu/hu/tartalom/5gk-magyarorszagi-5g-koaliciohttps://digitalisjoletprogram.hu/hu/tartalom/5gk-magyarorszagi-5g-koalicio (Letöltve:2020. 02. 13.).

29 Blackman, Colin – Forge Simon: 5GDeployment. Europarl.europa.eu, Brussels, 2019. Online: https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/631060/IPOL_IDA(2019)631060_EN.pdf (Letöltve:2020. 02. 13.).

fegyverkezelés és -használat rendjét, és növelik a hadsereg hatékonyságát. Az intelligens fegyverek működését illetően az az elképzelés, hogy a fegyverekbe épített operációs rendszernek köszönhetően megakadályozható az illetéktelenek eszközhasználata, továbbá az alkalmazások segítségével pontosabb célzás valósítható meg. Mindez nem csak átalakítja, de meg is könnyíti a katonák jövőbeli kiképzését. A fegyverek operációs rendszerrel való felszerelésével és digitalizációjával azonban megnő a hackertámadások esélye, amely eshetőségre a kiberbiztonsági rendszer megerősítésével szükséges felkészülnie a kormányzatnak.[30]

Az Egyesült Államok a rakétavédelmi képességek fejlesztésének keretében vizsgálja az F-35 II JSF lopakodó vadászgép új alkalmazási opcióit. A fejlesztés célja, hogy az F-35 szenzorait, adatkapcsolati rendszereit kihasználva képessé váljon az interkontinentális ballisztikus rakétákat akár már az indítási fázisban detektálni vagy megsemmisíteni. A fejlesztésekben érdekelt Kína és Észak-Korea is.[31]

2020. január 8-án Irán 18 rövid hatótávolságú ballisztikus rakétát indított az Irakba települt amerikai erők bázisai ellen. Erbílben csaknem 200 magyar katona szolgál, akik azonban a rakétatámadás kapcsán nem szenvedtek sérülést. A támadásokat követően Irán nyilatkozata szerint minden Amerikával szövetségben álló országra ellenségként tekinthetnek és célpontul szolgálhatnak számukra.[32]

A fenyegetettség növekvő tendenciája miatt a védelmi rendszer képességeinek bővítése nem odázható tovább. Ennek következtében nemcsak az Egyesült Államoknak, hanem a Szövetség- és EU-tagállamoknak is, köztük hazánknak, szükséges a legmodernebb technológia védelmi képességeire koncentrálni.

A digitális katona

Az intelligens katonai felszerelés ötletével elsők között az Amerikai Egyesült Államok állt elő az 1990-es évek végén. A fejlesztések során a lézeralapú technikát, a beépített számítógépként működő digitális taktikai térképet és a saját és csapathelyzetet megjeleníteni képes sisakképernyős rendszert alakították ki. Kifejlesztették az elődjénél jóval könnyebb golyóálló kevlár sisakot, amelyre olyan speciális kijelző erősíthető, amelyen egy másik katona fegyverére szerelt kamera képe vagy akár az ellenség helyzete és a harctéren történő események is elérhetőek. A jövő tervei szerint a felcsatolható gázmaszkkal együtt légmentesen záródó sisak 3D-s kijelzőkkel és 3D-s audiórendszerrel kerülne kibővítésre, mely technológia segítségével az ellenség már messzebbről észlelhetővé válna a katona számára. Az amerikai hadseregben a katonák olyan védőmellényt kaptak (interceptor), amely egyaránt védi a felsőtestet, a combot és a felkart is. A jövőben a jelenleginél súlyban könnyebb és hatékonyabb védelmet biztosító páncélkialakítás a cél titánkompozit védőpanelek alkalmazásával, amely képes akár a közelről kilőtt géppuskalövedék megállítására is.[33]

30 Kiss Adorján: Okosfegyverekkel látnák el a hadsereget. Vg.hu. 2019.10.21. Online: https://www.vg.hu/gazdasag/gazdasagi-hirek/okosfegyverekkel-latnak-el-a-hadsereget-2-1821681/ (Letöltve:2020. 01. 31.).

31 Lockheed Martin - F-35 Lightning II. Aerotech.hu, Online: http://www.aerotech.hu/f-35.php (Letöltve: 2021. 02. 28.)

32 Rakétatámadások Irakban: Irán gyorsan megtorolta Szulejmáni likvidálását. Hvg.hu, Budapest, 2020.01.08. Online: https://hvg.hu/vilag/20200108_Iran_raketacsapast_mert_az_amerikaiak_egy_iraki_tamaszpontjara (Letöltve:2020. 02. 13.).

33 Cifka Miklós: A jövő gyalogos katonája: baka a digitális korszakban. Sg.hu, Budapest, 2005.03.29 Online: https://sg.hu/cikkek/tudomany/36233/a-jovo-gyalogos-katonaja-baka-a-digitalis-korszakban (Letöltve:2020. 02. 13.).

A katonai egyenruháknak alkalmazkodniuk kell a különböző éghajlati övekhez. A modern technológia miatt azonban az egyenruhák nagyvolumenű fejlesztése tapasztalható, egyre alkalmazkodóbbak és kényelmesebb, praktikusabb viseletet biztosítanak a katonáknak, ezáltal hozzájárulnak a harctéri teljesítmény növeléséhez. A jövőbeli elképzelés szerint az egyenruhák megfelelően szellőző, víztaszító, ellenálló anyagokból készülnek majd, a speciális éghajlati övekhez alkalmazkodva hűtő- és fűtőfunkcióval ellátva. A hűtőmellényekben egy olyan kristályos anyag van, amely vízzel érintkezve gél állagúvá válik, így biztosítja a hűtőfunkciót. Ezt a technikát már a 2000-es évek közepén az iraki övezetben harcoló katonáknál sikerrel alkalmazták.[34]

Az amerikai hadsereg ruházat- és felszerelésmintája többgenerációs fejlődésen ment keresztül. A terepszínű egyenruhákat felváltotta a digitalizált minta. Az új pixeles cadpat nevű álcázómintát először 1996-ban használta a kanadai hadsereg, majd ezt felváltotta az amerikai tengerészgyalogság 2001-ben használt marpat mintája és végül az amerikai hadsereg 2005-ben hadrendbe állította az acupat nevű pixeles mintát, amely mára a világ számos katonai hadseregénél elterjedt. Az amerikaiak kutatják annak a lehetőségét, hogy a digitalizált egyenruha hogyan tudná kaméleon módjára felvenni a háttér színeit, illetve az öltözék hogyan tudna teljesen azonosulni a mögötte lévő táj képével.[35]

Az Egyesült Államok a Land Warrior majd az Objective Force Warrior program keretein belül fejlesztette az intelligens katonai egyenruhát és a digitális katonai felszereléseket. A digitális hadviselés célja, hogy minden katona rendelkezzen olyan adóvevővel, amely képes hangot, adatot és képet is közvetíteni a harctéren lévő katona és a parancsnokság között. Az elképzelések alapján a rádiórendszer, a számítógép és az elektromos rendszerek kábelei a hámban és ruházatban kerülnének elhelyezésre, ezáltal biztosítva a katona zavartalan mozgását.[36]

A 21. században fontos, hogy a magyar katona is olyan elektronikai eszközökkel rendelkezzen, amely hangot, szöveges és képüzeneteket képes fogadni vagy küldeni egy védett alapú kommunikációs csatornán. Ezért a nemzetközi fejlesztésekkel összhangban a Zrínyi 2026 keretein belül Magyarország is elindította a Digitális Katona Programját, amelynek központjában a katona áll. A Program célja az új, korszerű harcászati felszerelés: ruházat, bakancs, repeszálló mellény, málhamellény, sisak, hátizsák és egyéni fegyverzet biztosítása a kiképzési idő tartamára és a terepen lévő katona számára.[37]

---

34 GÁCSER Zoltán: A katona harci képességét növelő korszerű, hálózatba integrált egyéni felszerelésrendszrének kialakítási lehetőségei a Magyar Honvédségben c. PhD értekezés. Budapest, 2008.
Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12102/ertekezes.pdf;jsessionid=E53B0E3B1B43A817529E3C72C25CEF01?sequence=1 (Letöltve: 2021. 02. 28.).

35 Key Issues Relevant to The U.S. Army's Transformation to the Objective Force, An AUSA Torchbearer Issue, Vol.II. USA, 2002.
Online: https://www.ausa.org/sites/default/files/TBNSR-2002-The-US-Armys-Transformation-to-the-Objective-Force-Vol2.pdf (Letöltve:2020. 02. 09.).

36 Land Warrior Integrated Soldier System. Army-technology.com, USA.
Online: https://www.army-technology.com/projects/land_warrior/ (Letöltve:2020. 02. 09.).

37 Katonás Infotér. Honvedelem.hu, Budapest, 2019. 10. 16.
Online: https://honvedelem.hu/hirek/hazai-hirek/katonas-infoter.html (Letöltve:2020. 01. 27.).

Mivel az amerikaiak által kifejlesztett digitalizált ruha hazai terepen nem rejt túl jól, a Digitális Katona Program első fázisában a régi sötétebb színű gyakorlókat leváltották a világosabb színű, infrasugarakat elnyelő gyakorlóruhák. A magyar katonák egyéni fegyverzete a kiskunfélegyházi fegyvergyárban készül, ahol pisztolyok, géppisztolyok és gépkarabélyok gyártására kerül sor. A Zrínyi 2026-on belül a hadiipar fejlesztésének részeként megvalósul a kézifegyverek lőszereinek és a lőpor hazai előállítása.[38]

Önvezérlő járművek, mesterséges intelligencia

Egyre inkább elterjedt a robotok harctéri alkalmazása a katonák munkájának megkönnyítése érdekében. Ez azt jelenti, hogy találkozhatunk kerekes, lánctalpas, vagy lábakkal ellátott miniatűr katonai robotokkal, de léteznek nagyobb robotok is, amelyek nagy teherbírásúak, ezáltal képesek több tonnányi katonai felszerelést szállítani. Ezenkívül a háborús hadszíntereken megtalálhatóak a levegőben felderítő vagy csapásmérő feladatot ellátó távolról vezérelt repülőgépek és improvizált robbantótest semlegesítő tűzszerész robotok is. Az aknamentesítő, robbanótest-hatástalanító robotokat és a fegyverekkel felszerelt távirányítású robotokat a jövőben olyan fejlesztéseknek vetik alá, hogy képesek legyenek az előre meghatározott terület járőrözésére, és az ellenség kiiktatására.[39]

Az új generációs harci robotok fejlesztése is megkezdődött, így lánctalpas, gumikerekes egyre nagyobb hatótávolságú, okosabb rendszerek is hadrendbe állhatnak. Az Egyesült Államok, Oroszország és Kína is foglalkozik a mesterséges intelligencia katonai fejlesztésével.[40]

A robotizálás nemcsak az újonnan kifejlesztett mesterséges intelligencia hasznosításával, hanem a már meglévő járművek, repülőgépek autonóm működésének átépítésével is elérhető. Az amerikai haditengerészet így alkalmazza az MQ-8C távolról irányított helikoptert, amely a Bell 407-es helikopter átalakított változata. Oroszországban a BMP-3 típusú gyalogsági harcjármű átépítéseként számítógépek kerültek a kezelők helyére. Az orosz Uran-6 típusú tűzszerész robot, a horvát MV-4 DOK-Ing továbbfejlesztése, amely nagyméretű lánctalpas aknamentesítő rendszer. Kínában 2014-ben mutatták be a Sharp Clawt, amely egy gumikerekes könnyű páncélozott terepjáró jármű segítségével önállóan tudja megközelíteni az ellenséges területet. A robotjárműnek saját felderítő- és fegyverrendszere van, az utóbbi használatához katona szükséges. A jármű egyszerre képes a levegőben és a földön is felderítést végezni tekintettel a kis hatótávolságú quadrocopterre.[41]

Annak ellenére, hogy hazánk kevéssé érdekelt a hajók, illetve a tengeralattjárók robotizálásának fejlesztésében, mégis érdemes megemlíteni, hogy az Egyesült Államok és Oroszország már elkezdte a tengeralattjáró vadászok és hadihajók tesztelését, az amerikai haditengerészet pedig a hajókon és tengeralattjárókon kialakuló tűz oltására alkalmas robotok fejlesztését.[42]

38 Draveczki-Ury Ádám: Digitális világ a haza szolgálatában. Honvedelem.hu, Budapest, 2019. 04. 30. Online: https://honvedelem.hu/media/aktualis-videok/digitalis-vilag-a-haza-szolgalataban.html (Letöltve:2020. 02. 09.).

39 Négyesi Imre: A mesterséges intelligencia és a hadsereg I. Hadtudományi Szemle, Budapest, 2017/2. Online: http://epa.oszk.hu/02400/02463/00035/pdf/EPA02463_hadtudomanyi_szemle_2017_2_023-034.pdf (Letöltve:2020. 02. 13.).

40 Robotok uralják a jövő harctereit? Honvedelem.hu, Budapest, 2010. 08. 05. Online: https://honvedelem.hu/hirek/robotok-uraljak-a-jovo-harctereit.html (Letöltve:2020. 02. 13.).

41 Trautmann Balázs: Fémharcosok. Honvedelem.hu, Budapest, 2016. 07. 24. Online: https://honvedelem.hu/hatter/haditechnika/femharcosok.html (Letöltve:2020. 02. 09.).

42 uo.

Nemzetközi minták alapján megállapítható tehát, hogy a mesterséges intelligencia katonai hasznosítása földön, vízen és levegőben egyaránt kiemelkedő szerepet játszik a harctéren. A Zrínyi 2026 kapcsán az előzőekben bemutatott új beszerzések és a már meglévő eszközök modernizálása az első lépés ahhoz, hogy az MH is kiépítse a mesterséges intelligencia hadszíntéren történő eredményes használatát.

Digitális képességek fejlesztése

A honvédség jelentős átalakulásokon megy keresztül, melynek keretében a legkorszerűbb eszközök kerülnek beszerzésre, mindez megteremti a kutatás, fejlesztés és az innováció alapjait. Információs hadviselés megy végbe a kibertérben és valamennyi hadszíntéren egyaránt bekövetkeznek a változások. A terrorszervezetekkel szemben a hagyományos haderő már nem képes hatékonyan fellépni, ezáltal megkezdődött a negyedik generációs hadviselés kora. Ennek tükrében a haderők legfontosabb kérdése a reagálóképesség növelése és a megoldások keresése a digitális transzformáció haderőben történő sikeres végrehajtása kapcsán.

A 21. századi siker kulcsa a központi vezetői szándék decentralizálása mellett a kor aktuális kihívásainak felismerése és kezelése. Mindezek érdekében a problémamegoldás, a kritikus gondolkodás, kreativitás, a hálózatépítés és a változó körülményekhez történő gyors alkalmazkodás mint emberi képességek fejlesztése szükséges. A hadviselés innovációját nemcsak az új technológia jelenti, hanem e technológiák készségszintű alkalmazása, gyors elsajátítása, újszerű hasznosítása a legújabb fegyverek és gépek terén. Mindezek hozzájárulnak ahhoz, hogy az ország egy rugalmasabb haderővel rendelkezzen és az új technológiák alkalmazásához egy megfelelő szervezeti struktúra kerüljön kiépítésre.[43]

A HM-ben és az MH-ban 2019-ben kezdődtek meg az intézményi átalakulások és ezzel együtt a szervezetfejlesztés. Létrejött a Magyar Honvédség Modernizációs Intézete és a Védelmi Kutatóintézet. A Minisztérium magyar felsőoktatási intézményekkel működik együtt számos kutatási projekt beindítása kapcsán. A Nemzeti Közszolgálati Egyetem képzései és továbbképzései biztosítják az új technológiák szakszerű használatának elsajátítását, és az új biztonsági kihívásokkal való eredményes szembeszállást úgy a mérnökképzések, mint a hibrid hadviselés kialakítása szempontjából jelentős kiberbiztonsági képzések tekintetében.[44]

A katonai kiképzési és oktatási rendszer

Az új technológiák, a modern fegyverek és a védelmi képességek fejlesztése nemcsak fizikai többletterhet jelentenek a katonák számára, hanem megkövetelik a kognitív képességek fejlesztését is. Az agyi képességek fejlesztése ugyanúgy kivitelezhető, mint a fizikai állóképesség kiépítése. A haderőfejlesztés és modernizáció kapcsán digitalizált eszközök, fegyverek,

43 Bencze Áron: Digitális ugrásra készül a Magyar Honvédség. Innoteka.hu, Budapest, 2019. 05. 03. Online: https://www.innoteka.hu/cikk/digitalis_ugrasra_keszul_a_magyar_honvedseg.1909.html (Letöltve:2020. 01. 31.).

44 Középpontban a katona. Kormany.hu, Budapest, 2019.05.01. Online: https://2015-2019.kormany.hu/hu/honvedelmi-miniszterium/hirek/kozeppontban-a-katona (Letöltve:2020. 02. 13.).

ruházat és felszerelés ugyanúgy algoritmusokon alapszanak, mint a civil életben használatos applikációk. Ezek alapja a deep learning, amely neuronhálózatok alkalmazását jelenti.[45]

Az Amerikai Egyesült Államokbeli Defense Advanced Research Projects Agency (DARPA) és a Platypus Institute a katonai teljesítmény neurotechnológiai fejlesztésével foglalkozik. Az intézetek a kognitív képességek fejlesztésének lehetőségeit veszik számba az agy alkalmazkodóképességének a dinamikusan fejlődő technológiai környezetben történő vizsgálatával.[46] A kutatás tárgya a katona egyéni kognitív képességeinek és a katonák csoportjának együttes műveleti tevékenység során történő vizsgálata. Ezenfelül vizsgálatok tárgyát képezi az ember és a robot együttműködése is. A kutatásokra azért van szükség, mert a digitális technológia rohamosabb mértékben fejlődik, mint ahogy azzal az emberi agy képes lenne lépést tartani, ezért szükséges az egyéni képességek kognitív fejlesztése. Az amerikai hadsereg különleges műveleti erő felkészítő programjában alkalmaznak továbbá egy szimulációs programot. Az online szimulációs rendszert a parancsnoki képzési programon belül a vezetői magatartás és módszerek oktatására használják.[47]

Hazánkban a Digitális Katona Programban kialakított VR-alapú szimulációs rendszer járul hozzá a katonák kognitív képességeinek fejlesztéséhez.[48]

A nyilvántartási rendszerek digitalizálása

Az Integrált Jogalkotási Rendszer (a továbbiakban: IJR) fejlesztése 2016-ban kezdődött meg a közigazgatás adminisztratív terheinek csökkentése, valamint a szolgáltató képességének növelése érdekében.[49] Az IJR célja a színvonalasabb jogalkotás, ennek érdekében a rendszeren belül minden jogszabállyal kapcsolatos tevékenység informatikailag támogatott, az első tervezet megszületésétől a Magyar Közlönyben történő kihirdetésig.

Az IJR több alrendszerből áll, ilyen az Elektronikus Jogszabály-előkészítő Rendszer (EJR), amely a jogszabálytervezet-szerkesztést és -szövegezést, azaz a kodifikációt támogatja. Az IJR további alrendszerei a GovLex a Parlex és a LocLex. A GovLex a kormányzati jogszabályok előkészítéséért felelős. Olyan informatikai háttérrel rendelkezik, amely felületen keresztül elvégezhető a jogszabályok, előterjesztések, és jelentések véleményezése, megosztása, továbbá szervező, lekérdező, nyilvántartó és végrehajtó ellenőrző szolgáltatásokkal is rendelkezik. A Törvényalkotás Parlamenti Informatikai Rendszere a ParLex, amely egy parlamenti dokumentum- és irományszerkesztő, folyamatkezelő rendszer. A ParLex a megfelelő felhasználói és adatbiztonság mellett biztosítja az egyes irományok szerkesztését és elektronikus benyújtását.[50] A LocLex rendszer az önkormányzatok jogszabály-előkészítési, -szerkesztési és -feltöltési folyamatait támogatja.

45 Digitális megoldások a jövő hadseregében. Uni-nke.hu, Budapest, 2019. Online: https://www.uni-nke.hu/hirek/2019/08/07/digitalis-megoldasok-a-jovo-hadseregeben (Letöltve:2020. 01. 31.).

46 DARPA, Army & Team Platypus: Big Boosts For Artificial Intelligence. Breakingdefense.com, 2018. Online: https://breakingdefense.com/2018/09/darpa-the-army-team-platypus-artificial-intelligence-for-future-war/ Letöltve: 2021. 02. 28.).

47 Darpa.mil. Online: https://www.darpa.mil/ (Letöltve:2020. 02. 13).

48 Digitális megoldások a jövő hadseregében. Uni-nke.hu, Budapest, 2019. Online: https://www.uni-nke.hu/hirek/2019/08/07/digitalis-megoldasok-a-jovo-hadseregeben (Letöltve:2020. 01. 31.).

49 A Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program éves fejlesztési keretének megállapításáról szóló 1004/2016. (I. 18.) Korm. határozat.

50 Elektronikus irományszerkesztés és benyújtás (ParLex rendszer) Parlament.hu, Budapest, Online: https://www.parlament.hu/elektronikus-iromanyszerkesztes-es-benyujtas-a-parlex-rendszer- (Letöltve:2020. 02. 12.).

A HM az elektronikus ügyintézés jegyében 2015 februárjától alkalmazza sikeresen a Honvédelmi Minisztérium Költségvetés Gazdálkodási Információ Rendszer, Ügyfélszolgálati Rendszert (HM KGIR ÜSZR), amely univerzális portálként alkalmas a pénzügyi nyilvántartások és személyi ügyintézés mellett a teljes állomány számára elérhető gyors és személyes megjelenést mellőző elektronikus ügyintézésre is.[51] A HM is csatlakozott az IJR-projekthez, így a tesztüzemet követően az éles rendszer a tárcán belül is bevezetésre kerül. Az IJR éles üzemének bevezetésére a teszt üzemet követően, 2020. augusztus 1. napjától kerültsor.[52]

A magyar űrprogram

A magyar űrprogram fellendítése érdekében 2019 novemberében a magyar külgazdasági és külügyminiszter az orosz Roszkoszmosz állami űrkutatási vállalat igazgatójával folytatott tárgyalásokat. A magyar–orosz koalíció célja, hogy a jelenleg Oroszországban futó magyar technikai és technológiai értéket képviselő űrprogramok hivatalosan is magyar–orosz űrkutatási projektekként folytatódjanak. Az együttműködés hosszútávú célja egy magyar űrhajós munkájának 2024/2025-re a Nemzetközi Űrállomáson (a továbbiakban: ISS) történő biztosítása, valamint, hogy a magyar fejlesztéssel és szellemi értékkel létrehozott űripari eszközöket a magyar kutatóűrhajós vigye fel az ISS-re, és a kutatómunkáját 3-6 hónapon át végezhesse.[53]

A magyar űripari tevékenység, a magyar űripari vállalatok és a magyar egyetemek űriparral és űrtechnológiával foglalkozó kutatóinak a magyar–orosz koalíció új lehetőséget ad a magyar űripar fejlődése, fejlesztése és a már meglévő magyar technológiák elterjedése kapcsán. A sikeres koalíció és a magyar űripar fejlesztése érdekében az űrkutatás területével, a nemzeti űrkutatási alap létrehozásával bővül ki a külgazdasági és külügyminisztérium portfóliója.[54]

Katonai hírközlő és kommunikációs rendszer digitalizációja

Végezetül, de nem utolsó sorban az MH átfogó digitalizációjának eléréséhez elengedhetetlen a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának (a továbbiakban: MH KCEHH) fejlesztése. Az MH KCEHH egy speciális, zártcélú infokommunikációs hálózat, amelynek képesnek kell lennie akár békeidőben, akár minősített időszakban az MH vezetési és irányítási rendszereinek a támogatására a technológiai, technikai és szolgáltatási háttér, valamint a működési környezet biztosításával. A rendszer egy olyan hálózati alapú kritikus infrastruktúra, amely híradó és informatikai rendszerek és eszközök alapjain nyugszik. A hálózat feladata, hogy kiszolgálja a katonai felsővezetés híradó és informatikai igényeit, biztosítsa a vezetési-irányítási rendszerek technológiai és technikai alapjait, valamint lehetővé tegye béke- és minősített időszakban is a híradó és informatikai szolgáltatások elérését. További feladata más infokommunikációs hálózatokhoz való csatlakozás és az arról való leoldás, azaz önálló működés biztosítása is.[55]

51 A Honvédelmi Minisztérium fejezet Költségvetés Gazdálkodási Információs Rendszerről szóló 80/2014. (XII.5.) HM utasítás.
52 Az Integrált Jogalkotási Rendszer bevezetéséről és az ahhoz kapcsolódó feladatokról szóló 1612/2019. (X. 24.) Korm. határozat.
53 „Oroszországgal közös cél, hogy magyar űrhajós kezdhessen el dolgozni 2025-re" Magyarhirlap.hu, Budapest, 2019. 12. 13. Online: https://www.magyarhirlap.hu/kulfold/20191213-magyar-orosz-urkutatasi-projektek-indulnak (Letöltve:2020. 02. 12.).
54 Urvilag.hu. Online: http://www.urvilag.hu/ (Letöltve:2020. 02. 12.).
55 A Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának békeidejű üzemeltetési és felügyeleti rendjéről, valamint a központilag biztosított szolgáltatások igénybevételének szabályairól szóló 55/2013. (IX. 13.) HM utasítás.

Az MH KCEHH rendelkezésre állása honvédelmi érdek. A digitális kornak megfelelő alapú technikák és szolgáltatások mentén működő hálózat fejlesztése azonban nem odázható tovább. Egyrészt meg kell felelnie a digitális robbanás következtében fejlődő nemzetközi elvárásoknak azért, hogy más nemzetek hálózataival és rendszereivel tudjon együttműködni, másrészt ehhez összhangban kell állnia a szövetségi tagságunkból adódó követelményrendszerrel.

A fejlesztéseket az alábbiak mentén szükséges eszközölni: (1) sávszélesség, adatátviteli sebesség növelése; (2) hardveres és szoftveres átviteli utak kapacitásbővítése; (3) hardver, szoftverplatform, szerverfarmok cseréje, korszerűsítése; (4) tartalékképzés, tartalékeszközök biztosítása; (5) kibervédelmi képesség kialakítása, növelése; (6) hálózati, felhasználói, hardveres, szoftveres biztonság kiépítése; (7) rendelkezésre állás, megbízhatóság, rugalmasság biztosítása; (8) a szolgáltatás minőségének növelése.[56]

Az alapvető cél tehát a híradó és informatikai rendszer, szolgáltatás és információcentrikussá tétele, a felhasználóbarát többfunkciós, konvergált és korszerű digitális hálózat kiépítése és az általános fejlődés mellett a védelmi szféra fejlődése. További cél, hogy a szolgáltatások eljuthassanak a harctéren küzdő katonákhoz, valós idejű kép közvetítésével. A hálózatnak egyrészt biztosítania kell a polgári és rendvédelmi szervek hálózataival való együttműködést, másrészt kibertámadás, illetve különleges jogrend esetén az önálló zavartalan működést is.[57] Az MH KCEHH fejlesztésének hosszútávú célja tehát, hogy a digitális és hálózatalapú rendszerek képesek legyenek önállóan működtetni a közigazgatást, fenntartani az ország vezetését a békétől eltérő jogrendben is.

Összegzésképp megállapítható, hogy az MH teljes körű digitalizációja érdekében ajánlásokként megfogalmazott 10 platform különböző intenzitással bír. Ez azt jelenti, hogy nem azonos súllyal jelennek meg a digitalizációs célok eléréséhez tett lépésekben. Ahhoz azonban, hogy az MH áttérjen és felzárkózzon a fejlett katonai, informatikai, digitális és hálózatalapú rendszerekhez, ezzel biztosítva e rendszerek önálló és független működését, szükséges az ajánlások szerinti platformok azonos súllyal és intenzitással való kezelése.

Befejezés

A dolgozat azon a feltételezésen íródott, hogy a digitális robbanás időszakában az új biztonsági kihívásokkal való sikeres fellépés érdekében elengedhetetlen a hadsereg modernizációja, amelyet a Zrínyi 2026 keretében a HM az MH-val karöltve 2017-ben kezdett el megvalósítani.[58]

A Zrínyi 2026 célkitűzési között szerepel az MH áttérése és felzárkózása az informatikai, digitális és hálózatalapú katonai rendszerekhez. A fejlesztések megvalósulásának következtében a honvédelem egésze digitális platformra állítható lenne, amely azt eredményezné, hogy a piaci high-tech rendszerek és a közigazgatás által használt infrastruktúrákhoz igénybe vett

56 Jobbágy Szabolcs: A Magyar Honvédség kormányzati célú elkülönült hírközlő hálózata. Hadmérnök,2017. XII. évf. 233. o. Online: http://hadmernok.hu/173_20_jobbagy.pdf (Letöltve:2020. 02. 09.).

57 uo.

58 A Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról szóló 1298/2017. (VI. 2.) Korm. határozat.

védelmi, katonai, nemzetbiztonsági rendszerek önállóan, leválasztva is működhetnének a Kormány infokommunikációs támogatása érdekében.[59]

A dolgozat tézise az volt, hogy a honvédelmi, katonai és nemzetbiztonsági rendszerek hazai digitális hálózatba való beágyazódása szükséges annak érdekében, hogy a békeidőben megfelelően működő katonai informatikai, digitális és hálózatalapú rendszerek képesek legyenek önállóan működtetni a közigazgatást, fenntartani az ország vezetését a békétől eltérő különleges jogrendben is.[60]

A tézis igazolásaképp a dolgozat első fejezete bemutatta azokat a haderőfejlesztési és digitális platformokat, amelyek mentén a Zrínyi 2026 hosszútávon lefektette az MH digitalizációja és modernizációja érdekében tett cél- és eszközrendszerét, különös tekintettel a Zrínyi 2026 bemutatására továbbá a légierő és a szárazföldi erők modernizálására. A második szakaszban, a teljesség igénye nélkül, nemzetközi példák bemutatásával 10 ajánlás fogalmazódott meg a honvédség teljes körű digitális platformra helyezése érdekében.

Következtetésképp megállapítható, hogy a Zrínyi 2026 teljes programja összhangban áll a honvédség digitalizációjával. Ez azt jelenti, hogy a már megvalósult beszerzések, beruházások, képzések, továbbképzések, honvédelmi programok egyre inkább a digitalizáció érdekében történtek.

A már elért eredmények és a további célok ismeretének hatására fogalmazódott meg a dolgozat második felében bemutatott 10 ajánlásba rendezett platform, amelyek megismerése, alkalmazása és fejlesztése által a honvédelem egésze digitális alapokra helyeződhetne.

Ahhoz azonban, hogy az MH áttérjen és felzárkózzon az informatikai, digitális és hálózatalapú katonai rendszerekhez, szükséges az ajánlások szerinti platformok azonos súllyal és intenzitással való kezelése. A Zrínyi 2026 célkitűzéseinek megvalósulása, valamint a digitális platformok azonos súllyal és intenzitással való kezelése esetén tehát a honvédelem egésze digitális platformra állítható, amely azt eredményezné, hogy a piaci high-tech rendszerek és a közigazgatás által használt infrastruktúrákhoz igénybe vett védelmi, katonai, nemzetbiztonsági rendszerek önállóan, leválasztva is működhetnének a Kormány infokommunikációs támogatása érdekében.

59 Babos Tibor: A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái. Hadtudomány, Budapest, 2018. Online: http://real.mtak.hu/82604/1/2018ebabos2.pdf (Letöltve:2020. 01. 26.).

60 uo.

Irodalomjegyzék

1. A haza védelme, a nemzet szolgálata. Honvedelem.hu, Budapest, 2019. Online: https://honvedelem.hu/files/files/116159/honvedseg_kiadvany_165x235mm_v2_6_.pdf (Letöltve:2020. 02. 14.).
2. A Honvédelmi Minisztérium fejezet Költségvetés Gazdálkodási Információs Rendszerről szóló 80/2014. (XII. 5.) HM utasítás.).
3. A járványról és a haderőfejlesztésről is beszélt a honvédelmi miniszter. Honvedelem.hu; Budapest, 2020. 12.05. Online: https://honvedelem.hu/hirek/a-jarvanyrol-es-a-haderofejlesztesrol-is-beszelt-a-honvedelmi-miniszter.html (Letöltve: 2021. 02. 27.).
4. A Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program éves fejlesztési keretének megállapításáról szóló 1004/2016. (I. 18.) Korm. határozat.
5. A Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának békeidejű üzemeltetési és felügyeleti rendjéről, valamint a központilag biztosított szolgáltatások igénybevételének szabályairól szóló 55/2013. (IX. 13.) HM utasítás.
6. A Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról szóló 1298/2017. (VI. 2.) Korm. határozat.
7. Aki már huszonöt éve ismeri a „nagymacskákat". Honvedelem.hu, Budapest. Online: https://honvedelem.hu/hirek/aki-mar-huszonot-eve-ismeri-a-nagymacskakat.html (Letöltve: 2021. 02. 27.).
8. Átadták a Magyar Honvédség Kiber Képzési Központját. Kormany.hu, Budapest, 2019. 06. 13. Online https://2015-2019.kormany.hu/hu/honvedelmi-miniszterium/hirek/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat (Letöltve:2020. 02. 13.).
9. Az Integrált Jogalkotási Rendszer bevezetéséről és az ahhoz kapcsolódó feladatokról szóló 1612/2019. (X. 24.) Korm. határozat.
10. Babos Tibor: A biztonság globális és európai összefüggései. Hadtudomány, Budapest, 2019/4. Online: http://real.mtak.hu/105840/1/016-029_Babos.pdf (Letöltve:2020. 02. 12.).
11. Babos Tibor: A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái. Hadtudomány, Budapest, 2018. Online: http://real.mtak.hu/82604/1/2018ebabos2.pdf (Letöltve:2020. 01. 26.).
12. Baranyai Gábor: Megérkeztek a honvédség új helikopterei a német gyárból. Magyarnemzet.hu, 2019. 11. 19. Online: https://magyarnemzet.hu/belfold/megerkeztek-a-honvedseg-uj-helikopterei-a-nemet-gyarbol-7505657/ (Letöltve: 2020. 01. 25.).
13. Bencze Áron: Digitális ugrásra készül a Magyar Honvédség. Innoteka.hu, Budapest, 2019.05.03. Online: https://www.innoteka.hu/cikk/digitalis_ugrasra_keszul_a_magyar_honvedseg.1909.html (Letöltve:2020. 01. 31.).
14. Blackman, Colin – Forge Simon: 5GDeployment. Europarl.europa.eu, Brussels, 2019. Online: https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/631060/IPOL_IDA(2019)631060_EN.pdf (Letöltve:2020. 02. 13.).
15. Cifka Miklós: A jövő gyalogos katonája: baka a digitális korszakban. Sg.hu, Budapest, 2005.03.29. Online: https://sg.hu/cikkek/tudomany/36233/a-jovo-gyalogos-katonaja-baka-a-digitalis-korszakban (Letöltve:2020. 02. 13.).

16. DARPA, Army & Team Platypus: Big Boosts For Artificial Intelligence. Breakingdefense.com, 2018. Online: https://breakingdefense.com/2018/09/darpa-the-army-team-platypus-artificial-intelligence-for-future-war/ (Letöltve: 2021. 02. 28.).
17. Darpa.mil. Online: https://www.darpa.mil/ (Letöltve:2020. 02. 13).
18. Digitális megoldások a jövő hadseregében. Uni-nke.hu, Budapest, 2019. Online: https://www.uni-nke.hu/hirek/2019/08/07/digitalis-megoldasok-a-jovo-hadseregeben (Letöltve: 2020. 01. 31.).
19. Draveczki-Ury Ádám: Digitális világ a haza szolgálatában. Honvedelem.hu, Budapest, 2019.04.30. Online: https://honvedelem.hu/media/aktualis-videok/digitalis-vilag-a-haza-szolgalataban.html (Letöltve: 2020. 02. 09.).
20. Elektronikus iromány szerkesztés és benyújtás (ParLex rendszer) Parlament.hu, Budapest, Online: https://www.parlament.hu/elektronikus-iromanyszerkesztes-es-benyujtas-a-parlex-rendszer- (Letöltve: 2020. 02. 12.).
21. GÁCSER Zoltán: A katona harci képességét növelő korszerű, hálózatba integrált egyéni felszerelésrendszerének kialakítási lehetőségei a Magyar Honvédségben c. PhD értekezés. Budapest, 2008.Online:https://nkerepo.uninke.hu/xmlui/bitstream/handle/123456789/12102/ertekezes.pdf;jsessionid=E53B0E3B1B43A817529E3C72C25CEF01?sequence=1 (Letöltve: 2021. 02. 28.).
22. https://honvedelem.hu/media/aktualis-videok/tovabb-gyarapodo-legi-kepesseg.html (Letöltve: 2021. 02. 27.).
23. Irán támadást intézett két amerikai bázis ellen Irakban. Hirtv.hu, Budapest, 2020.01.08. Online: https://hirtv.hu/hirtvkulfold/iran-ballisztikus-raketakkal-tamadott-meg-amerikai-celpontokat-irakban-2492968 (Letöltve: 2020. 01. 31.).
24. Jobbágy Szabolcs: A Magyar Honvédség kormányzati célú elkülönült hírközlő hálózata. Hadmérnök,2017. XII. évf. 233. o. Online: http://hadmernok.hu/173_20_jobbagy.pdf (Letöltve: 2020. 02. 09.).
25. Key Issues Relevant to The U.S. Army's Transformation to the Objective Force, An AUSA Torchbearer Issue, Vol.II. USA, 2002. Online: https://www.ausa.org/sites/default/files/TBNSR-2002-The-US-Armys-Transformation-to-the-Objective-Force-Vol2.pdf (Letöltve: 2020. 02. 09.).
26. Kiss Adorján: Okosfegyverekkel látnák el a hadsereget. Vg.hu. 2019.10.21. Online: https://www.vg.hu/gazdasag/gazdasagi-hirek/okosfegyverekkel-latnak-el-a-hadsereget-2-1821681/ (Letöltve: 2020. 01. 31.).
27. Land Warrior Integrated Soldier System. Army-technology.com, USA. Online: https://www.army-technology.com/projects/land_warrior/ (Letöltve: 2020. 02. 09.).
28. Lockheed Martin - F-35 Lightning II. Aerotech.hu, Online: http://www.aerotech.hu/f-35.php (Letöltve: 2021. 02. 28.).
29. Már a szolnoki bázison vannak a honvédség első új helikopterei. Honvedelem.hu, Budapest, 2019. 11. 19. Online: https://honvedelem.hu/cikk/mar-a-szolnoki-bazison-vannak-a-honvedseg-elso-uj-helikopterei/ (Letöltve: 2020. 01. 25.).

30. Négyesi Imre: A mesterséges intelligencia és a hadsereg I. Hadtudományi Szemle, Budapest, 2017/2. Online: http://epa.oszk.hu/02400/02463/00035/pdf/EPA02463_hadtudomanyi_szemle_2017_2_023-034.pdf (Letöltve: 2020. 02. 13.).
31. „Oroszországgal közös cél, hogy magyar űrhajós kezdhessen el dolgozni 2025-re" Magyarhirlap.hu, Budapest, 2019. 12. 13. Online: https://www.magyarhirlap.hu/kulfold/20191213-magyar-orosz-urkutatasi-projektek-indulnak (Letöltve: 2020. 02. 12.).
32. Online: https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf (Letöltve: 2020. 01. 24.).
33. Rakétatámadások Irakban: Irán gyorsan megtorolta Szulejmáni likvidálását. Hvg.hu, Budapest, 2020. 01. 08. Online: https://hvg.hu/vilag/20200108_Iran_raketacsapast_mert_az_amerikaiak_egy_iraki_tamaszpontjara (Letöltve: 2020. 02. 13.).
34. Révész Béla: Csúcstechnika a levegőben. Honvedelem.hu, Budapest, 2019. 11. 18. Online: https://honvedelem.hu/galeriak/csucstechnika-a-levegoben/ (Letöltve: 2020. 01. 25.).
35. Robotok uralják a jövő harctereit? Honvedelem.hu, Budapest, 2010. 08. 05. Online: https://honvedelem.hu/hirek/robotok-uraljak-a-jovo-harctereit.html (Letöltve: 2020. 02. 13.).
36. Tovább gyarapodó légi képesség. Honvedelem.hu, Budapest, 2020. június 22. Online: https://honvedelem.hu/media/aktualis-videok/tovabb-gyarapodo-legi-kepesseg.html (Letöltve: 2021. 02. 27.).
37. Újabb helikopterek érkeztek. Honvedelem.hu, Budapest, 2020. december 10. Online: https://honvedelem.hu/hirek/ujabb-helikopterek-erkeztek.html (Letöltve: 2021. 02. 27.).
38. Védelmi ipar ágazati koncepciója. Hmarzenal.hu, Budapest, 2018. Online: http://www.hmarzenal.hu/vedelmi-ipar/vedelmi-ipar-agazati-koncepcioja.pdf (Letöltve: 2020. 02. 13.).
39. Zrínyi 2026 honvédelmi és haderőfejlesztési program, A haza védelmében. Honvedelem.hu, Budapest. Online: https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf (Letöltve: 2020. 01. 24.).
40. Trautmann Balázs: Fémharcosok. Honvedelem.hu, Budapest, 2016. 07. 24. Online: https://honvedelem.hu/hatter/haditechnika/femharcosok.html (Letöltve: 2020. 02. 09.).
41. Draveczki-Ury Ádám: Zrínyi 2026. Honvedelem.hu, Budapest, 2017. 01. 16. Online: https://honvedelem.hu/cikk/zrinyi-2026/ (Letöltve: 2020. 01. 27.).
42. Középpontban a katona. Kormany.hu, Budapest, 2019. 05. 01. Online: https://2015-2019.kormany.hu/hu/honvedelmi-miniszterium/hirek/kozeppontban-a-katona (Letöltve: 2020. 02. 13.).
43. Katonás Infotér. Honvedelem.hu, Budapest, 2019. 10. 16. Online: https://honvedelem.hu/hirek/hazai-hirek/katonas-infoter.html (Letöltve: 2020. 01. 27.).
44. Urvilag.hu. Online: http://www.urvilag.hu/ (Letöltve: 2020. 02. 12.).
45. 5GK-Magyarországi 5G Koalíció. Digitalisjoletprogram.hu, Budapest. Online: https://digitalisjoletprogram.hu/hu/tartalom/5gk-magyarorszagi-5g-koalicio (Letöltve: 2020. 02. 13.).

Csutak Zsolt

Hálózatok útvesztőjében, a 21. századi technológiák társadalmi hatásai és biztonsági kockázatai

Rezümé

A 21. században az emberiség korábban még nem tapasztalt technológiai változásokkal szembesül, amelyek teljesen új társadalmi kihívásokat jelentenek és nyilvánvalóan jelentős biztonsági kockázatokat is hordoznak. E virtuális ökoszisztémában változatos hátterű szereplők versengenek és konfliktusokat gerjesztenek, bűncselekményeket követnek el, ami napjainkban már elsőszámú globális problémává fejlődött. Az online médiaszolgáltatók befolyása, a kiberfegyverek, harci robotok, okos gépek hálózatai immár a jelen és a közeljövő világának aggodalomra is okot adó trendjeinek alkotói. Ugyanakkor e problémákat könnyebb beazonosítani, mint megfelelő válaszokat találni rájuk.

Resume

In the 21st century, the human race must face and cope with such new revolutionary technological challenges and trends that had never been encountered before. These factors feature brand new psychologic, social challenges and evidently pose serious security risks, too. In this inter-connected digital ecosystem, various actors commit diverse acts simultaneously, which altogether constitute global security risks. Issues, such as cyber warfare, weaponization of digital information and growing impact of social media platforms cannot be neglected anymore. However, finding proper solutions proves to be a bigger intellectual and political challenge than identifying the emerging problems.

Vezetői összefoglaló

Az utóbbi évtizedben a kibertér hadszíntérré alakult, a digitális információ kiberfegyverként is alkalmazható destruktív eszközzé vált, míg a felhasználók köre követhetetlen és ellenőrizhetetlen módon globalizálódott.

Az új technológiai alkalmazások társadalmi, lélektani hatásáról és a mesterséges intelligencia alkalmazásának biztonsági, humán és etikai kockázatairól igencsak kevés szó esik, következésképp egyre fontosabb mélyreható, holisztikus és antropocentrikus szemléletű elemzéseket és kutatásokat végezni úgy az egyén, mint az állami felhasználók szintjén.

A politikai döntéshozók lépéskényszerben vannak a kibertér folyamatainak, a digitális alkalmazások és a nagyon befolyásos online médiaszolgáltatók jogi szabályozását illetőleg, továbbá a sokasodó kiberbiztonsági kockázatok feltárása és ellenőrzése tekintetében.

Alapvetések

„A képzelet fontosabb, mint az ismeret"
Albert Einstein

Albert Einstein elhíresült gondolatával indítva eszmefuttatásunkat a 21. század elején a biológiai és kibertéri vírusjárványok korában érdemes a tudományos-fantasztikus írók, jövőkutatók elképzeléseit is megvizsgálni, akár még a múlt század elejéről is, hiszen kísérteties hasonlóságokra, megfelelésekre és megvalósult disztópikus jelenségekre bukkanhatunk napjaink globalizált társadalmaiban. Elég, ha csak a brit H. G. Wells, Arthur C. Clarke, William Gibson vagy az amerikai sci-fi nagymesterének számító Isaac Asimov megvalósult elképzelésire gondolunk, mint a világméretű számítógép-alalapú könyvtárra, lakható űrállomásra vagy épp okos beszélő gépek és emberek összekapcsolódott hálózatára.[1]

Az emberiség létét fenyegető vírustámadásról, sőt másodlagos virtuális valóságkettőzésről (mátrix) is olvashatunk ezekben a tudományos-fantasztikus művekben, amelyek révén, ha megfogadjuk Einstein fent említett bölcsességét, tulajdonképpen könnyebben értelmezhetjük jelen valóságunk kihívásait is. Az emberiség írott történelmének körülbelül hét évezrede során még nem tapasztalhattunk olyan szintű gyors technológiai és életmódbeli változásokat, mint amilyenek az utóbbi évtizedekben meghatározzák hétköznapjainkat.

A következő oldalakon arra az alapkérdésre keresünk választ, hogy milyen jellemző vonásokkal írhatjuk le a posztmodern társadalmak és az új digitális technológiák komplex kapcsolatát, összefüggéseit. A téma kevésbé vizsgált társadalmi vetületeit és tudományetikai problémáit, illetve a biztonságpolitikai veszélyforrások feltárását fogjuk áttekinteni és elsődlegesen elemezni.

Elöljáróban, mintegy tézisszerűen megállapíthatjuk, hogy a teljesen új digitális technológiák, illetve a mesterséges intelligencia beláthatatlan fejlődési horizontja és perspektívái reális kockázati tényezőhalmazt hordoznak magukban. Továbbá, e technológiák immanens fejlődési potenciálját tekintve, és a történelmi tapasztalatok alapján az emberiség pusztításra és építésre egyaránt hajlamos orientációját figyelembe véve, az új technológiák számos és jelentős veszélyforrást hordoznak a demokratikus társadalmak működésére és az emberi kapcsolatok alakulására nézve.

Emberi létünk és egyre jobban összefonódó globalizált társadalmaink egészét vizsgáló holisztikus szemléletű filozófusok szerint napjainkban a számítógépek vezérelte digitális rendszerek és a mesterséges intelligencia (a továbbiakban: MI) fejlődésének korában olyan drasztikus átalakulásnak és paradigma-szintlépésnek lehetünk tanúi, mint amit fél évezreddel ezelőtt a könyvnyomtatás megjelenése, illetve a 19. század végén az elektromos áram elterjedése jelenthetett.[2] Érzékelhető módon, a McLuhan által csak Gutenberg-galaxisnak[3] is nevezett könyv-, és papíralapú, tudásmegosztáson alapuló civilizációs korszak élettartamának végéhez közelít, helyesebben szólva gyökeresen átalakul, digitalizálódik, virtualizálódik, és

1 Több mint beszédes Isaac Asimovnak, a The New York Timesnak adott jövőbelátó interjúja 1964-ből a „2014-es világkiállítás" technikai csodáiról beszélve: „Visit to the World Fair of 2014".
2 Martin Ford: Robotok kora. Budapest, HVG, 2017, 10 – 13.
3 Marshall McLuhan: The Gutenberg Galaxy, Toronto, University of Toronto Press, 2011

ami talán a legjellemzőbb új vonása: különböző médiaplatformokra szakosodva hálózatokba szerveződik. Az emberiség történetében soha nem voltak az emberi és gépi hálózatok olyan fontosak és befolyásosak, mint napjainkban, a legnagyobb ember alkotta mesterséges hálózat, az internet korában, amely, amint látni fogjuk, már túlságosan is meghatározza a 21. századi „posztposztmodern" társadalmakat, azok minden szegmensével együtt.

Felmérések szerint[4] 2018 óta az emberiség nagyobbik fele (több mint 4 milliárd ember) már napi rendszerességgel használ valamilyen digitális online eszközt, és az összekapcsolódott globális okoseszköz állomány *(smart devices)* mérete, az úgynevezett IoT *(internet of things)*, vagyis a világhálóra kapcsolódott készülékek száma ma már 25 milliárdra tehető, és 2025-re elérheti a döbbenetes 75 milliárdos számarányt is.[5] Ezen új, tulajdonképpen önálló életet élő gigászi eszközállomány (az okos óráktól önjáró mini tengeralattjárókon és katonai robotokon keresztül a teljesen automata budapesti 4-es metróig) már részben mesterséges intelligencia felügyelete alatt dolgozik, amely már önmagában biztonsági kockázati tényezőt jelent még a rosszindulatú külső behatások nélkül is.

A következő oldalakon rövid betekintést nyújtunk a számítógép-alapú (közkeletű szóhasználatban digitális) eszközállomány és milliónyi alkalmazástípus jelentette új paradigma fő jellemvonásaiba, és különösképpen az új világjelenség biztonságpolitikai vetületeibe, amelyek nemcsak az egyéni végfelhasználók, hanem a multinacionális társaságok és nemzetállamok biztonságát is jelentősen meghatározzák és befolyásolják. Kérdés, hogy az emberi természet és hagyományos interperszonális együttműködésen alapuló társadalmaink felkészültek-e a forradalmian új és radikális digitális átállásra, életmódra és mindez milyen kulturális, társadalmi és következésképp politikai következményekkel járhat? Ahogy számos világhírű gondolkodó, mint Albert Einstein, Neumann János, Stephen Hawking vagy Yuwal Noah Harari és technológiai forradalmár nagyvállalkozó, mint Elon Musk is feltette már a kényelmetlen kérdést: foglalkozunk-e eleget az új, gyakran embert helyettesítő okos technológiai megoldások (például a mesterséges intelligencia és robotika) erkölcsi és emberi vonatkozásaival, vagy a kényes kérdések megválaszolását a jövő generációira hagyjuk?[6]

A világháló biztosította globális virtuális összekapcsolódás *(global interconnectedness)* előzmény nélküli az emberiség történetében, és sajnálatos módon az ezzel járó álhírek, áltudományos fórumok és összeesküvés-elméletek viharos terjedése is komoly társadalmi és biztonságpolitikai kockázatot jelent egyéni, közösségi és állami szinten egyaránt. Az emberi természet kettős jellege révén az internet és az új digitális technológiai megoldások is lehetnek egyben fegyverek és oktató, nevelő, gyógyító hatású eszközök a felhasználók kezében. Ugyanakkor, a történelmi tapasztalat és a hobbesiánus antropológiai pesszimizmusból származó filozófiai álláspont alapján[7] némi általánosítással megállapíthatjuk, hogy az emberek (egyéni és közösségi szinten egyaránt) hajlamosak egoista érdekeik, vágyaik kielégítése céljából inkább kártékonyan és mások számára előnytelen módon használni bármilyen eszközt, legyen az a közösségi média vagy a mesterséges intelligencia.

4 Statista 1: https://www.statista.com/topics/1145/internet-usage-worldwide/ letöltés ideje:2020.01.15
5 Statista 2.: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide letöltés ideje: 2020. 01. 28
6 Clifford, Catherine: „Elon Musk on AI". In CNBC. https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-a-i-is-more-dangerous-than-nuclear-weapons.html letöltés ideje:2020. 03. 19.
7 Leo Strauss: A politikai filozófia története. Európa, Budapest, 1994, 409–412.

Következésképp, a növekvő biztonságpolitikai aggodalmakon és potenciális kiberveszélyforrásokon túl, fontosnak tarjuk megvizsgálni az új digitális technológia alapú társadalmaink szociálpszichológiai, kulturális átalakulási folyamatát és kulcsfontosságú tényezőit, amelyek még a biztonsági kihívásoknál is drasztikusabb változásokat és radikális jelenségeket tartogatnak az elemzők számára. Társadalomtudósok és kritikus elemzők véleménye szerint[8] a digitális információs technológiák tervezői és előállítói rendszerszerűen elfeledkeznek új megoldásaik közvetett egyéni és társadalmi hatásáról, vagy csak évekkel később, felemás érzésekkel szembesülnek azokkal, mint ahogy lentebb látni fogjuk, az internet tervezésekor is történt.

Általánosítással élve, a közép-, illetve hosszútávú társadalmi, kulturális és egyéb emberi következmények vizsgálata, figyelembevétele nem tartozik a programozók, szoftverfejlesztő mérnökök prioritásai közé, és természetesen ezért nem szeretnénk őket kárhoztatni, hiszen egy digitális termék, szolgáltatás megtervezéséhez és előállításához teljesen más képességekre és ismeretekre van szükség, mint azok későbbi biztonságpolitikai vagy össztársadalmi hatásának elemzéséhez. Ugyanakkor, mindezen technológiák hatáselemzése újszerűségük, egy-két évtizedes vagy csupán pár éves múltjuk miatt, nem kis szellemi kihívást jelent. Olyan kutatókat, elemzőket kell találni, akik, egyrészt behatóan ismerik az új digitális technológiákat, másrészt a társadalmi vonatkozásokra és az emberi rezgésekre is fogékonyak, valamint a tágabb társadalomtudományi összefüggések feltárására is képesek.

Feltehetőleg ezen okból kifolyólag e puhább technológiai vonatkozások kevésbé kutatott és feltárt területnek számítanak a jelen pillanatig, mondhatnánk egészen addig a fokig, amikor számos negatív hatásuk már a laikusok számára is nyilvánvalóvá válik. Ezzel kapcsolatban érdemes megjegyeznünk két kiragadott és elgondolkodtató példát, amelyek már igencsak meghatározzák hétköznapjainkat a kiberkorban. Egyrészt Norton A. Schwartz, az amerikai légierő tábornokának és kibervédelmi parancsnokának *bon mot*-vá vált megjegyzése sokat mondó, miszerint napjainkban „egy áramszünet lehet, hogy csupán áramszünet, ellenben a kiberhadviselésben már lehet, hogy egy előzetes katonai csapás része."[9]

Másrészt, érdemes felidéznünk az internet két alapító atyjának is tartott Vinton Cerf és Sir Tim Berners-Lee keserű hangvételű interjúját a *The Guardian*ben az általuk kifejlesztett világhálózat átalakulásáról, sorsáról.[10] Nevezetesen, a két világhírű szakember meglátása szerint a számítógép-alapú világhálózat (internet) eredeti elképzelésük helyett – mint globális digitális tudás piactér – az 1991 óta eltelt három évtized alatt valami teljesen más képződménnyé alakult a közösségi média és a tömeges online játékok uralta korban. Elég, ha csak arra az elszomorító adatra gondolunk, miszerint a mély internet *(deep web)* alvilági bugyrait uraló sötét web *(dark web)* körülbelül 80%-a gyomorforgató gyermekpornográf és egyéb illegális tartalommal van feltöltve,[11] amely óriási veszélyforrást jelent úgy az egyének, mint a társadalom számára. Nem beszélve arról az elszomorító tényről, hogy a nemzetközi bűnüldöző szervezetek és internetes biztonsági cégek kutatásai szerint már 2016 óta az internetalapú

8 Harari, Yuwal: Homo Deus. Budapest, Animus, 2017, 195-200.

9 Clarke, Richard A. – Knake, Robert K.: Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins, New York, 2010, 25.

10 Solon, Olivia: „Tim Berners-Lee on the future of the web: ‚The system is failing'". In The Guardian. https://www.theguardian.com/technology/2017/nov/15/tim-berners-lee-world-wide-webnet-neutrality letöltés ideje: 2019. 12. 29

11 Ld. Chen, Hsinchun: Dark Web: Exploring and Data Mining the Dark Side of the Web. Springer, New York, 2012.

kiberbűnözés globálisan átvette a vezetést a kábítószer-, illetve illegális fegyver- és emberkereskedelemtől. Megdöbbentő adat, miszerint az új típusú, láthatatlan és névtelen kiberbűnözők által okozott kár mértéke a világon eléri az évi 5 500 000 000 000 dollárt, amely az Egyesült Államok mintegy másfél éves szövetségi költségvetésének megfelelő összeg.[12]

A szándékosan károkozó internetes szereplőkön keresztül a világháló, és különösképpen a közösségi hálózatok világa, szélsőségesen demokratizálta az információáramlást, eszmék és gondolatok cseréjét, terjedését a világban, és a fent említett realista-pesszimista emberi alapvonások révén inkább negatív előjellel. Az utóbbi évtizedekben jelentős mértékben erodálódott és megroppant a hagyományos társadalmi, politikai és akadémiai elitbe vetett hit és bizalom mértéke, és ezzel fordítottan arányosan az internetes valláspótlékszerű összeesküvés-elméletek *(konteók)*, babonaságok, hamis ezoterikus tanok népszerűsége, valamint a képzetlen megmondó-emberek, önjelölt szakértő *vlogger* influenszerek[13] befolyása sajnálatosan az egekbe szökött.[14]

Habár nem tartozik tanulmányunk elsődleges fókusztémakörébe az okos eszközök elterjedése és az emberi intelligencia kapcsolatának alakulásának vizsgálata, nagyon fontos vonatkozásnak tartjuk, amiről még valószínűleg sokat fognak értekezni a jövőben. Néhány kritikusabb amerikai kutató és tanulmány már rámutatott,[15] hogy az utóbbi évek felfoghatatlanul gyors és precedens nélküli digitalizálódása nyomán az egyre okosabb eszközök és alkalmazások révén az emberek mentálisan elkényelmesedtek, szellemi kreativitást és agilitást vesztő végfelhasználó fogyasztókká váltak, sőt egy vizsgált fókuszcsoport tagjainak mérhető általános intelligenciaszintje még kis mértékben csökkenést is mutatott.[16]

A felhasználók millióinak, különösképpen a fiatal generáció jelentős részének a digitalizált, virtuális (avagy kibertéri) másodlagos valóság már az elsődleges fizikai valóság kiterjesztésévé vált, sőt, sokuk esetében a világháló inkább elsődleges információ és élményforrásnak, megélt valóságnak tekinthető, annak minden személyiségtorzító és akár tudatmódosító veszélyforrásaival.

Fogalmak virtuális útvesztőjében

Az alábbiakban arra keresünk választ, hogy milyen tudományos paradigmák és percepciók jellemzik digitális világunkat, illetve milyen fogalmi keretrendszerben ragadhatjuk meg leginkább a világban zajló folyamatokat.

Manapság a köznyelvben gyakran szinonimaszerűen, jelentésbeli átfedésben használják a digitális és kiber kifejezéseket, habár az utóbbi lenne inkább helytállóbb és a valóságot jobban leképező fogalom, a sokkal szűkebb értelmezési dimenziójú digitálissal ellentétben. Természetesen mindkét fogalomnak van létjogosultsága, akárcsak magyar tudományos vonatkozása is, főleg a 2. világháború elől Amerikába menekült magyar atomfizikusok, elméleti

12 CyberCrime Magazine: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ letöltés deje: 2020. 01. 15.
13 Többnyire saját készítésű multimédiás tartalmakat rendszeresen közzétevő, célközönségüket aktívan befolyásolni képes online médiaszemélyiségek, celebek.
14 Krekó Péter: „Netes konteók" Index TNT Podcast: https://index.hu/techtud/2020/04/12/tnt_osszeeskuves_kreko_peter_podcast/ letöltés ideje: 2020. 04. 12.
15 Ld. Nicholas Carr: The Shallows: What the Internet is doing to our Brains. W. Norton, New York, 2011
16 Frischmann, Brett:" Is Smart Technology Making Us Dumb?" In Scientifc American, Dec., 27 2018.

matematikusok kimagasló kutatói munkássága révén. A második világháború idején az ifjú amerikai John W. Tukey princetoni matematikus zseni és magyar származású professzortársa, Neumann János kidolgozta és megalapozta a 0 és 1, kettes számrendszerbeli számjegy- *(binary digit),* vagyis egy egységnyi, bitalapú (0 vagy 1, igaz/hamis) algoritmusrendszert, amely a 20. század úttörő digitális számítástechnikai paradigmájává vált.[17] Tehát a digitális kifejezés elsősorban az elektronikus számítástechnikai folyamatokhoz és bináris rendszerű algoritmusokhoz kapcsolódik. Ezzel ellentétben felettébb sok félreértésre ad okot és alkalmat a *kiber* kifejezés és *kibernetika* tudományterület összemosása, önkéntelen és félrevezető felcserélése.

A kibernetika az információszerzés és dinamikus rendszerek irányításának, vezérlésének majd számítástechnikai modellezésének és programozásának új tudománya 1946 óta Norbert Wiener nevéhez fűződik, és a ma használatos kiber kifejezéstől teljességgel eltérő tudományos kontextusban volt használatos. Wiener, aki a görög kormányos *(kübernétész)* kifejezésből kölcsönözte új tudományágának elnevezését, az állatok és az ember alkotta mesterséges gépek dinamizmusát és irányítását hasonlónak vélte, amit aztán a játékelmélet és egyéb forradalmian új oldalági tudományos diszciplínák révén Neumann János és Harsányi János, Nobel-díjas amerikai magyar tudósok a számítástechnikában, valamint a társadalmi folyamatok (különösképpen háborús konfliktusok) lemodellezésére is kiterjesztettek, hiszen többségükben az amerikai védelmi kutatások szolgálatában működtek.[18] Ezzel kapcsolatban helytállónak bizonyult Bertrand Russell, híres brit matematikus és pacifista filozófus megjegyzése, miszerint háborús időszakban nem lehet tudományt művelni, ha annak nincs valamiféle hadászati kapcsolódása vagy jelentősége.[19]

A sokat használt kiber *(cyber)* kifejezés a szó napjainkban is használt értelmében elsősorban William Gibson kanadai fizikus, sci-fi íróhoz kapcsolódik, aki a *Burning Chrome* című novellájában 1982-ben használta először ezt a kifejezést mint számítógép és ember kölcsönhatásán alapuló rendszer metaforáját. Ugyanakkor, a teljesség igényével meg kell említenünk a sci-fi brit nagymesterének Arthur C. Clarke-nak *A város és a csillagok* című remekművét 1956-ból, amelyben már használta a virtuális mátrix és virtuális valóság fogalmakat teljesen hasonló kontextusban.[20]

Napjaink szakszerű alkalmazási módja és kontextusa szerint elsősorban a hadtudományban és biztonsági tanulmányokban használatos fogalomtár alapján, a kibertér a teljes elektromágneses spektrumon belül működő elektronikus eszközök, információs hálózatok rendszerére utal,[21] tehát jóval szélesebb dimenziójú és tartalmú kifejezés, mint a rokon értelmű szóként is használt és jóval régebbi „digitális" fogalma. A 2000. évben kidolgozott *Joint Vision 2020* címet viselő amerikai összhaderőnemi stratégiai dokumentumban nevesítették először a különféle katonai hadviselési tartományokat *(warfighting domain)* és működési környezetet *(operational environment)*, valamint területeket *(terrain)*, amelyek közé bekerült az

17 Father of digital computer János Neumann was born 114 years ago: http://abouthungary.hu/news-in-brief/father-of-digital-computer-janos-neumann-was-born-114-years-ago/ letöltés ideje: 2020. 03. 20.

18 Norbert Wiener:https://www.britannica.com/biography/Norbert-Wiener letöltés ideje: 2020. 03. 10.

19 Olivier Esteves: „Bertrand Russell: the utilitarian pacifist". In French Journal of British Studies. XX-1/2015https://journals.openedition.org/rfcb/308 letöltés ideje: 2020. 03. 25.

20 William Gibson: Cyberspace. http://www.technovelgy.com/ct/content.asp?Bnum=53 letöltés ideje: 2019. 12. 25.

21 Haig Zsolt: Információs műveletek a kibertérben. Dialóg Campus, Budapest, 2019. 22–26.

információs környezeten belül a kibertér is. A 2007. áprilisi Észtország elleni kibertámadás, a híres *web war one*[22] drámai eseményei után 2008-tól az új NATO kibervédelmi stratégiájában szintén megjelent a kibertér mint a dinamikus katonai és civil információs környezet része, és egyben mint potenciális új hadszíntér.[23] Sőt, az egyre szaporodó és komoly aggodalomra okot adó burkolt és nyílt kibertámadások, zsarolóvírusok 2014-be arra késztették a NATO legfőbb döntéshozó szervét, az Észak Atlanti Tanácsot, hogy a jövőben egy tagállamuk ellen elkövetett bizonyítható és visszakövethető kibertámadást valódi háborús indoknak és támadásnak *(casus belli)* nyilvánítsanak, és beemelték a kollektív védelmet nyújtó Washingtoni Szerződés híres 5. cikkelyének rendelkezései közé.[24]

A NATO ez irányú stratégiai megközelítéséhez és definíciójához hasonló elveket valló módon a hazai kibertér fogalmi tisztázásában élen járnak Haig Zsolt ezredes és Kovács László tábornok hadtudományos munkásságuk révén. Az információs műveletek és kiberhadviselés magyar szakértői szerint a kibertér elsődlegesen hadtudományos kontextusban nem más, mint „a harctéren a különböző hálózatba kapcsolt elektronikai rendszerek az információs színtérnek azt a részét használják, amelyben a különféle elektronikus információs folyamatok (elektronikai úton végrehajtott adatszerzés, adatfeldolgozás, kommunikáció stb.) realizálódnak, illetve az elektronikai rendszerek elleni tevékenység és a védelem megvalósul. Az információs színtér e tartományát gyakran *cybertérnek* is nevezzük."[25] Tehát, a tisztánlátás végett és a fogalmi, szemantikai zűrzavar elkerülése érdekében a szűkebb számítástechnikai dimenzióra szorítkozó digitális ökoszisztéma kifejezés helyett érdemes és javasolt a kiberdimenzió, avagy kibertér kifejezés használata, amely lefedi az adatközvetítő és feldolgozó fizikai hálózatot *(internet hardware),* az okos eszközök rendszerét *(Internet of Things),* illetve a rajtuk futó alkalmazások és programcsomagok *(software)* tömkelegét egyaránt az elektromágneses spektrum teljes skáláján.

A rekordgyorsasággal lezajló forradalmi technológiai paradigmaváltással valójában az átlagemberek milliói, illetve az állami szereplők jelentős része azóta sem tudnak mit kezdeni, főleg, ha berögzült 20. századi mentalitás és szokásrendszer rabjaiként közelítenek az új kihívások felé.

Adat és információ mint hatalom és fegyver a kiberkorban

„Az adat a 21. század olaja."[26]

Az alábbiakban arra a problémakörre, illetve jelenségre keresünk választ, hogy a világunkban észlelhető egyre növekvő mennyiségű digitális adattömeg és információállomány milyen általános tulajdonságokkal rendelkezik, mire használható, és milyen kiberbiztonsági veszélyeket hordozhat a felhasználók széles spektrumára.

22 Stephen Blank: Web War I: Is Europe's First Information War is a New kind of War? https://www.tandfonline.com/doi/full/10.1080/01495930802185312 letöltés ideje: 2020. 01. 12.

23 Häußler, Ulf: Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO's Treaty, https://www.sbs.ox.ac.uk/cybersecuritycapacity. letöltés ideje: 2020. 01. 10.

24 Brent, Laura: „NATO's role in cyberspace". In NATO Review, Febr., 2019

25 Haig Zsolt – Kovács László:"Fenyegetések a cybertérből". Nemzet és Biztonság, 2008/5. 63.o

26 Clive Humby brit matematikus, nagyvállalati marketing managernek tulajdonított mondás 2006-ból https://www.quora.com/Who-should-get-credit-for-the-quote-data-is-the-new-oil letöltés ideje: 2020. 01. 30.

Az információ – fogalomtisztázás végett: mint feldolgozott adat (halmaz) – már évszázadok óta hatalmi tényező, katonai, politikai vagy gazdasági előnyszerzés szempontjából kulcsfontosságú eszköz a döntéshozók kezében. Ez a megállapítás még hangsúlyosabban igaz napjainkban, amikor az emberi elme számára már felfoghatatlan mennyiségben termelődik virtuális elektronikus adat a világhálón. A humán felhasználók (plusz az IoT és az MI) által generált átlagos napi adatforgalom az interneten (2019-ben kb. 8.000 petabyte-nyi[27]), amely az arányosítás és az érzékelhetőség kedvéért megfelel a washingtoni Kongresszusi Könyvtár 40 000 000 kötetes könyvállománya kétszeresének. Nyilvánvaló módon ez a folyamatosan növekvő és többnyire értelmezhetetlen adatmennyiség egyrészt leterheli az adathordozó digitális rendszert, másrészt komoly mentális kihívást jelent az embereknek, hiszen az emberi elme nem képes ilyen mennyiségű és ilyen radikálisan gyorsan változó méretű és minőségű adattenger, külső benyomás (input) feldolgozására. Ennek a legérzékelhetőbb megnyilvánulása az elektronikus hírtengerben elvesző, összezavarodó és irányt vesztett emberek sokasága, illetve az emberiség felét elérő, a közösségi hálózatokon uralkodó álhírek, áltudományos babonaságok reneszánsza, amelyek nem kis társadalmi, politikai és biztonsági problémát jelentenek napjainkban. Internetbiztonsági szakemberek és társadalomtudósok megállapításai szerint aggasztó és komoly biztonsági kockázatot jelent a kibertérben kibontakozó korlátlan információs szabadosság és kontrollálatlan demokratizmus, amint azt R. Waltzman professzor, az amerikai Rand Corporation és védelmi technológiák kutatója is megállapította. A professzor eredményei szerint az utóbbi három évtized során az emberiség történetében egyedülálló és példátlan módon keletkezett és vált hozzáférhetővé óriási tudásbázis, és ezzel párhuzamosan még nagyobb mennyiségű rosszindulatú, káros információs tartalom is.[28] Az online digitális tartalmak vagy különféle kártevő programok előállításához és terjesztéséhez ma már csupán két dologra van szükség: egy hálózatra kapcsolható számítástechnikai eszközre és némi infokommunikációs ismeretre, illetve szoftverkezelési vagy programozási készségekre.

A Z, illetve alfa generáció több száz milliónyi tagja világszerte már az internet, avagy kiberkor szülötte, és jelentős részük rendelkezik a fent említett két alapfeltétellel a hackerré váláshoz. A Rand kutatói szerint az elmúlt évtized botrányos kibertéri eseményei megmutatták, hogy az információs tartomány túlságosan demokratizálódott, és az információ fegyverré alakult.[29]

Mindemellett, a rendszerrengető WikiLeaks[30] és Edward Snowden-féle[31] szivárogtatási és hírszerzési kémbotrányok óta sokan nagyon túlzóan úgy gondolják, hogy az internetes virtuális világot és kommunikációt komoly kormányzati felügyelet és ellenőrzés jellemzi, de ez csak részben helytálló megállapítás. Az Egyesült Államok, Kína, Nagy Britannia (valamint kisebb mértékben Oroszország) rendelkezik a legnagyobb, legkorszerűbb és legátfogóbb digitális adatforgalmat felügyelő és akár korlátozó személyi, tárgyi eszközökkel és képességekkel a világon[32], de még a technológiailag legfejlettebb nagyhatalmak sem képesek totális kontrollra

27 Statista 3.: https://www.statista.com/statistics/267202/global-data-volume-of-consumer-ip-traffic letöltés ideje: 2019. 12. 26.
28 Waltzman, R.: The Weaponization of Information. Rand Corp., Sta Monica, CA, 2017
29 Waltzman, i.m. 24
30 Ld. Leigh, D és Harding, L.: WikiLeaks-akták. Geopen, Budapest, 2011
31 Greenwald, Glen: A Snowden-ügy. HVG, Budapest, 2014.
32 Ld. Bruce Sussman összesítését a The Secured World-ben: https://www.secureworldexpo.com/industry-news/top-10-most-powerful-countries-in-cyberspace letöltés ideje: 2021. január 31.

a kibertér gigászi adatmennyisége és az internetes fizikai hálózat többcsomópontos sejthálózatszerű felépítése miatt.

A 2016-os amerikai elnökválasztásra is árnyakat vető külső befolyásolási botrányok, illetve az Európát megrendítő brit Brexit-népszavazás kimenetelét is kardinálisan befolyásoló kis adatelemző IT-cég, a *Cambridge Analytica*[33] esete rávilágított a közösségi hálózatok kontrollálatlan működési kockázatára és igencsak aggályos adathasználati gyakorlataira, amelyek mind puha fegyverként, egyfajta hatalmi politikai és kommunikációs eszközként *(soft power tools)*[34] is használhatóak. Mark Zuckerberg, a Facebook, a világ legismertebb online közösségi platformjának alapító vezérigazgatója a 2018. áprilisi amerikai kongresszusi meghallgatásán a hírhedt Cambridge Analytica és a Facebook vélt vagy valós üzleti kapcsolata révén maga is hangot adott aggodalmának és igényének a komolyabb és átláthatóbb kiberbiztonsági, adathasználati és személyiségi jogi szabályozás iránt.

A digitális írástudás és kultúra több szintű és típusú szakadékokkal szabdalt sajátosságokkal rendelkezik a világ lakossága körében. Egyrészt létezik a közismert digitális generációs szakadék, másrészt a világgazdaság széttöredezettségét is tükröző északi-déli vagy fejlett-fejlődő/fejletlen tengely mentén megfigyelhető Európa, Észak-Amerika és a Távol-Kelet szembenállása Afrikával, Dél-Amerikával, Dél-Ázsiával, amely tulajdonképpen párhuzamos világok, társadalmak egymásmellettiségét is jelenti.[35]

A 21. századi digitális technológiai civilizációjában élő emberek milliói számára a víz, élelem és üzemanyag mellett szinte elsődleges létszükségletté vált a megfelelő információhoz való hozzáférés joga és lehetősége, akárcsak a hozzáférhető adattömeg szűrésének, feldolgozásának és értelmezésének képessége. A sokat említett online platformok és közösségi médiaoldalak mögött álló internetes szolgáltatók, többnyire amerikai technológiai cégóriásoknak, mint a Facebook, Twitter, Amazon, Apple, Microsoft vagy Alphabet (a Google cégcsoport anyavállalata), minden eddiginél nagyobb szerepük és felelősségük van a hiteles, megbízható és leellenőrzött digitális adat- és információszolgáltatás terén. Mindazonáltal a világ legfontosabb adatkezelői és véleményformálói különféle jogi kiskapuk kihasználása és gazdasági megfontolások mentén mindezeknek a fenti elvárásoknak nem igazán tesznek eleget. Zuckerberg kényszerű kongresszusi szigorítási igényléséhez nemrég csatlakoztak brit és amerikai polgárok széles tömegei is. Egyrészt a közismert 2016-os Brexit-népszavazás és amerikai elnökválasztás körüli botrányok miatt és aztán különösképpen 2020 elején a koronavírus-világjárvány révén elszaporodó internetes trollok[36], konteók és álhírdömping miatt a britek és amerikaiak többsége szigorúbb adatkezelési, információmegosztási és internetes szolgáltatásokat ellenőrző és felügyelő jogszabályokat szeretnének, ha nem is globális joghatállyal, de legalább saját országaik kiberterében.[37]

33 Tom Warren: „The Cambridge Analytica Scandal" In The Verge April 2018.: https://www.theverge.com/2018/4/10/17165130/facebook-cambridge-analytica-scandal letöltés ideje: 2019. 12. 10.

34 Joseph S Nye hatalmi tipológiája szerint a kultúra, kommunikáció is a hatalmi erőkivetítés összetevője lehet, ld. Maxime Gomichon: Joseph Nye on Soft Power: E-International Relations. March 8, 2013

35 Khanna, Parag: Konnegtográfia. HVG, Budapest, 2017, 28–32.

36 Online közösségi oldalakon tevékenykedő fizetett véleményközlők, kommentelők

37 James Tapper: „Social Media Giants…" a The Guardianben: https://www.theguardian.com/technology/2020/apr/04/social-media-giants-must-tackle-trolls-or-face-charges-poll letöltés ideje: 2020. 04. 15.

A fent említett felfoghatatlan mennyiségű és gyakran ellentmondó információdömping, valamint a tudományos szűrők, úgynevezett kapuőrök visszahúzódása, az elektronikus médiaalanyok szerkesztőbizottságainak drasztikus csökkenése, illetve gyakran MI-alapú alkalmazásokkal való helyettesítése együttesen megteszik negatív hatásukat a felhasználók és online médiafogyasztók tömegeire. Ez a sajnálatos világtendencia jól kimutatható és megfigyelhető az utóbbi évtizedekben elvégzett médiatudatossági és szociálpszichológiai vizsgálatokban[38] az összeesküvés-elméletek és áltudományos hírportálok, különféle *influenszerek, vloggerek* befolyásának és a közösségi média tartalommegosztásainak vizsgálatakor. Olyan új, mondhatni kiberpszichológiai kifejezések, mint visszhangkamra *(echo-chamber)*, médiabuborék és kognitív disszonancia, vagyis saját magunk igazába és kényelmes, önigazoló előítéleteink valóságába vetett hit, a kibertérben élő és tevékenykedő felhasználók milliárdjainak alapvonásává vált napjainkra. A kibertérben terjedő kifejezetten rosszindulatú és károkozó programokkal, zsarolóvírusokkal párhuzamosan a 21. század eddigi legnagyobb globális egészségügyi és társadalmi kihívását jelentő koronavírus-járvánnyal kapcsolatban is az egekbe szöktek a változatos összeesküvés-elméletek, amelyekben például a vizsgált amerikai lakosság közel harmada hisz.[39]

Az alternatív valóságba és torz, áltudományos magyarázatokba vetett hit az online közösségi média globális elterjedésével soha nem tapasztalt lendületet kapott, természetesen, amint fentebb is olvashattuk, a világháló megálmodóinak eredeti magasztos elképzelésivel gyökeres ellentétben. A világhírű amerikai író és újságíró Mark Twainnek tulajdonított bölcsesség szerint, „amíg az igazság felveszi a csizmáját, addig a hazugság már kétszer megkerülte a földet".[40] A 19. század végén a távíró, telefon és bulvársajtó kezdeti korszakában és a világunkat átszövő kibertér előtt több mint egy évszázaddal, ez a szellemes kijelentés különösen kifinomult ember- és társadalomismeretre vall, amely sajnálatos módon napjainkban még hatványozottan érvényes. Mondanunk sem kell, hogy ez a globális jelenség, felvett emberi tulajdonság igen súlyos társadalmi és politikai biztonsági kockázatot jelent úgy az országok vezetése, mint az emberi közösségek fennmaradása, avagy szétforgácsolódása szempontjából. A szabadjára engedett adatforgalom és kontrolálatlan információmegosztás tekintetében, erkölcsfilozófiai szempontból olyan dilemma előtt állunk, mint amihez hasonlóval az amerikai atomfizikusok is szembesültek 1945 júliusában. A világháború során szupertitkos amerikai Manhattan-terv több vezető tudósa a magyar Szilárd Leó vezetésével az atombomba első bevetésének küszöbén, tudományetikai és általános erkölcsi aggályainak és fenntartásának adott hangot F. D. Roosevelt elnöknek címzett petíciójában. Ugyanis még nem tartották az emberiséget mentálisan és morálisan felkészültnek az atomenergia használatára, főleg nem háborús pusztító szándékból, polgári célpontok ellen.[41]

38 Krekó Péter: Tömegparanoia. Athaeneum, Budapest, 2018

39 Schaeffer, Katherine elemzése a FactTank-en : https://www.pewresearch.org/fact-tank/2020/04/08/nearly-three-in-ten-americans-believe-covid-19-was-made-in-a-lab/?utm_source=Pew+Research+Center&utm_campaign=9a8a1fc2a0-EMAIL_CAMPAIGN_2020_04_09_06_59&utm_medium=email&utm_term=0_3e953b9b70-9a8a1fc2a0-400906701 letöltés ideje: 2020. 04. 12.

40 Ld. Mark Twain idézetek: http://www.twainquotes.com/Lies.html letöltés ideje: 2020. 04. 12.

41 Szilárd Leó Petíciós levele: http://www.dannen.com/decision/45-07-17.html letöltés ideje: 2020. 04. 12.

Napjaink radikálisan átalakuló digitális ökoszisztémája is ehhez hasonló, ha nem nagyobb volumenű és még mélyrehatóbb tudományos-technológiai és szociálpszichológiai kihívást jelent az emberiség számára. Hiszen az atomenergia (és az atomfegyverek) felhasználásának célja és módja mindössze pár tucatnyi csúcs döntéshozó és szakember köré összpontosult a 2. világháború utolsó évében, akárcsak a hidegháború fél évszázada során is, miközben napjaink másodlagos virtuális univerzuma bárki számára hozzáférhető, és valós biztonsági szelepek, illetve korlátok nélküli alkalmazásmódot kínál jó és rossz célokra egyaránt. Gondoljunk csak a mesterséges intelligencia még feltáratlan lehetőségeire, illetve az emberi társadalmaink alapszükségleteit, biztonságát és fizikai létét meghatározó számítógépek vezérelte kritikus infrastruktúrák sebezhetőségére.

Ma már egyáltalán nem valóságtól elrugaszkodott fantazmagóriák körébe tartoznak az alábbi esetek: amikor például, egy fiatal erdélyi magyar hacker, narcisztikus kivagyiságtól vezérelve (avagy az orosz katonai titkosszolgálat jutalma fejében) pusztán egy notebook és középszintű informatikai szaktudás segítségével Aradról feltöri az amerikai külügyminiszter magánlevelezését és mobiltelefonját,[42] behatol egy hőerőmű vezérlőrendszerébe, amely több százezer ember energiaellátásáért felelős; akárcsak annak a 13 éves fiúnak az esete, aki a világhálón egy észtországi szigetről szélsőjobboldali terrorista sejtet szervezett az Egyesült Államokban ...[43]

A legendás Herbert Norman Schwarzkopf Jr. az amerikai hadsereg tábornoka 1991-ben az Öböl-háború előestéjén még mondhatta kissé ingerülten, hogy „egy istenverte laptoppal nem lehet háborúzni, csak golyókkal és bombákkal,"[44] ma már ez a kijelentés, amint tapasztalhatjuk, egyáltalán nem tartható, de már a 2003-as második Öböl-háború során sem bizonyult annak...

Robotok gyűrűjében, a szingularitás hajnalán?

„Ki mondja meg, hogy
miért Ma lesz a Holnap Tegnapja?"
Lord Alfred Tennyson, angol költő

A virtuális hálózatok és a mesterséges intelligencia jelentette biztonsági kihívások és nem utolsó sorban társadalmi problémák, morális aggályok egyre inkább meghatározzák a 21. század hétköznapjait. A mottóban feltett két évszázados költői, filozofikus kérdésre nincs válaszunk, akárcsak arra sem, hogy pontosan mire számíthatunk az elkövetkező évek, évtizedek során a felfoghatatlan léptékű technológiai fejlődés által kiváltott változások, események és jelenségek kapcsán. Az alábbi oldalakon áttekintjük az önjáró okos eszközök, robotok és a mesterséges intelligencia lehetséges kiteljesedési potenciálját, védelmi technológiai fejlesztési dimenzióit. Továbbá választ próbálunk találni arra a komplex tudományfilozófiai kérdésre, hogy mennyire lehet hasznos, illetve káros az emberiség számára a technológiai forradalom e szegmense.

42 Catalin Cimpanu: „Hacker Guccifer…". In Zero Day News. https://www.zdnet.com/article/hacker-guccifer-who-exposed-clinton-private-email-server-ready-for-us-prison-sentence/ letöltés ideje: 2020. 04. 14.

43 Deutsche Welle News: Far Right Terrorist Ringleader: https://www.dw.com/en/far-right-terrorist-ringleader-found-to-be-teenager-in-estonia/a-53085442 letöltés ideje: 2020. 04. 15.

44 Clarke – Knake: Cyber War. 2010, 19-21.

A 21. század generációi az internetalapú gyors, instant digitális megoldások világában élnek és szocializálódnak, illetve a szinte minden számítási és előjelzési problémára választ adó forradalmi kvantum-számítástechnika, és az öntanuló mesterséges intelligencia bűvkörében nőnek fel. Nyilvánvalóan a technológiai „varázslat" kezdeti időszakában, amely napjainkat is jellemzi, a felhasználók nem az árnyoldalakról és negatív tényezőkről fognak elsősorban gondolkodni, hiszen ez elsősorban az elemzők, és a társadalmi, biztonsági vonatkozásokra fogékonyabb szakértők feladata. Mindazonáltal a történelmi tapasztalat alapján kijelenthetjük, hogy minden eszköz vagy alkalmazás, amely alkalmas lehet akár destruktív célokra is, azt az emberek (államok) jelentős része gátlástalanul fel fogja használni klasszikus hobbesiánus (önérdekvezérelt) céljai elérése érdekében. Amint Waltzman professzor és társai megállapították, az információ és digitális megoldások militarizálása, fegyverré alakítása már évtizedek óta tartó jelenség, amelynek hatása alól nem lehet kivétel a kibertér sem (mint hadszíntér), vagy az emberszerű robotok *(cyborgs)*, illetve az őket irányító mesterséges intelligencia.[45] Különösképpen ez utóbbi igen sok nemzetközi vitára és aggodalmaskodó megnyilvánulásra adott okot, bár az elméleti vita, és az erről való futurológus gondolkodás jóval régebbi, mint gondolnánk.

A modern, digitális számítástechnika megszületésével párhuzamosan a 2. világháború vége felé néhány tudóst, különösképpen az angol Alan Turingot és a magyar–amerikai Neumann Jánost már a mesterséges (gépi) intelligencia kifejlesztésének gondolata kezdte foglalkoztatni. Azok az elméleti problémák (és fenntartások), amelyekről közel egy évszázaddal ezelőtt ők már elgondolkodtak, napjainkra egyre égetőbb és válaszra váró technológiai és tudományfilozófiai kérdésekké váltak. Mint például a gépi, avagy mesterséges intelligencia, amely 2020-ban már gépi tanulásra is képes, elérheti-e (sőt, akár túlszárnyalhatja-e) az emberi elme komplexitását és működési szintjét? Ha igen (és, miért ne történhetne ez meg?), kérdés, hogy mikor következik be a forradalmi „szingularitás pillanata" az emberiség történetében? Vajon igaza lesz a számítógép-tervező Neumann Jánosnak, illetve a sci-fi írással is foglalkozó amerikai matematikus kollégájának, Vernor Vinge-nek, akik már az 1950-es években a technológiai és az informatikai paradigmaváltásról – a bizonyos technológiai szingularitásról – értekeztek, amely, ha bekövetkezik, akkor szerintük az általunk ismert és megszokott történelem véget érhet…[46]

Ray Kurzweil, a népszerű amerikai jövőkutató mérnök szerint – aki nem mellesleg a Google első műszaki fejlesztési igazgatója volt, és a Szilícium-völgyi Szingularitás Kutatóegyetem társalapítója – a sokat emlegetett szingularitás, sőt akár az emberi és gépi elme összekapcsolódása *(HMI–human machine interface/interaction)* megállíthatatlanul közeledik, és várhatóan 2045 körül bekövetezik.[47] Meglátása szerint, amivel számos kutató egyetért, abban a történelmi momentumban bekövetkezik majd a MI nagy pillanata, felnőttéválása, és egyben elkezdődhet az „emberiség 2.0." időszaka is. Hogy ez az esemény jó vagy rossz lesz számunkra, nos, az már más kérdés, arról sokat kell és fogunk még tárgyalni, de Kurzweil egyértelműen az optimista, emberbarát MI-forgatókönyv elkötelezett híve…

45 Waltzman i.m. 28.

46 Vinge, Vernor: „Technological Singularity". In Whole Earth Review, January 2003. http://cmm.cenart.gob.mx/delanda/textos/tech_sing.pdf letöltés ideje:2020.04.05.

47 Reedy, Christianna: https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045 letöltés ideje:2020. 04. 15.

Tanulmányunk terjedelmi korlátai miatt nem fogunk technológiai részletekbe bocsátkozni az egyszerű és fejlett MI-ről *(advanced AI)*, illetve kifejlesztésének fázisairól, ugyanakkor röviden körbejárjuk azokat a biztonságpolitikai és társadalmi, szociálpszichológiai vonatkozásokat, amelyek a robotikával és a MI fejlődésével szoros összefüggésben állnak.

Közismertek és igen nagy visszhangra leltek az utóbbi években neves tudósok és technológiai újítók nyilvános kritikai észrevételei az úgynevezett emberhelyettesítő okos technológiák, elsősorban a mesterséges intelligencia és a robotika szédületes fejlődése vonatkozásában: a néhai Stephen Hawking világhírű brit fizikus és kozmológus, Martin Ford amerikai MI-kutató szociológus, illetve Elon Musk nagyvállalkozó, technológiai forradalmár szerint nem ajánlott, illetve kifejezetten veszélyes olyan technológiai megoldásokkal kísérletezgetni, amelyek egyrészt fegyverként is használhatóak és feltáratlan biztonsági kockázatokat rejtenek, másrészt tömeges alkalmazásukkal embermilliók munkáját vehetik el.[48] Musk, az önjáró autók (és űrrakéták) világszerte elismert gyártója meglehetősen kritikusan és ellenségesen viszonyul az önálló döntésekre is képes mesterséges intelligencia vezérelte gépekhez, egyenesen veszélyesebbnek tartja őket az emberiség biztonságára nézve, mint a tömegpusztító nukleáris fegyvereket.[49] 2015-ben az MI által vezérelt értelmes robotok katonai, támadó célra való felhasználása Elon Musk vezetésével ellen több mint száz hírneves tudós, globális technológiai vállalkozó közös kiáltványban is felemelte szavát, és aggodalmának adott hangot.[50]

Hasonló, bár akadémikusan kifinomultabb véleményt fogalmazott meg már jóval korábban Hawking professzor is, aki rávilágított arra az evolúciós ellentmondásra, miszerint egy törékeny, halandó testű ember korlátolt mentális képességeivel hogyan lesz képes vetélkedni egy „fémszövetű", és sokkal gyorsabb elméjű, tanulékonyabb mesterséges intelligenciájú robottal, *kiborggal*, még akkor is, ha saját alkotása, teremtménye elméletileg még akár tökéletesebbé is válhat emberi alkotójánál?[51] Hawking ugyancsak osztotta a brit állami kommunikációs és hírszerzési szervezet (GCHQ) vezetőjének véleményét, illetve Sir Berners Lee és Vinton Cerf „internetalapítók" aggodalmait a világháló biztonsági kockázatairól, amely kiberbűnözők globális fórumává alakult, és akár eltörpülhet majd az elszabaduló, avagy rosszra fordítható MI disztópikus világához képest. A sci-fi amerikai nagymestere Isaac Asimov és barátja John W. Campbell által már 1940-ben megálmodott és megszövegezett humanista robotika törvényei,[52] miszerint a robot nem árthat embernek, vagy nem fordulhat az alkotója ellen, sajnálatosan csak könyvben létező szabályok, és a valóságban teljességgel használhatatlanok és érvénytelenek. Mint a legtöbb forradalmi műszaki tudományos újítás, az okos, önjáró katonai (harci) eszközök és robotok is elsődlegesen a katonai védelmi technológiai szektor termékei, amelyeket az amerikai, orosz, kínai vagy izraeli hadmérnökök nem békés célokra terveznek már évtizedek óta.

48 Ford, Martin: i.m., 228

49 Catherine Clifford: „Musk: mark my word…" in CNBC.: https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-a-i-is-more-dangerous-than-nuclear-weapons.html letöltés ideje: 2020. 04. 15.

50 Gibbs, Samuel: „Elon Musk leads 116 experts calling for outright ban of killer robots". In The Guardian, 20 Aug 2017. https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-banlethal-autonomous-weapons-war letöltés ideje: 2019. 03. 11.

51 Rory Cellan-Jones: „Stephen Hawking warns A.I. could end mankind." In BBC https://www.bbc.com/news/technology-30290540 letöltés ideje: 2020. 04. 15.

52 Isaac Asimov: Én, a robot. Móra, Budapest, 1991

Putyin orosz elnök egy 2017-es tudományos diákkonferencián tett futurisztikus kijelentése bejárta a világot, miszerint „a 21. században a mesterséges intelligencia előtt óriási lehetőségek és veszélyforrások is állnak: ez a jövő nemcsak Oroszország, hanem minden állam számára (…) mindenesetre az az ország, amelynek sikerül uralnia az MI-t, uralhatja majd a nemzetközi kapcsolatok rendszerét is."[53] Természetesen erre a kijelentésre sok államfő és kutató felkapta a fejét, figyelembe véve azokat a tényeket, hogy az Orosz Föderáció kiberstratégiájának megfelelően a védelmi kiadási tételei között több különleges katonai projekt foglalkozik a robotika és mesterséges intelligencia szakirányú felhasználási módjaival[54], habár a titkosítások miatt nincsenek megbízható adatok az orosz védelmi kutatások mibenlétéről és fejlettségéről. Ugyanakkor sokatmondó volt a FEDOR nevű, az űrhajózásban alkalmazandó emberszerű orosz robot bemutatása a sajtónak 2017-ben, revolverrel a kezében…[55]

Az orosz MI- és robotika-kutatásokhoz képest az amerikai és kínai erőfeszítések valószínűleg jóval előrébb tartanak és magasabb szinten működnek, elsősorban a nyilvános eredmények és a befektetett anyagi erőforrások gigantikus mértékét tekintve. A kínai katonai technológiai és tudományos ambíciók nem kisebb célra törnek, minthogy 2030-ra Kína legyen a világ elsőszámú és legfejlettebb MI-gyártója és használója, megelőzve az Egyesült Államokat. Ehhez a grandiózus cél elérése érdekében évente mintegy 7-10 000 000 000 dollárt költenek a kínaiak, és Peking mellett felépült a világ legnagyobb, 55 hektáros MI-kutatóközpontja, több mint 2 000 000 000 dollárból, ahol több tízezer tudós, mérnök, informatikus a gépi tanulás *(deep/machine learning)* folyamatait, a mesterséges intelligencia, felhőszolgáltatások *(cloud computing services)* és a nagybani adatelemzés *(big data)* alkalmazási módjait kutatja.[56]

A kínai diktatórikus egypártrendszer politikai viszonyainak ismeretében komoly emberjogi és erkölcsi aggodalmakra ad okot az orwelli disztópiánál is szenvtelenebb kínai egyéni értékelési, úgynevezett Társadalmi Kreditrendszer *(Social Credit System)* bevezetése 2014-ben. A több mint 500 000 000 köztéri kamera segítségével és MI-alapú big data-elemző algoritmusok felhasználásával az eddig elvégzett 450 000 000 egyéni értékelés alapján 2020-ig már több mint 5 000 000 megbízhatatlan lojalitású kínai polgárt szűrt ki a rendszer a Kínai Kommunista Párt érdekei, és torz, emberi alapjogokat sértő biztonsági megfontolásai mentén.[57] Az így kiszűrtek sorsa igencsak kérdéses, illetve nehezen követhető, hiszen jogfosztott állampolgárokká váltak a világ legnépesebb és legnagyobb digitális kontroll alatt élő országában…

Teljességgel érthető, hogy az amerikai védelmi és nemzeti biztonsági stratégiában megfogalmazott célkitűzéseknek megfelelően nevesítik úgy a kiberhadviselés és a mesterséges intelligencia alkalmazási módjainak fontosságát, mint az ellenséges állami és állam alatti aktorok törekvéseinek visszaszorítását és ellensúlyozását.[58] Az Egyesült Államok, amely évente

53 James Vincent: „Putyin says on AI..." In The Verge.: https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world letöltés ideje: 2019. 12. 11.

54 Bilyanna Lilly- Joe Cheravitch: The Past, Present and Future of Russia's Cyber Strategy and Forces. NATO CCDCOE, Tallinn, 2020, 149

55 Ld. FEDOR orosz robot sajtótájékoztatója: https://nerdist.com/wp-content/uploads/2017/06/FEDOR-Feature-Image-06212017.jpg letöltés ideje: 2019. 03. 08.

56 Cyranoski, David: „China enters the batte for AI talent." In Nature, 15 January 2018. https://www.nature.com/articles/d41586-018-00604-6 letöltés ideje: 2019. 03. 07.

57 Nicole Kobie: „The complicated Truth about China's credit system". In Wired. https://www.wired.co.uk/article/china-social-credit-system-explained letöltés ideje: 2020. 04. 11.

58 US National Security Strategy, 2017 és National Defense Strategy of the U.S.,Washington D..C., 2018

összességében mintegy 100 000 000 000 dollár körüli rekordnagyságú összegben folytat kiterjedt kutatásokat ebben a vonatkozásban,[59] már Kínát tartja első számú gazdasági és katonai riválisának a szuperhatalmi státusért folytatott harcban, így a kiberhadviselés és a MI-kutatás terén is. Ezért az amerikai kormányzat minden lehetséges szövetségesével, elsősorban a NATO keretein belül keresi és elvárja a védelmi, kutatási együttműködést Kína és másodsorban Oroszország, továbbá egyéb kisebb, de veszélyes állami tényezők, mint Irán vagy Észak-Korea kiberfeltartoztatása *(cvber containment)* érdekében.[60] Chuck Hagel, egykori amerikai védelmi miniszter a *Third Offset Strategy* című stratégiai védelmi dokumentumról szóló előadásában 2014-ben kifejtette, hogy a 21. század meghatározó védelmi technológiái között első helyen állnak az okoseszköz-megoldások, különösképpen a mesterséges intelligenciát felölelő alkalmazások.[61] Értékelése szerint az Egyesült Államok, a világ legnagyobb tudományos technológiai kutatási szervezetén keresztül – amely nem más, mint a Pentagon intézményrendszere – pénzt és energiát nem kímélve folytat kutatásokat, hogy ezen a téren is megőrizze az amerikai stratégiai elsőséget és dominanciát. Az amerikai hardware-készítésben úttörő munkát végeznek a Boston Dynamics, Texas Instruments, Lockheed Martin, Boeing, Raytheon, Space X nevű óriás vállalatok, míg a mesterséges intelligencia és szoftverfejlesztésben élen járnak az MIT, NASA, Google, Apple, Microsoft kutatóközpontjai. Minden fontos tudományos technológiai szereplő tevékenységét tulajdonképpen meghatározza trendállító alapkutatásaival a Pentagon felügyelete alatt működő Fejlett Védelmi Kutatási Programok Ügynöksége, avagy az internet bölcsőjének is számító DARPA.

Az új idők új gyakorlatának beszédes adata, hogy közel egy évtized alatt már több önjáró légi harci jármű *(Unmanned Combat Aerial Vehicle)*, vagyis harci drónirányító „pilótája" *(Remotely Piloted Aircraft pilot)* van az amerikai légierőnek (közel 2000), mint valódi, aktív állományú harci pilótája (1700).[62] A nevadai sivatag konténer irányítóközpontjaiból vezérelt amerikai „égi figyelő szemek" *(eyes in the sky)*, mint az ikonikus *MQ-1 Predator, MQ-4 Global Hawk* vagy a rettegett *MQ-9 Reaper* önjáró repülőgépek a világ bármelyik pontján képesek megfigyelő vagy precíziós csapásmérő beavatkozó akciókat végrehajtani. Az Obama és Trump elnökök kormányzatának 12 éve alatt ugyanis pontosan ez történt, több mint kétezer alkalommal, Jemen, Szomália, Pakisztán, Afganisztán, Irak vagy Szíria célpontjai ellenében.[63]

A nagyhatalmi érdekérvényesítés területiuma természetesen kiterjed az új hadszíntérnek számító kibertérre is, sőt 2019 óta immár a világűrre is,[64] akárcsak az ezekkel szoros összefüggésben alkalmazandó robotikai és mesterséges intelligenciát használó megoldások, eszközök vonatkozásában egyaránt.

---

59 The National Artificial Intelligence Research and Development Strategic Plan. NSTC NITRD, October 2016. https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf letöltés ideje: 2020. 02. 28.

60 Yasmin Tadjdeh: „DoD seeks alliance to counter China and Russia." In: National Defense. https://www.nationaldefensemagazine.org/articles/2020/3/3/algorithmic-warfare-dod-seeks-ai-alliance-to-counter-china-russia letöltés ideje: 2020. 04. 16.

61 Chuck Hagel: A Game-changing third offset strategy. https://warontherocks.com/2014/11/a-game-changing-third-offset-strategy/ letöltés ideje: 2019. 11. 15.

62 „US Drone Milestone…" in The Military: https://www.military.com/daily-news/2017/03/08/drone-milestone-more-rpa-jobs-any-other-pilot-position.html letöltés ideje: 2019. 11. 25.

63 Bureau of Investigative Journalism: Obama's drone strikes. 2017. https://www.thebureauinvestigates.com/stories/2017-01-17/obamas-covert-drone-war-in-numbers-ten-times-more-strikes-than-bush letöltés ideje: 2019. 12. 29.

64 2019 dec. 20-án létrejött az űr hadszíntérért felelős US Space Force, mint a hatodik önálló amerikai haderőnem: https://www.spaceforce.mil/About-Us/Fact-Sheet letöltés ideje: 2020. 04. 15.

A légi és vízi drónok fejlődési trendjét, illetve az MI egyre erőteljesebb befolyását és komplexitását követve, számos katonai elemző felveti annak a potenciális forgatókönyvnek a biztonsági és morális kockázatát, amikor egy felderítő drón gépi elméje által talált és kielemzett (emberi vagy tárgyi) célpontot a szintén önjáró csapásmérő légi vagy vízi drón megsemmisíti, tulajdonképpen emberi beavatkozás nélkül.[65] A vezetési-irányítási és kommunikációs rendszer *(command-control, communication)* jelenlegi felépítése révén és a parancsnoki lánc hierarchiáját ismerve ez napjainkban még elképzelhetetlen lenne, de a tendenciákat követve a közeljövőben már egyáltalán nem lehet kizárni, amely jelentős paradigmaváltást eredményezhet a jogi és erkölcsi rendszerekben egyaránt.

A tisztán katonai vonatkozásoktól eltekintve a robotok és az önjáró, mesterségesintelligencia-alapú technológiai megoldások nyilvánvalóan társadalmi nyugtalanságot, ellenérzéseket, és egyben politikai felfordulást is eredményezhetnek. Az első számú komoly aggodalomra okot adó tényező a gépi intelligencia és az emberszerű okos robotok embert helyettesítő szerepe lehet. Számos szakértő és politikus egyetért az univerzális garantált munkabér bevezetésének vitatott gondolatával, amit többek között Martin Ford, a robotika témájának szociológus kutatója is támogat nagy hatású bestseller művében.[66] Érvelésük szerint ez a nagyon méltányos, egyedülálló szociális megoldás tudná megfelelően, de csak részben, orvosolni a milliószám munkanélkülivé váló emberek kilátástalan helyzetét a 21. század furcsa világában. Sőt, a római katolikus egyházfő, Ferenc pápa meglátása szerint a 2020-as koronavírus-járvány okozta globális gazdasági recesszió tömeges munkanélküliségi gondjait is talán ez a megoldás tudná a leghatékonyabban enyhíteni rövid- és középtávon.[67]

Amerikai munkaerő-piaci felmérések és szociológiai számítások szerint a fejlett világban (elsősorban az Egyesül Államokban és Kanadában) a mai munkahelyek és szakmák harmadát fenyegeti megszűnés, illetve a csak középfokú végzettséggel rendelkező felnőtt munkavállalók közel 60%-át az állásvesztés a gépi kihelyettesítés, automatizálás miatt a közeljövőben, ami soha nem látott feszültségeket, konfliktusokat, gazdasági és politikai válságot is előidézhet majd.[68]

Nem meglepő módon az 19. század eleji híres-hírhedt angol géppromboló luddita[69] követői két évszázad múltán újra népszerűségnek örvendenek, hiszen a neoluddita, „le az (energia) hálózatról, ki a modern társadalomból" *(off-the-grid, into the woods)* mozgalom követői több százezer főt számlálhatnak, elsősorban az Egyesült Államokban és Kanadában.[70]

A gyorsan változó és válságidőszakokkal tarkított világunkban technológiaellenes erőszakos, akár anarcho-terrorista jellegű fellépések egyáltalán nem kizárható események és jelenségek lesznek a jövőben, amennyiben a fenti pesszimista munkaerőpiaci és technológiai előrejelzések bekövetkeznek, továbbá, ha nem születnek ezekre kielégítő válaszok a vezetők részéről.

---

65 Porkoláb Imre: Digitális katona. TEDx Győr, 2019

66 Ford. i.m., 294

67 Cindy Wooden: „Pope on 'universal basic wage'" In CruxNow. April 2020. https://cruxnow.com/vatican/2020/04/pandemic-is-time-to-consider-universal-basic-wage-pope-says/ letöltés ideje: 2020.04.14.

68 Michael Webb: The Impact of AI on Labor Market. Stanford Univ. Pr., January 2020, 21 – 25.

69 Ned Ludd vagy Ludland kezdeményezésére (ha valóban létezett?), 1799 és 1817 között álarcos férfiak csoportjai rendszeresen szétverték a textilipari fonó- és szövőgépeket Angliában ld. Evan Andrews: Who were the Luddites? https://www.history.com/news/who-were-the-luddites letöltés ideje: 2020.04.02.

70 John Bartlett: „Will 2018 be the year of the neo-Luddites?" In The Guardian. https://www.theguardian.com/technology/2018/mar/04/will-2018-be-the-year-of-the-neo-luddite letöltés ideje:2020.04.16.

Mindazonáltal, a kockázatok és negatív vonatkozásokról nem elfeledkezve, a modern technológiák és a MI-alkalmazások egyáltalán nem ördögtől való találmányok, hiszen optimista és technológiabarát értelmezésben, mint amit a világhírű amerikai japán asztrofizikus Michio Kaku is képvisel, ezek a megoldások nagymértékben jobbá és könnyebbé teszik életünket, segítenek az univerzum titkainak tudományos feltárásában, a nanotechnológiás gyógyászat és számítástechnika egyéb vívmányairól már nem is beszélve.[71]

Záró gondolatok

A fentiekben láthattuk, hogy bár számos szegmensét áttekintettük a kibertéri digitális alkalmazások és a mesterséges intelligencia, illetve robotika emberi, társadalmi és biztonsági vonatkozásainak még számtalan témakör maradt érintetlenül a digitális ökoszisztémában, avagy kibermátrixban, amelyekről fontos lenne analitikus, kritikai észrevételeket tenni és mélyrehatató kutatásokat végezni. Ugyancsak figyelemre méltó és kutatásra érdemesült fontos téma napjainkban a közösségimédia-platformok és a dezinformációs kampányok, álhírek társadalomtorzító és akár demokráciát is veszélyeztető jelensége, amely állami és nem állami szereplők kezében komoly befolyásoló eszköz és akár puha fegyverként is értelmezhető.

Összegzésképp megállapíthatjuk, hogy a számítógépes rendszerek uralta kibertér hadszíntérré is alakult a 21. században, és a digitális információk ugyancsak fegyverként alkalmazhatóak állami és nem állami szereplők kezében politikai és egyéb célok érdekében. A könyv és papíralapú írásos kommunikáció és tudásközvetítés világa egy új paradigmaváltás keretében elektronikussá, digitálissá, virtuálissá vált, ahogy Neumann János vagy Isaac Asimov is elképzelte. Ugyanakkor az internetes tudás piactér világa nem igazán úgy alakult az utóbbi három évtized folyamán, mint ahogy tudós megálmodói jó szándékú, idealista módon elképzelték. A történelmi tapasztalat és az antropológiai pesszimizmus alapján kijelenthetjük, hogy az emberi alapvonásnak megfelelően szinte minden kimagasló technológiai találmány hadászati, védelmi, illetve támadó, pusztító célra került felhasználásra. Természetesen így van ez a gépi vagy fejlett mesterséges intelligencia és a robotika terén is, amely nemcsak a hadviselést fogja forradalmasítani, hanem hétköznapjainkat, a munkaerőpiacot és az emberi civilizációnkat is, ahogy Neumann János vagy Ray Kurzweil is kifejtette.

A fent említett tudós szakértők véleménye alapján, és Hawking professzor aggodalmaiban osztozva kijelenthetjük, hogy az emberiség nincs felkészülve a „túlfejlett mesterséges intelligencia" jelentette kihívásokra, és főleg nem katonai célra való alkalmazására, amely beláthatatlan kockázatokat hordozhat, még a nukleáris fegyvereknél is nagyobb mértékben, ezért az ENSZ közgyűlésének is elítélő állásfoglalást kellene nyilvánítania a gyilkos robotok *(killbot)* rendszerbe állítása ellen. Ugyancsak ebben a vonatkozásban nagy sajtóvisszhangot kapott az amerikai védelmi minisztérium és a Google közös MI-alapú robottechnológia- kutatási botránya a „gyilkos okos eszközök, robotok" morális és biztonsági kockázatai miatt.[72]

71 Michio Kaku: Az emberiség jövője. Akkord, Budapest, 2019, 110–126.

72 Henry McDonald: „Ex Google-worker fears…" In The Guardian. Sept.,2019 https://www.theguardian.com/technology/2019/sep/15/ex-google-worker-fears-killer-robots-cause-mass-atrocities letöltés ideje: 2019. 12. 04.

Amint az internet atyjai is keserűen megjegyezték, az információs szupersztráda és a rá települő kibertér sajnálatosan többnyire negatív, káros és destruktív tartalmakkal töltődött fel, és a kiberbűnözés néhány év alatt az első számú és legnagyobb kárt okozó bűncselekménytípussá vált a világon. Úgy tűnik, még a koronavírus pusztító világjárványa idején sem pihennek a bűnözői csoportok, akik még ebben az emberpróbáló időszakban is hihetetlen módon zsarolóvírus programokkal támadják a biológiai kutatólaboratóriumokat és kórházakat.[73]

A digitális mediatizáció világméretű tendenciáját tekintve ugyancsak ellentmondásos a közösségimédia-felületek, a multimédiás információmegosztó alkalmazások dominanciája és a *vlogger* influenszerek befolyása, amelyek abszolút elsődleges információforrásokká váltak, akár az iskola és családi közeg ellenében a kiberkor Z és Alfa generációi számára.[74] Az emberi elme számára felfoghatatlan és követhetetlen mértékben és mennyiségben keletkezik új digitális információ nap mint nap, amely még inkább megnehezíti a tájékozódást a felhasználók számára. Mindez lélektani szempontból gyakran zavarodottsághoz, dezinformációhoz, egyéni és kollektív frusztrációhoz, valamint elidegenedéshez, illetve virtuális visszhangkamrák kényelmes és torz világához vezethet, amelyek akár a társadalmi békét és politikai rendet is veszélyeztethetik.

A kibertéri alkalmazások és a gépi intelligencia fejlődése megállíthatatlannak tűnik, amelyek már önmagukban *per se* hordoznak biztonsági kockázatokat, nem beszélve az eleve rossz szándékú technológiahasználókról, akiknek a számarányáról csak becsléseink vannak, pontos adatok, kimutatások nem igazán állnak rendelkezésre.

Nassim N. Taleb, világhírű amerikai filozófusprofesszor és kockázatelemező értékelése szerint a technológiai komplexitás és a számtalan társadalmi és természeti változó, ismeretlen tényező következtében a jövőben egyre több ismeretlen, előre nem jelezhető világméretű válsággal (úgynevezett „fekete hattyú" jelenséggel), vagy lekicsinyelt, és valószerűtlennek tartott biztonsági kihívással, problémával („szürke hattyú") kell majd megbirkóznunk.[75] Legyen az biológiai eredetű világjárvány (koronavírus), kisbolygó-becsapódás, egy átfogó regionális vagy kontinentális áramszünet, nem beszélve a sokkal valószerűbb, pusztító kiberbűncselekmények elszaporodásáról vagy a mesterséges intelligencia közelgő szingularitásáról és annak ma még beláthatatlan következményeiről…

Az egyik legnehezebb kihívás az emberiség számára a tanulmányban felvázolt technológiai csapdából való kiút és felhasználóbarát megoldás megtalálása, amelyre leegyszerűsítve két fő opció létezik. Egyrészt technológiai hozzáférés korlátozása vagy teljes tiltás révén, amely diktatórikus és kontraproduktív rossz megoldási mód, másrészt letisztult és szigorú jogi keretrendszer kidolgozásával a kibertérben működő digitális médiaszolgáltatókra és gépiintelligencia-alkalmazásokra a felhasználók és univerzális emberi értékek és érdekek védelmében, amelyet kiegészít a kiberbiztonsági felvilágosítás, médiatudatos és kritikai gondolkodásra, illetve netetikettre való felkészítés a formális iskolai és digitális oktatás keretei között.

73 Ld. https://healthitsecurity.com/news/560-healthcare-providers-fell-victim-to-ransomware-attacks-in-2020 letöltés ideje: 2021. 02. 01.

74 Greg Jarboe: „Generation Z can't live without YouTube". In Tubular Insights, June, 2017. https://tubularinsights.com/generation-z-youtube/ letöltés ideje: 2020. 04. 16.

75 Taleb, N.N.: The Black Swan. New York, Random House, 2010, 189–195.

Megállapíthatjuk, hogy a kritikai és analitikus gondolkodás oktatásával és gyakorlati alkalmazásával számos kiberbiztonsági és társadalmi probléma könnyen és hatékonyan orvosolható lehet a társadalom széles tömegei körében. Mindehhez azonban szükséges a mértéktartó racionalitás alkalmazása a döntéshozók és a felhasználók részéről, valamint a célok (például humánus társadalmi, tudományos fejlődés) elkülönítése és nem felcserélése az eszközökkel (digitális technológiák, robotika, MI), hogy elkerülhetővé váljon Einstein és Bertrand Russell profetikus megállapítása, miszerint az okos technológia világa elbutult, elkényelmesedett emberiséghez vezethet…

Irodalomjegyzék

1. Asimov, Isaac: „Visit to the World Fair of 2014". In *The New York Times*, August 16, 1964. http://www.nytimes.com/books/97/03/23/lifetimes/asi-v-fair.html letöltés ideje: 2019. 12. 02.
2. Asimov, Isaac: *Én, a robot.* Móra, Budapest, 1991.
3. Andrews, Evan: *Who were the Luddites?* https://www.history.com/news/who-were-the-luddites letöltés ideje: 2020. 04. 02.
4. Bartlett, Jamie: „Will 2018 be the year of the neo-Luddites?" In *The Guardian.* https://www.theguardian.com/technology/2018/mar/04/will-2018-be-the-year-of-the-neo-luddite letöltés ideje: 2020. 04. 16.
5. Blank, Stephen: *Web War I: Is Europe's First Information War is a New kind of War?* https://www.tandfonline.com/doi/full/10.1080/01495930802185312 letöltés ideje: 2020. 01. 12.
6. Brent, Laura: „NATO's role in cyberspace".In NATO *Review*, Febr., 2019 https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html letöltés ideje: 2019. 12. 29.
7. Bureau of Investigative Journalism: *Obama's drone strikes.* https://www.thebureauinvestigates.com/stories/2017-01-17/obamas-covert-drone-war-in-numbers-ten-times-more-strikes-than-bush letöltés ideje: 2019. 12. 29.
8. Carr, Nicholas: *The Shallows: What the Internet is doing to our Brains.* W. Norton, New York, 2011.
9. Chen, Hsinchun: *Dark Web: Exploring and Data Mining the Dark Side of the Web.* Springer, New York, 2012.
10. Clifford, Catherine: „Musk: mark my word…". In *CNBC.* https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-a-i-is-more-dangerous-than-nuclear-weapons.html letöltés ideje: 2020. 03. 19.
11. Cimpanu, Catalin: „Hacker Guccifer…". In *Zero Day News.* https://www.zdnet.com/article/hacker-guccifer-who-exposed-clinton-private-email-server-ready-for-us-prison-sentence/ letöltés ideje: 2020. 04. 14.
12. Clarke, Richard A.; Knake, Robert K.: *Cyber War: The Next Threat to National Security and What to Do About It.* Harper Collins, New York, 2010.

13. Cyranoski, David: „China enters the batte for AI talent." In *Nature*, 15 January 2018. https://www.nature.com/articles/d41586-018-00604-6 letöltés ideje: 2019. 03. 07.
14. Deutsche Welle English News: *Far Right Terrorist Ringleader.* https://www.dw.com/en/far-right-terrorist-ringleader-found-to-be-teenager-in-estonia/a-53085442 letöltés ideje: 2020. 04. 15.
15. Esteves, Olivier: „Bertrand Russell: the utilitarian pacifist". In *French Journal of British Studies.* XX-1/2015 https://journals.openedition.org/rfcb/308 letöltés ideje: 2020. 03. 25.
16. Galeon, Dom; Reedy, Christianna: „Kurzweil Claims That the Singularity Will Happen by 2045". In *Futurism*, 5 October 2017. https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045/ letöltés: 2019. 12. 22.
17. Gibbs, Samuel: „Elon Musk leads 116 experts calling for outright ban of killer robots". In *The Guardian*, 20. August 2017. https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-banlethal-autonomous-weapons-war letöltés: 2019. 11. 10.
18. Gibson, William: „*Cyberspace*" In *Technovelgy* online sci-fi magazine. http://www.technovelgy.com/ct/content.asp?Bnum=53 letöltés ideje: 2019. 12. 25.
19. Gomichon, Maxime: *Joseph Nye on Soft Power.* E-International Relations. March 8, 2013
20. Hagel, Chuck: *A Game-changing third offset strategy.* https://warontherocks.com/2014/11/a-game-changing-third-offset-strategy/ letöltés ideje: 2019. 11. 15.
21. Haig Zsolt: *Információs műveletek a kibertérben.* Dialóg Campus, Budapest, 2018
22. Haig Zsolt – Kovács László: „Fenyegetések a cybertérből". *Nemzet és Biztonság,* 2008/5., 63.
23. Haizler, Omry: „The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking". In *Cyber, Intelligence, and Security.* Vol.1. No.1.,| January, 2017.
24. Harari, Yuwal: *Homo Deus – a holnap rövid története.* Animus, Budapest, 2017
25. Häußler, Ulf: *Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO's Treaty*, https://www.sbs.ox.ac.uk/cybersecuritycapacity. letöltés ideje: 2020. 01. 10.
26. Ford, Martin: *Robotok Kora.* HVG Könyvek, Budapest, 2016.
27. Greenwald, Glen: *A Snowden-ügy.* HVG Könyvek, Budapest, 2014.
28. Jarboe, Greg: „Generation Z can't live without YouTube". In *Tubular Insights*, June, 2017. https://tubularinsights.com/generation-z-youtube/ letöltés ideje: 2020. 04. 16.
29. Jones, Rory Cellan: „S. Hawking warns A.I. could end mankind." In BBC https://www.bbc.com/news/technology-30290540 letöltés ideje: 2020. 04. 15.
30. Kaczysnki, Ted: „The Unabomber Manifesto". In *Washington Post Special Edition Sept.,22, 1995:* https://www.washingtonpost.com/wp-srv/national/longterm/unabomber/manifesto.text.htm letöltés ideje: 2020. 04. 11.
31. Michio Kaku: *Az emberiség jövője.* Akkord, Budapest, 2019.
32. Kaplan, Jerry: *Artificial Intelligence: What Everyone Needs to Know.* Oxford University Press, New York, 2016.
33. Khanna, P.: *Konnektográfia.* HVG, Budapest, 2017.

34. Kobie, Nicole: „The complicated Truth about China's social credit system". In *Wired*. https://www.wired.co.uk/article/china-social-credit-system-explained letöltés ideje: 2020. 04. 11.
35. Krekó Péter: *Tömegparanoia.* Athaeneum, Budapest, 2018.
36. Krekó Péter: „Netes konteók" In Index TNT Podcast: https://index.hu/techtud/2020/04/12/tnt_osszeeskuves_kreko_peter_podcast/ letöltés ideje: 2020. 04. 12.
37. Lilly, Bilyanna - Joe Cheravitch: *The Past, Present and Future of Russia's Cyber Strategy and Forces.* NATO CCDCOE, Tallinn, 2020, 149
38. Leigh, D; Harding, L.: *WikiLeaks-akták.* Geopen, Budapest, 2011Mazarr, Michael J., Ryan
39. Michael Bauer, Abigail Casey, Sarah Heintz, Luke J. Matthews: *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment.* Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR2714.html. letöltés ideje: 2020. 03. 10.
40. Military: „US Drone Milestone…" in *The Military:* https://www.military.com/daily-news/2017/03/08/drone-milestone-more-rpa-jobs-any-other-pilot-position.html letöltés ideje: 2019. 11. 25.
41. Molander, Roger C., Andrew Riddile, Peter A. Wilson: *Strategic Information Warfare: A New Face of War.* Santa Monica, CA: RAND Corporation, 1996. https://www.rand.org/pubs/monograph_reports/MR661.html. letöltés ideje: 2020. 03. 11.
42. Munk Sándor: „A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései." *Hadtudomány,* 2018/1.
43. Newton, Casey: „Lessons from Zuckerberg's Senate Hearing" https://www.theverge.com/2018/4/10/17222444/mark-zuckerberg-senate-hearing-highlights-cambridge-analytica letöltés ideje: 2019. 12. 10.
44. NSTC NITRD: *The National Artificial Intelligence Research and Development Strategic Plan.* October 2016. https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf letöltés ideje: 2020. 02. 28.
45. Porkoláb Imre: *Digitális katona.* TEDX Győr, 2019.
46. Póti László (szerk.): *Nemzetközi Biztonsági Tanulmányok.* Zrínyi, Budapest. 2006.
47. Reedy, Christianna: „Kurzweil on Singularity". In *Futurism.* https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045 letöltés ideje:2020.04.15.
48. Schaeffer, Katherine: „COVID-19 origins." In *FactTank:* https://www.pewresearch.org/fact-tank/2020/04/08/nearly-three-in-ten-americans-believe-covid-19-was-made-in-a-lab/?utm_source=Pew+Research+Center&utm_campaign=9a8a1fc2a0-EMAIL_CAMPAIGN_2020_04_09_06_59&utm_medium=email&utm_term=0_3e953b9b70-9a8a1fc2a0-400906701 letöltés ideje: 2020. 04. 12.
49. Statista 1: https://www.statista.com/topics/1145/internet-usage-worldwide/ letöltés ideje: 2020. 01. 15.
50. Statista 2.: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide letöltés ideje: 2020. 01. 28.

51. Statista 3.: *Data volume of global consumer IP traffic from 2015 to 2021*. https://www.statista.com/statistics/267202/global-data-volume-of-consumer-ip-traffic letöltés ideje: 2019. 12. 26.
52. Strauss, Leo; Cropsey, Joseph: *A politikai filozófia története I.* Európa, Budapest, 1994.
53. Szilárd Leó: *Petíciós levél Roosevelt elnökhöz.* Washington D.C. http://www.dannen.com/decision/45-07-17.html letöltés ideje: 2020. 04. 12.
54. O'Neill, Patrick Howell: „The cyberattack that changed the world". In *The Daily Dot.* 2016. https://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/ letöltés: 2019. 10. 08.
55. Tadjdeh, Yasmin: „DoD seeks alliance to counter China and Russia." In: *National Defense.* https://www.nationaldefensemagazine.org/articles/2020/3/3/algorithmic-warfare-dod-seeks-ai-alliance-to-counter-china-russia letöltés ideje: 2020. 04. 16.Taleb, N. Nicholas: The Black Swan. Random House, New York, 2010.
56. Toonders, Joris: „Data Is the New Oil of the Digital Economy". In *Wired.* July 2014. https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ letöltés ideje: 2020. 01. 25.
57. Vinge, Vernor: „Technological Singularity". In *Whole Earth Review,* January 2003. http://cmm.cenart.gob.mx/delanda/textos/tech_sing.pdf letöltés ideje: 2019. 12. 21.
58. Vincent, James: „Putyin says on AI..." In *The Verge.*: https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world letöltés ideje: 2019. 12. 11.
59. Waltzman, R.: *The Weaponization of Information.* Rand Corp., Santa Monica, CA, 2017
60. Warren, Tom: „The Cambridge Analytica Scandal" In *The Verge.* April 2018.: https://www.theverge.com/2018/4/10/17165130/facebook-cambridge-analytica-scandal letöltés ideje: 2019. 12. 10.
61. Webb, Michael: T*he Impact of AI on Labor Market.* Stanford Univ. Pr., January 2020
62. Wooden, Cindy: „Pope on 'universal basic wage'" In *CruxNow.* April 2020. https://cruxnow.com/vatican/2020/04/pandemic-is-time-to-consider-universal-basic-wage-pope-says/ letöltés ideje: 2020. 04. 14.

Drabancz Áron – El-Meouch Nedim Márton

A kibertér jövője, avagy az állami kibervédelem vizsgálata elméleti modellkeretben

Rezümé

A tanulmány bemutatja, hogy a technológiai fejlődés miként ágyazott meg a kiberhadviselés nagyfokú terjedésének. Optimalizációs modellkeretben rámutattunk arra, hogy az államok jövőbeli kiberaktivitása erőteljesen növekedhet (Nash-egyensúly), egyre távolabb kerülve a jóléti optimumot nyújtó pacifizmustól. Kellően nagy és koordinált globális szankciók bevezetése esetén lehetne az országok kiberaktivitását csökkenteni, azonban ennek kivitelezhetősége kérdéses.

Resume

The study shows how technological advances have embedded the high prevalence of cyber warfare. In an optimization model framework, we pointed out that the future cyber activity of states may increase strongly (Nash equilibrium), moving further and further away from the pacifism that provides the welfare optimum. The introduction of sufficiently large and coordinated global sanctions could reduce countries' cyber activity, but its feasibility is questionable.

Vezetői összefoglaló

A számítási kapacitás, a dolgok internete, illetve a mesterséges intelligencia terén lezajló technológiai fejlődés miatt a kiberhadviselés az egyik legjelentősebb új hadviselési formává vált. Optimalizációs modellkeretünk alapján a kiberaktivitás, s az ebből fakadó jóléti veszteség nagysága a jövőben még tovább emelkedhet, és csak kellően nagy és koordinált globális szankciók bevezetése esetén lenne esély a folyamat erőteljes lassítására.

„War is no longer declared, only continued"
Ingeborg Bachmann

Bevezetés

A második világháborúban megjelenő elsőgenerációs számítógépek töretlen fejlődésen mentek keresztül napjainkig: a korábban ormótlan, szobákat elfoglaló, lassú gépek napjainkra mindenki számára elérhető gyors, olcsó gépekké váltak, melyek alapvetően határozzák meg a világ képét. A számítási teljesítmény növekedése, illetve a szoftverek fejlődése mára lehetővé teszi, hogy a számítógépek korábban elképzelhetetlen területeken is egyre jelentősebb szerepet töltsenek be: a mobilitás alapstruktúráját változtathatják meg a jövőben várhatóan megjelenő teljes önvezetőképességgel rendelkező járművek, a munkafolyamatokat írhatják át a mesterséges intelligencián alapuló legújabb optimalizációs eljárások, melyek a monoton, jól strukturált feladatok kapcsán egyre kevésbé kívánják majd meg az emberek jelenlétét. A fegyveres erők számára is egyre fontosabb a technológia jelentősége: az Amerikai Egyesült Államok haderejében ma már részben önvezető drónok cikáznak külföldi légterekben[1], illetve a korábbi évek műholdképei és időjárási adatai alapján mesterséges intelligencia segítségével meg lehet becsülni, hogy mely térségekben várható aszály, szélsőséges időjárás és emiatt esetleg turbulens politikai helyzet.[2]

A tevékenységek digitalizációja a jövőben még tovább gyorsulhat: a Moore-törvény alapján az integrált áramkörök összetettsége továbbra is körülbelül 18-24 hónaponta megduplázódik[3], az adatokat szolgáltató érzékelők száma exponenciálisan növekszik[4], továbbá a Google 2019-ben bejelentette a kvantumfölényt, azaz olyan kvantumszámítógépet épített, melynek a képességei a klasszikus számítástechnika legfelső határait messze meghaladja.[5]

A technológiai változások miatt más országok adatainak megszerzése vagy manipulálása jelentős hatalmat ad a birtokló kezébe. A helyzet fokozódását mutatja, hogy egyre több kibertámadást hajtanak végre a világon, egyre többféle célpont ellen, s mára a kormányzati intézmények mellett a kulcsfontosságú infrastruktúra és technológia is a támadók célpontjává vált. A nemzetközi szabályozások hiánya, illetve a támadások visszafejtésének nehézségei miatt még a komolyabb kibertámadások se tekinthetők legtöbbször háborús cselekménynek, inkább szürke zónának kezeli azt a nemzetközi közösség, mely a (klasszikus) háború küszöbértéke alatt marad.[6]

Tézisünk szerint a jövőben a kibertér mint harcászati tér aktivitása és az általa kiváltott károk nagysága is növekedni fog, így a kiberhadviselés problémája globális szempontból – a globális összjóléthez egyre negatívabb hozzájárulása miatt – egyre fontosabbá válhat. A tézis bizonyítására először röviden körüljárjuk, hogy a világ digitalizálódása, illetve az adatközpontúság

1 Gilmore, C. K. – Chaykowsky, M. – Thomas, B. (2019): Autonomous Unmanned Aerial Vehicles for Blood Delivery: A UAV Fleet Design Tool and Case Study. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR3047.html (2020. június 15.)

2 Descartes Lab (2020): https://www.descarteslabs.com/#overview (2020. június 15.)

3 Takahashi, D. (2017): https://venturebeat.com/2017/03/28/intel-moores-law-isnt-slowing-down/ (2020. június 15.)

4 Dahlqvist, F. – Mark Patel, M. – Alexander Rajko, A. – Shulman, J. (2019): Growing opportunities in the Internet of Things. https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things# (2020. június 15.)

5 Szepesi, A. (2019): Holnaptól borul a fél világ? Mit jelent a kvantumfölény, mire számíthatunk ezután? https://hvg.hu/tudomany/20191028_google_sycamore_kvantumfoleny_jelentese_hogyan_mukodik_kvantumszamitogep_mukodese_egyszeruen_qubit_kubit_ibm_summit_szuperszamitogep (2020. június 15.)

6 Porche, I. R. III (2019): Fighting and Winning the Undeclared Cyber War. https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html (2020. június 15.)

erősödése milyen technológiai, gazdasági és társadalmi folyamatokra vezethető vissza, és ezek a jövőben miképpen kellene, hogy megváltoztassák a társadalmak, illetve a kormányzat hozzáállását az adatok védelméhez. Ezt követően egy dinamikus optimalizációs modellkeretben becsüljük meg, hogy az elektronikus eszközök növekvő száma, és egyre kiemeltebb jelentősége miként nehezítheti meg a kormányzat számára az adataink védelmét. A 2. fejezetben ismertetjük a kérdéshez kapcsolódó főbb technológia trendeket, ezt követően a 3. fejezetben a kiberhadviseléshez kapcsolódó fontosabb fogalmakat mutatjuk be. A 4. fejezetben a dinamikus optimalizációs modellkeret elemei, illetve a különböző szcenáriók melletti eredmények kerülnek bemutatásra. A záró fejezetben összegezzük a tanulmány eredményeit, rámutatunk azok limitációira, illetve továbblépési irányokat fogalmazunk meg a téma kapcsán.

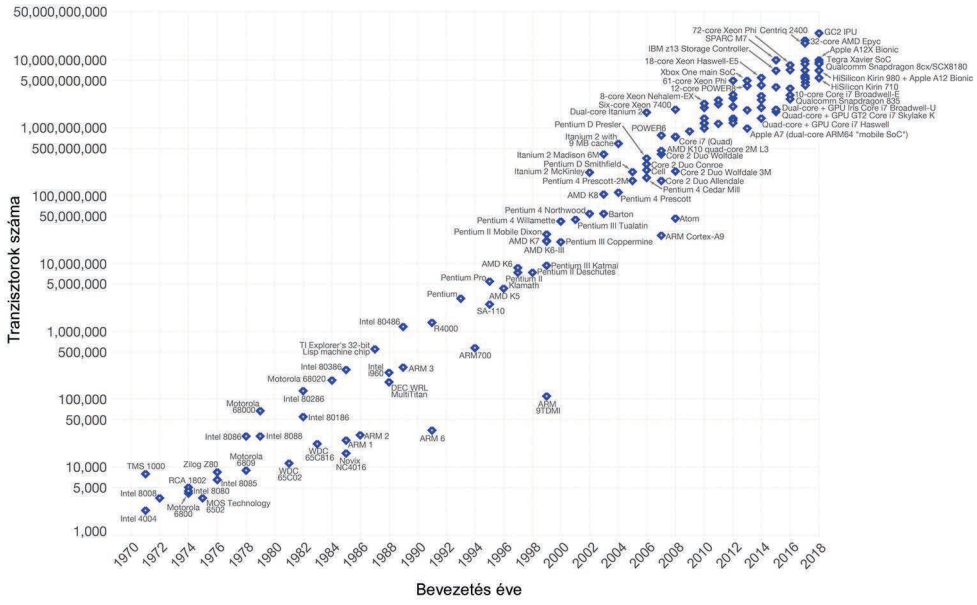
Technológiai fejlődés

A technológiai fejlődéssel kapcsolatban azt a résztézist járjuk körül, hogy az elmúlt évtizedek dinamikus technológiai fejlesztései miatt a számítógépek mára nagy mennyiségű strukturálatlan adatokat képesek egyszerre feldolgozni, mely alapjaiban ágyaz meg az online hadviselés terjedésének. Egyrészt növekedett a számítógépek számítási kapacitása, másrészt egyre több eszköz szolgáltat digitális adatot, illetve az adatok feldolgozásában is egyre inkább előrehaladott a technológia. Ezen három tényező egymással párhuzamos fejlődése miatt mára korábban felfoghatatlanul nehéz feladatok megoldása került látható távolságba. A fejezet célja röviden bemutatni a három tényező elmúlt években tapasztalt fejlődését és a lehetséges jövőbeli folyamatokat.

Számítási kapacitás

A számítógépek számítási kapacitásának növekedése kapcsán a Moore-törvényt érdemes mindenképp megemlíteni. A törvény alapján az integrált áramkörök összetettsége 18-24 hónaponként megduplázódik, vagyis az 1000 dollárért vásárolható számítási teljesítmény 1,5-2 évenként duplájára nő. A törvény az elmúlt évtizedekben alapvetően fennállt (lásd 1. ábra), amely kimagasló fejlődést jelent a számítási kapacitás terén. Ezt egy szemléletes példával érzékeltetve, amennyiben 1920-ban csupán 2 dollárt fektetünk volna be, és a befektetésünk hozama a Moore-törvény szerint alakul, akkor 2014-ben a befektetésünk értéke nagyjából a világ GDP-jének felelne meg, mára pedig már 16-szor nagyobb lenne.[7] A példa jól rámutat arra, hogy a legutolsó években lezajló duplázódások egy relatíve magas kapacitásszint mellett mentek már végbe, így az itteni ugrások igazán jelentősnek tekinthetők.

7 Saját számítás az IMF (2020): https://www.imf.org/external/index.htm (2020. június 15.) adatai alapján.



1. ábra: A tranzisztorok számának növekedése 1970–2018.
(Forrás: Our World in data (2020)

Internet of Things

Ezzel párhuzamosan a lényegi információt felismerni képes, azt egy internetalapú hálózaton egy másik eszközzel megosztani tudó eszközök (dolgok internetje = Internet of Things = IoT) száma is jelentősen növekszik a világban. A testünkön viselhető eszközök (pl. okosóra), a lakásunkban elhelyezett szenzorok (pl. okosotthon érzékelői), illetve az egyre kisebb ipari eszközök valós idejű nyomon követése mind egyre több adatot generál a kibertérben. A technológia alapja az RFID, mely rádiófrekvenciás elektromágneses mezőt használ, hogy adatokat továbbítson az RFID-olvasóba. A csökkenő árak lehetővé teszik, hogy egyre több és több eszköz rendelkezzen érzékelőkkel, „okosodjon fel" és kapcsolódjon össze az interneten keresztül. Az Ericsson (2016) elemzése szerint 2016 és 2022 között évente 21%-kal növekedhet az IoT eszközök száma, 2022-ben közel 30 milliárd csatlakoztatott eszköz lehet a világon.[8] A Business Insider (2019) riportja alapján a növekedés még jelentősebb lehet, ők elemzésükben 64 milliárdra becsülik az IoT-eszközök számát 2025-re.[9] Az eszközök terjedését segítheti az 5G-hálózat 2020-as években történő kiépítése, mely az adatátviteli sebesség, hatékonyság, megbízhatóság, kapacitás és biztonság terén is jelentős előrelépésnek ígérkezik, így várhatóan új lehetőségeket nyit az IoT-eszközök számára. Az eszközök számának, illetve a továbbított

8 Ericsson (2016): Ericsson Mobility Report (2016 November) – on the pulse of the networked society. https://www.ericsson.com/en/mobility-report/reports (2020. június 15.)

9 Business Insider (2019): IoT Report: How Internet of Things technology growth is reaching mainstream companies and consumers. https://www.businessinsider.com/internet-of-things-report (2020. június 15.)

adatok mennyiségének jelentős növekedése miatt már ma is gyakran felmerülő kérdés az adatok biztonsága, a hálózatok és eszközök esetleges sebezhetősége az internetes támadásokkal szemben.

Mesterséges intelligencia

A különböző eszközök által előállított tömérdek adatmennyiség és a számítógépek számítási kapacitásának exponenciális növekedése önmagában nem elég ahhoz, hogy a rendelkezésre álló adatokból minőségi információt lehessen kiszűrni, harmadik összetevőként a mesterséges intelligenciához, gépi tanuláshoz tartozó algoritmusokra is szükség van. A mesterséges intelligencia kutatása már az 1950-es években elkezdődött, de a kezdeti fellendülés után a 20. század második felére megakadt a fejlődés, melyet a szakirodalom a *mesterséges intelligencia telének* nevez. Emögött okként pont azon tényezők fejlődésének megakadása áll, melyek a 2010-es években újraéledő, és újult erővel meginduló mesterséges intelligencia trendet vezették: az adattermelődés és a számítási kapacitás növekedése és annak olcsó elérése.

Manapság a mesterséges intelligencia legnagyobb áttörése, hogy nem strukturált adatokon, akár felügyelet nélkül is képesek önálló információkinyerésre. A nem strukturált adatok legjellemzőbb példái a képi, hangi és írásos adatforrások, amelyeknek ötvözésére a legjobb példa a közösségi oldali aktivitásból kinyerhető adatok, melyek sok esetben a kibertámadások centrumában állnak. Jó példa erre az orosz beavatkozás a 2016-os választásokba az Amerikai Egyesült Államokban. Ekkor a felhasználókat a közösségi oldalakon végzett tevékenységük alapján célzott, az adott felhasználó életében relevánsnak számító témákat érintő, politikai indíttatású üzenetekkel manipulálták, a választói meggyőződések és preferenciák átállítására vagy elbizonytalanítására téve így (sikeres) kísérletet.[10] Mindehhez elengedhetetlen volt a mesterséges intelligencia annak érdekében, hogy a közösségi oldalaikról kinyerhető adatok alapján jól és pontosan tudják feltérképezni a választópolgárokat, az ő életükben létfontosságú vitatott témákat.

Emellett a mesterséges intelligencia mögötti gépi tanulásos algoritmusok a kiberbűnözés elleni védelemben is meghatározó szerepet játszhatnak, többek között oly módon, hogy segíthetnek időben felismerni a lehetséges veszélyeket, így azelőtt ellentámadást indítani a gyanús (az általánostól különbözően, kirívóan viselkedő, „outlier") szoftverek ellen, mielőtt a probléma óriásivá duzzadna.[11] Fő előnye, hogy az adott tűzfal valós időben, emberi beavatkozás nélkül képes alkalmazkodni a bejövő adatok alapján, így rugalmasabb és egyúttal hatékonyabb tud lenni a bejövő támadások kivédésében, automatikusan blokkolva azokat.[12]

A jövőben várhatóan az egyes entitások mesterséges intelligenciával védekeznek majd a bejövő, mesterséges intelligencia által vezérelt támadások ellen.[13] A Capgemini Research Institute

10 Bodine-Baron, E. – Helmus, T. C. – Radin, A. – Treyger, E. (2019): Countering Russian Social Media Influence. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR2740.html (2020. június 15.)

11 Ramachandran, R. (2019): How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks. https://www.entrepreneur.com/article/339509 (2020. június 15.)

12 Cyber Security Intelligence (2019): The Future Of Cyber Security Is AI. https://www.cybersecurityintelligence.com/blog/the-future-of-cyber-security-is-ai-4550.html (2020. június 15.)

13 Columbus, L. (2019): 10 Predictions How AI Will Improve Cybersecurity In 2020 https://www.forbes.com/sites/louiscolumbus/2019/11/24/10-predictions-how-ai-will-improve-cybersecurity-in-2020/#56712eb96dd7 (2020. június 15.)

(2019) által 850 vállalatvezető megkérdezésével készült kutatás alapján a vállalatvezetők többsége szerint, a mesterséges intelligencia oly módon fejleszti a kibervédelmet, hogy csökkenti a szivárgás és az arra adott reakciónak a költségét (megkérdezettek 64 százaléka), gyorsabb válaszreakciók elvégzésére alkalmas (74 százalék), valamint segítségével pontosabban lehet azonosítani a szivárgásokat (69 százalék). Emellett, a kutatás alapján, a vállalatok 63 százaléka tervez mesterségesintelligencia-alapú kibervédelmet implementálni a vállalatában.[14] Összességében megállapítható, hogy egy új korszak kezdetén vagyunk, amelyben az alkalmazott számítástechnikai eljárások is jelentősen meghatározzák az egyes vállalatok sikerességét.

Kiberhadviselés kora

A kibertér és kiberhadviselés pontos keretei nehezen meghatározhatók, ám résztézisünk szerint egyre több és több tevékenység online térbe kerülésével ezen hadviselési forma költségei jelentősen emelkedhetnek. Az előző fejezetből levonható egyik fő következtetés is erre mutat rá, miként az információs technológiai fejlődés eredményei egyre növekvő mértékben határozzák meg mindennapi életünket. Emellett a 21. században a gazdaság és a polgári társadalom tevékenysége is egyre kiterjedtebbé és sokoldalúbbá válik, mely tevékenységek védelmét az állam a hagyományos eszközökkel már nem képes garantálni. A kibertérben az ellenséges erők átugorják a 20. század hagyományos frontvonalait, és közvetlenül érik el a hátországot. A gyorsuló technológiai átalakulás is erősíti a háborús elemek átstruktúrálódását: a NATO a kibervédelmet a kollektív védelmi feladatai közé sorolta, így a szövetség egy tagállama elleni támadást a szövetség egésze elleni támadásként értelmezhet.[15] A Világgazdasági Fórum éves globális gazdasági rangsorában is egyre előrébb sorolódnak a kibertér fenyegetései: míg 2015-ben az adatlopás és kiberkémkedés kockázata a 9. és 10. legvalószínűbb nagykockázat volt a világon, addig a 2019-es jelentésben már a 4. és 5. helyen szerepeltek. Emellett mára már az állam működése szempontjából fontos kritikus információs infrastruktúra összeomlása is jelentős kockázattá lépett elő.[16] A kiberbűnözés így a jelenkorban is már jelentős gazdasági károkozó, a Lewis (2018) elemzése alapján a kár nagysága ma az éves globális GDP közel 1 százalékára tehető és folyamatosan növekszik.[17] Ez nem is meglepő nagyságrend annak tudatában, hogy az internettel rendelkező számítógépeket átlagosan 39 másodpercenként érheti támadás, illetve a vállalatok 62 százaléka tapasztalt adathalász kísérletet az elmúlt években.[18] A fejezet célja így röviden ismertetni a legfontosabb kiberbiztonsági fogalmakat, áttekinteni a jelentősebb kiberkockázatokat, valamint bemutatni a kritikus infrastruktúrák fogalmát.

14 Capgemini Research Institute (2019): Reinventing Cybersecurity with Artificial Intelligence - The new frontier in digital security https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf (2020. június 15.)

15 Tálas, P. (2016): A varsói NATO-csúcs legfontosabb döntéseiről. http://www.nemzetesbiztonsag.hu/cikkek/nb_2016_2_09_talas_peter_-_a_varsoi_nato-csucs_legfontosabb_donteseirol.pdf (2020. június 15.)

16 WEF (2015): Global Risk 2015 – Insight Report. http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf (2020. június 15.) és WEF (2019): Global Risk 2019 - Global Risk 201 – Insight Report. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf (2020. június 15.)

17 Lewis, J. (2018): Economic impact of cybercrime. https://www.csis.org/analysis/economic-impact-cybercrime (2020. június 15.)

18 Milkovich, D. (2019): 15 Alarming Cyber Security Facts and Stats. https://www.cybintsolutions.com/cyber-security-facts-stats/ (2020. június 15.)

A kiberhadviselés megértéséhez fontos tisztázni a „hadszínteret", amelyben a támadások végbemennek. A kibertér a 2013-as Nemzeti Kiberbiztonsági Stratégia megfogalmazása szerint a „…globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.".[19] Már a definíció is jól rámutat a kibervédelem nehézségére: a decentralizált, ám globálisan összekapcsolt informatikai rendszerek megnehezítik az államok számára annak eldöntését, hogy hol kezdődik a megvédendő informatikai hálózat, illetve a hálózatok nagy száma és összekapcsoltsága még inkább ellehetetleníti az állandó kiberbiztonság fenntartását. A Nemzetközi Távközlési Egyesület (ITU), az ENSZ távközlésre szakosodott szervezetének kibervédelemre vonatkozó 2008-as X.1205 ajánlásgyűjteménye is a lehető legtágabban, komplex megközelítéssel értelmezi a kiberbiztonság fogalmát: „eszközök, politikák, biztonsági koncepciók, biztonsági garanciák, irányelvek, kockázatkezelési módszerek, akciók, a képzés, a legjobb gyakorlatok, a biztonsági technológiák összessége, amelyek célja, hogy megvédjék a számítógépes környezetet, az azt használó szervezet és felhasználók eszközeit. A szervezet és a felhasználói eszközök és rendszerek körébe tartoznak a hálózathoz csatlakoztatott számítástechnikai eszközök, személyek, infrastruktúra, alkalmazások, szolgáltatások, telekommunikációs rendszerek, valamint a számítógépes környezetben küldött és/vagy tárolt információk összessége."[20]

A kiberhadviselés célpontjai széles spektrumra kiterjednek: a kormányzati szektor, a vállalati szektor és az állampolgárok is egyre növekvő mértékben kitettek a jelenségnek. A kormányzati szektort ért támadások a közszolgáltatások veszélyeztetésétől, a kormányzati infrastruktúrák lehallgatásán, az államtitkok tudatos kiszivárogtatásán, s az álhírek közzétételén át a szabotázsig is terjedhet.[21]

Az elmúlt években számos közszolgálati infrastruktúrát ért támadás: 2016-ban hackerek törték fel az ukrán elektromos hálózatot, és több mint 80 000 ember maradt áram nélkül,[22] India pedig legújabb atomerőművéről nyilatkozta, hogy számítógépes támadás áldozata lett.[23] A 2010-es évek elején a feltehetően Izrael és az Amerikai Egyesült Államok által bevetett Stuxnet vírus fő célja pedig az iráni urándúsítási program lelassítása volt, mely nagyrészt sikeresnek bizonyult: a számítógépes program az urándúsítás kapcsán kulcsfontosságú natanzi erőműegység urán-centrifugáinak körülbelül 20%-át semmisítette meg. Az elemzések szerint a támadás 1-2 évvel is visszavetette az iráni atomprogramot, s valószínűleg csak azért ilyen kevéssel, mert egy hiba miatt a féreg egy mérnök laptopját is megfertőzte, majd az interneten keresztül a világ számos számítógépén megjelent, így lehetővé vált azonosítása.[24]

---

19 1139/2013. (III. 21.) kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf (2020. június 15.)

20 ITU (2008): X.1205: Overview of Cybersecurity. https://www.itu.int/rec/T-REC-X.1205-200804-I (2020. június 15.) és Kovács, L. (2018): A kibertér védelme. Dialóg Capmus Kiadó, Budapest. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf (2020. június 15.)

21 Feledy, B. (2018): A kibertér mindent felfalhat. https://index.hu/tech/2018/07/03/kiberter_cyber_kiberhadviseles/ (2020. június 15.)

22 Wired (2016): Everything We Know About Ukraine's Power Plant Hack. https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ (2020. június 15.)

23 FT (2019): India confirms cyber attack on nuclear power plant. https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6 (2020. június 15.)

24 Bányi, B. (2019): Szemelvények a kiberhadviselés jelenéből. III. rész. Nemzetközi haditechnikai szemle. http://real.mtak.hu/98525/1/HT_2019-1_cikk-04.pdf (2020. június 15.)

A példa jól rámutat arra, hogy számítógépes programmal mekkora károkat lehet okozni: ha egy új féreg célja az urán-centrifuga sebességének szabályozása helyett egy atomerőmű vagy atommeghajtású tengeralattjáró szabályozó eszközeinek manipulálása lenne, a károk felfoghatatlanok lennének. A vállalati szektor megtámadása esetén az ipari létesítmények leolvasztása vagy a tőzsde megbénítása akár napokon belül gazdasági válságot okozhatna globális szinten. A lakosság kitettsége is növekvő: a számítógépeinket mint plusz kapacitásokat lehet kihasználni a támadásokhoz, de személyiséglopások, zsarolóvírusok áldozatává is válhatunk.[25] Emellett az intézményrendszert is felforgathatja a kiberhadviselés: a külföldi, ellenséges haderő a választások tisztaságát képes megkérdőjelezhetővé tenni az elektronikus választási rendszerek meghekkelésével vagy az online információs térben dezinformáció (fake news) terjesztésével.

A kritikus infrastruktúra, létfontosságú rendszerelemek védelme kifejezetten fontos az államok számára. Magyarországon ezen rendszerelemek védelméről való szabályozás kapcsán 2008 volt fontos mérföldkő: megjelent a *Kritikus Infrastruktúra Védelem Nemzeti Programjáról* szóló kormányhatározat, mely először tartalmazta ezen infrastruktúrák ágazatok és alágazatok szerinti bontását.[26] A 2012. évi CLXVI. törvény 1. § f. pontja az alábbiakat írja a létfontosságú rendszerelemekről: „meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna".[27] A gazdasági tevékenységek és a társadalmi aktivitás digitalizáció irányába való eltolódása miatt egyre több infrastruktúra válhat kiemelt fontosságúvá a kibervédelem szempontjából. A törvény végrehajtásához kapcsolódó 65/2013. (III. 8.) kormányrendelet alapján ma öt fő horizontális kritérium alapján azonosítják a létfontosságú rendszerelemeket.[28] A *veszteségek kritériuma* a lehetséges áldozatok és súlyos sérültek alapján mérlegel, a *gazdasági hatás kritériuma* a károk bruttó nemzeti jövedelemhez való viszonyát figyeli, a *társadalmi hatás kritériuma* a sűrűbben lakott vidékek köznyugalom megzavarásának nagyságát monitorozza, a *politikai hatás kritériuma* az állam és intézményei iránti bizalom nagyságát figyeli, míg a *környezeti hatás kritériuma* az épített vagy természetes környezet rongálódását elemzi.[29]

A veszteségek minimalizálása miatt az országok és vállalatok számára egyre fontosabbá válik a védelemre való berendezkedés. Ezt az Európai Unió is felismerte, hisz 2016-ban a Bizottság egy közel 2 milliárd euró értékű kezdeményezést jelentett be, melynek célja, hogy elősegítse a köz- és a magánszférában a kiberbiztonsághoz kapcsolódó kutatási és innovációs folyamatokat. A kezdeményezés egyrészt erősítheti az EU-ban az innovációt, másrészt

25 Feledy, B. (2018): A kibertér mindent felfalhat. https://index.hu/tech/2018/07/03/kiberter_cyber_kiberhadviseles/ (2020. június 15.)

26 Kovács, L. (2018): A kibertér védelme. Dialóg Capmus Kiadó, Budapest. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf (2020. június 15.)

27 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. https://net.jogtar.hu/jogszabaly?docid=a1200166.tv (2020. június 15.)

28 65/2013. (III. 8.) kormányrendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról. https://net.jogtar.hu/jogszabaly?docid=a1300065.kor (2020. június 15.)

29 Kovács, L. (2018): A kibertér védelme. Dialóg Capmus Kiadó, Budapest. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf (2020. június 15.)

segítheti, hogy az elektronikus szolgáltatások felé való közbizalom erősödjön. Napjainkban ugyanis csak az európai állampolgárok 22 százalékának van teljes bizalma a keresőmotorokban, közösségi oldalakban, illetve az e-mailes szolgáltatásokban.[30]

Az európai kibervédelmi piac mérete várhatóan töretlenül növekedhet a jövőben, 2025-ben elérheti a 60 milliárd eurót. Bizonyos szektorokban a növekedés igazán kiemelkedő lehet, például a bankszektor kibervédelemhez kapcsolódó költségei várhatóan ezen idő alatt meg is duplázódnak.[31] Az államok kibervédelemhez kapcsolódó kiadásai nemzetbiztonsági érdekek miatt nem teljesen átláthatók, azonban valószínűleg az állami és azon belül a hadi szférában is tetemes kiadások valósulnak meg, illetve ezek a jövőben jelentősen növekedhetnek is. A következő fejezetben egy olyan modellt konstruálunk, ami a fenti trendek alapján próbálja megbecsülni, hogy az állami entitások számára a kibervédelmi kiadások miképpen alakulhatnak.

Kibertámadások modellezése

A fejezetben modellezéssel vizsgáljuk meg a főtézisünket: a jövőben a kibertér mint harcászati tér aktivitása, és az általa kiváltott károk nagysága is növekedni fog, így a kiberhadviselés problémája globális szempontból – a globális összjóléthez egyre negatívabb hozzájárulása miatt – egyre fontosabbá válhat. Emiatt a szupranacionális szervezetek jogköreinek erősítése, illetve a kiberhadviseléshez kapcsolódó szankciók bevezetése miatt a jövőben elszenvedett károk esetlegesen csökkenthetők.

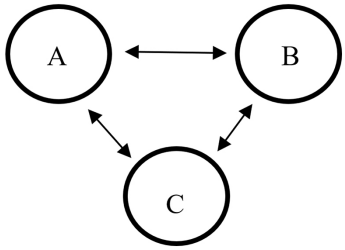
A modellkeret célja egy olyan absztrakt világ megalkotása, ahol különböző szimulációkat lehet futtatni arra vonatkozóan, hogy a kiberhadviselés terén az egyes tagországok számára milyen hadviselési stratégia a kifizetődő. A modellben a résztvevő ágensek végig hasznosságmaximalizálási döntéseket hoznak, azaz minden egyes döntési pontban eldöntik, hogy részt kívánnak-e venni kiberhadviselésben, és ha igen, azt milyen módon teszik. Összesen 20 döntési pont van a modellben, tehát 20-szor döntenek arról az ágensek, hogy háborúzzanak-e vagy sem. A 20 döntési pont tekinthető például 20 évtizednek/évnek és az adott évtizedben/évben az ágens eldönti, hogy mekkora erőforrást allokáljon kiberhadviselésre és kibervédelemre. A modellezés célja felmérni, hogy a jövőbeli trendek teljesülése – elektronikus eszközök számának és jelentőségének növekedése – esetén milyen folyamatok várhatók a kiberhadviselés terén. A modellben a digitalizáció mélyülését a kritikus infrastruktúra változó proxyzza. A modell keretei kizárólag az államok egymás elleni kiberhadviselésének elemzésére alkalmasak, így eltekintünk a nem állami kiberbűnözési csoportok tevékenységétől, melyek céljai meglehetősen sokrétűek (pl. pénz, hírnév szerzése vagy a jelenlegi politikai struktúra megdöntése), így modellezésük nehézkes.

A „modellvilágban" összesen három ország-/szövetségi rendszer van (A, B, C), melyek ellenségként tekintenek egymásra (lásd 2. ábra). Az országok az első modellkeretben csak is kizárólag kiberhadviselés segítségével tudnak egymással harcolni, és optimalizálási problémájuk

30 European Commission (2019): Cybersecurity industry. https://ec.europa.eu/digital-single-market/en/cybersecurity-industry?fbclid=IwAR27gK72s-_GNuMDBwwUYZ8rkQB5v2-_gl3I-pEKHysdimcu53SyEpJAknM (2020. június 15.)

31 HelpNetSecurity (2019): European cybersecurity market to exceed $65 billion by 2025. https://www.helpnetsecurity.com/2019/12/03/european-cybersecurity-market/?fbclid=IwAR3GcwGwXvd_zA1OKgHvJ3hsDTSdKNileHefuDVCGl0X0nJ2etqd9xK9eWk (2020. június 15.)

minden egyes döntési pontban azt eldönteni, hogy az adott évben érdemes-e a másik féllel vagy felekkel háborúzni vagy sem, illetve, hogy milyen mértékben védjék meg a saját kritikus infrastruktúrájukat az ellenséges országtól érkező támadásoktól.



2. ábra: Konstruált világ egymáshoz viszonyított szerepei

Az országok optimalizációs problémát oldanak meg, céljuk, hogy a saját hasznosságukat maximalizálják. Az országok ismerik egymás hasznosságfüggvényeit, melyek maximalizálása az alábbi forma alapján történik:

$$\max u = (av - bx - cy - dz) \qquad (1)$$

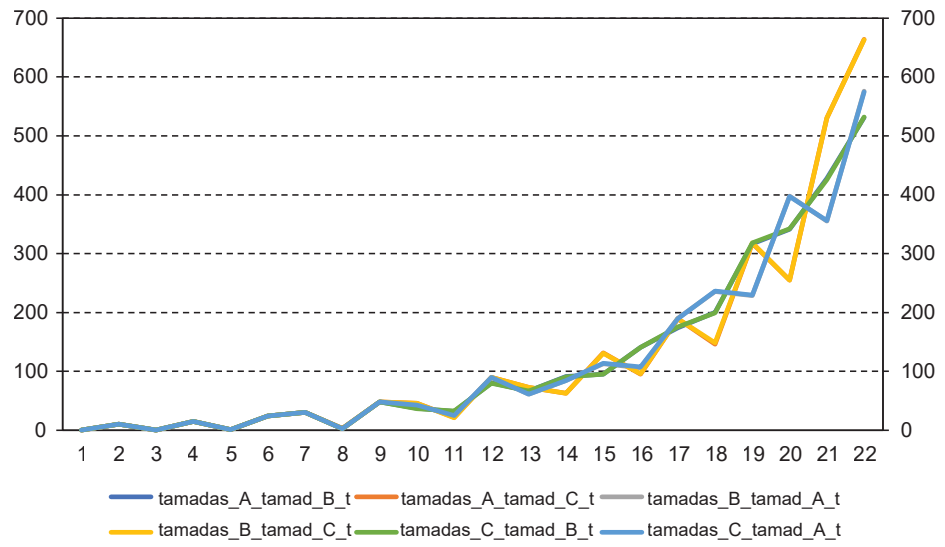
ahol „a" egy sikeres kibertámadásért járó jutalom nagysága, „b" egy kibertámadás költsége, „c" egy kritikus infrastruktúra kiberbiztosítási védelmi költsége, „d" pedig annak költsége, ha feltörik az egyik kritikus infrastruktúrájukat. Az adott ország így dönt arról, hogy mennyi kibertámadást hajt végre (x), illetve hány darab kritikus infrastruktúrát szerel fel védelemmel (y). A sikeres kibertámadások száma (v) a többi ország tevékenységétől függ: amennyiben a megtámadott infrastruktúra fel van szerelve védelemmel, a támadás sikertelen, ha nincs felszerelve védelemmel, a támadás sikeres. A megtámadott ország csak az ellene sikeresen végrehajtott támadásokról (z) értesül, a sikertelenekről nem. (A modell „a", „b", „c", „d" paramétereit lásd részletesen az A. mellékletben.)

Az országokban folyamatos az ágazatok digitalizálódása: az első döntési pontban még csak 5 kritikus infrastruktúra van, majd 1-1 döntési pont között a kritikus infrastruktúrák száma mindig 25 százalékkal növekszik. A technológia fejlődése miatt a korábban védett infrastruktúrák védelmi rendszere elavulttá válik, így újra be kell fizetni az országban a kiberbiztosítás védelmi költségét, hogy az adott objektum védetté váljon. Az országok az adott döntési pontban a megelőző két időszak eseményeit figyelembe véve döntenek arról, hogy mennyi kibertámadást indítsanak, illetve hány kritikus infrastruktúrát védjenek meg (a modell specifikációját lásd részletesen az A. mellékletben). Az országok döntési struktúrájában továbbá egy felejtési paraméter is szerepel, tehát ha az infrastruktúrákat sok ideig nem éri kibertámadás, akkor az államok egyre kevesebb és kevesebb infrastruktúrára fizetik ki a kiberbiztosítás védelmi költségét. A modellbe véletlen változók is be vannak építve abból a célból, hogy ha például bizonyos ideig nem éri meg kibertámadást végrehajtani egy ellenséges ország ellen, pár időszak múlva az adott ország újra próbálkozzon kisebb támadásokkal, hogy felmérje a

jelenlegi helyzetet, akár azon az áron is, hogy a hasznossága bizonyos mértékben csökken. Emiatt a modell egyes futtatásai más és más eredményt adnak, így az elkövetkezőkben a modell 20 futtatásának eredményeinek átlagát vesszük figyelembe elemzésünk elvégzésénél.

A döntési probléma hasonlít egy klasszikus játékelméleti, közgazdaságtani problémához, a *fogolydilemmához*. Itt a rendőrök által elfogott két rabló dönt arról, hogy valljon vagy tagadjon az általuk vélhetően elkövetett bűncselekmények kapcsán. Attól függően, hogy az egyik vagy másik rabló vall vagy tagad, a kifizetések, vagy a börtönévek száma eltérően alakul (lásd melléklet B.1. táblázat). Ha mindkét fél tagad, akkor bizonyíték hiányában a két rabló viszonylag kis büntetéssel megússza, azonban, ha már az egyik fél vall, akkor a letöltendő évek száma jelentősen emelkedik. Mivel mindkét rabló számára a másik rabló tevékenységétől függetlenül jobban megéri vallani, mint tagadni, így a végén végül mindketten vallani fognak és 5 évre börtönbe kerülnek (Nash-egyensúly), miközben, ha kitartanak a tagadás mellett, mindketten jobban járnának (Pareto-hatékony állapot).[32]

Hasonló dilemmával szembesülhetnek a kibertámadás során is az egyes tagállamok. Amennyiben egyikőjük sem támad, így nem kell a kritikus infrastruktúrát védeni, és Pareto-hatékony pontba kerülünk. Ekkor azonban bármelyik állam számára jövedelmezőbb támadási stratégiát folytatni, mert az ellenség infrastruktúrája nem védett, így a könnyű célpont jelentős hasznot hajthat. Azonban a többi tagállam is eszerint gondolkodik, ami végül, ahhoz vezet, hogy jelentős támadásokat fognak intézni egymás ellen, miközben a védelmi kiadásaik is jelentősen megugranak. Ezt az elméleti levezetést a modellünk eredményei is alátámasztják, hisz a támadások száma exponenciálisan növekszik az egyes döntési pontok között (3. ábra). Az infrastruktúrák növekvő száma újabb és újabb támadási lehetőségeket nyit a tagállamok számára, melyeket a fenti okfejtés miatt a tagállamok ki is használnak.



3. ábra: Az egyes országok összes támadásának alakulása 20 szimuláció átlagában

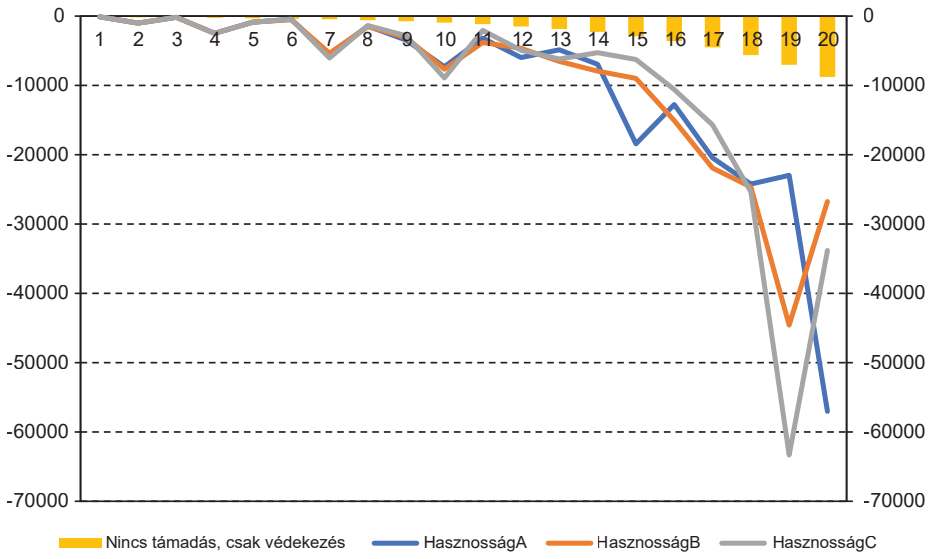
32 Varian, H. (2010): Intermediate Microeconomics – A modern approach. New York :W.W. Norton & Company.

Ezt a fogolydilemma jellegű hatást a modell legegyszerűbb felépítésekor (lásd 1. táblázat) biztosan ki is lehet mutatni. Az ágenseknek ilyenkor ugyanis nincs egyértelmű, stabil stratégiája, a támadások által szerezhető hasznosságnövekmény támadásra ösztökélik az egyes országokat, így a Pareto-hatékony állapot – Nem védekezik – Nem támad páros – nem elérhető.

1. táblázat: Két ország kifizetésfüggvénye egy időszakra vonatkozóan a modell paraméterei alapján, amennyiben 1-1 kritikus infrastruktúrával rendelkeznek (* jelölve az adott stratégiához tartozó legjobb válasz függvényeket)

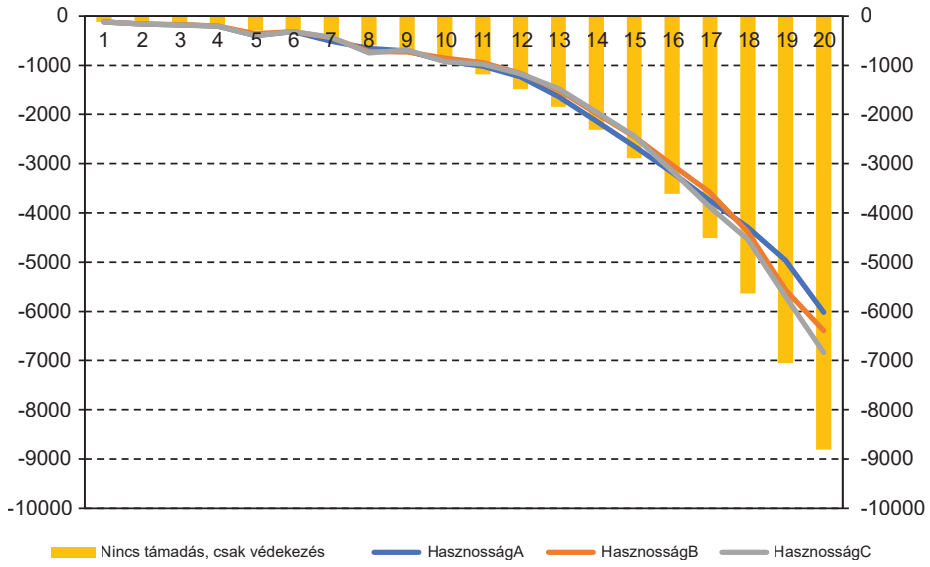
		„B" ország			
		Nem védekezik – Nem támad	Védekezik – Nem támad	Nem védekezik – Támad	Védekezik – Támad
„A" ország	Nem védekezik – Nem támad	(0;0)	(0*; -10)	(-400; 90*)	(-400; 80)
	Védekezik – Nem támad	(-10; 0*)	(-10; -10)	(-10*; -10)	(-10*; -20)
	Nem védekezik – Támad	(90*; -400)	(-10; -10)	(-110; -110)	(-410; 80*)
	Védekezik – Támad	(80; -400)	(-20; -10*)	(80; -410)	(-20; -20)

Az alapmodell első fontosabb eredménye, hogy az országok átlagos hasznossága az idő előrehaladtával csökken. A veszteség mértéke egyre jelentősebben eltér attól a pályájától, mikor az államok egyáltalán nem támadnak, hanem minden döntési pontban minden kritikus erőforrásukat újra megvédik (lásd 4. ábra). Ennek hátterében természetesen a növekvő számú támadások állnak, melyek sok esetben sikeresnek is bizonyulnak (lásd melléklet B.1. ábrája). Ezek az eredmények így párhuzamba állíthatók a *fogolydilemmával*, a támadások jelentette esetleges hasznosságnövekmény miatt az országok egyre több és több támadásba hajszolják egymást, mely a hasznosságukat végül jelentősen csökkenti, így a Pareto-hatékony ponttól az idő előrehaladtával egyre távolabb és távolabb kerülnek.



4. ábra: Az egyes országok hasznosságának alakulása 20 szimuláció átlagában, illetve a hasznosság, ha az összes kritikus infrastruktúrájukat megvédik és sosem támadnak

Így érdemes megvizsgálni, hogy ha egy külső, szupranacionális szervezet vagy valamilyen „világkormány" képes szankcionálni a kibertámadásokat végrehajtó országokat, akkor az egyes országok agressziója csökkenhet-e. A modellben így azon országok, melyek kibertámadást hajtottak végre, az elkövetkező két időszakban szankcióban (e) részesülnek, mely csökkenti az adott ország hasznosságát. Megfelelően nagy szankció (e = 1000) esetén a kibertámadások száma jelentősen visszaszorul, mely maga után vonja a költségek csökkenését is, így a három ország összesített hasznossága jelentősen javul az előző esethez képest (lásd 5. ábra, illetve az B.2., B.3. ábra a mellékletben). A támadások átlagos száma nagyjából század részére esik vissza, illetve a jóléti veszteség értéke több, mint 80 százalékkal csökken (hasznosságfüggvény értéke nő) az előző eset eredményeihez képest.



5. ábra: Az egyes országok hasznosságának alakulása 20 szimuláció átlagában, amennyiben e = 1000 szankcióban részesül a kibertámadást végrehajtó ország

Azonban csak igazán magas szankció esetén hatékony az elrettentés: amennyiben a szankció nagysága csupán 100 egység, akkor a támadások száma 35 százalékkal, illetve a jóléti veszteség csupán 25 százalékkal csökken. Magas szankció esetén válik csak a támadás határköltsége elég jelentőssé ahhoz, hogy a kiinduló Pareto-hatékony pont Nash-egyensúlyi ponttá is váljon. A korábban használt egyszerű modellt kibővítve a szankciókkal már egyik résztvevőnek sem éri meg támadni, hisz az ebből származó plusz haszon minden egyes esetben alatta marad a kapott szankció nagyságának. Így ebben a struktúrában az országok sosem kísérelnek meg támadást, illetve infrastruktúrájukat se védenék, hiszen ez a pont a játék Nash-egyensúlyi pontja (lásd 2. táblázat).

2. táblázat: Két ország kifizetésfüggvénye egy időszakra vonatkozóan a modell paraméterei alapján, amennyiben 1-1 kritikus infrastruktúrával rendelkeznek, illetve támadás esetén 1000 szankcióval néznek szembe. (* jelölve az adott stratégiához tartozó legjobb válasz függvényeket)

		„B" ország			
		Nem védekezik – Nem támad	Védekezik – Nem támad	Nem védekezik – Támad	Védekezik – Támad
„A" ország	Nem védekezik – Nem támad	(0*;0*)	(0*; -10)	(-400; -910)	(-400; -920)
	Védekezik – Nem támad	(-10; 0*)	(-10; -10)	(-10*; -920)	(-10*; -1020)
	Nem védekezik – Támad	(-910; -400)	(-1010; -10*)	(-1110; -1110)	(-1410; -920)
	Védekezik – Támad	(-920; -400)	(-1020; -10*)	(-920; -1410)	(-1020; -1020)

Összegzés

Tanulmányunk egyik célja volt bemutatni, hogy a technológiai fejlődés, illetve a világ digitalizálódása milyen folyamatokat indíthat el a jövőben, és ezek miképpen kellene, hogy megváltoztassák a társadalmak, illetve a kormányzat hozzáállását az adatok védelméhez. Elemzésünk alapján következtetésként levonható, hogy a kibertámadások egyre komolyabb fenyegetést jelentenek mind a vállalati, mind a lakossági, mind a kormányzati szektor számára. Az elektronikus eszközök és hálózatok feltörése legtöbbször nemzetgazdasági érdeket sért, így az államok számára kulcsfontosságú, hogy az adott területen erősítsék jelenlétüket. A kibervédelem szempontjából kritikus infrastruktúrák pontos meghatározása a változó technológia, illetve a változó információs technológiai iparág miatt teljeskörűen nem lehetséges, azonban a keretek meghatározása mára nagyrészt végbement. A tanulmányunk célja volt továbbá megvizsgálni a jövőbeni állami kibertámadási, illetve kibervédelmi költségek alakulását. A dinamikus optimalizációs modellünk eredményei alapján következtettünk arra, hogy az államok számára a kibertámadások fokozása nemzetgazdasági érdek lehet, hisz szankciók hiányában a kibertámadások kapcsán elszenvedett költségek jelentősen alatta maradnak a potenciális nyereségnek. Így a jövőben a globális optimumtól egyre távolabb kerülhetünk, beavatkozás nélkül a kibertámadások száma valószínűsíthető, mely egyre nagyobb veszteséget is indukálhat globális szinten. Ezután további modellezésünkben arra a következtetésre jutottunk, hogy egy megfelelő jogosultságokkal felruházott szupranacionális szervezet – amennyiben kellően magas szankciót határoz meg – jelentős mértékben csökkenthetné a kibertámadások jövőbeli számát, így a kibertámadások, illetve kibervédelemből származó jóléti veszteséget is. Így javaslatunk szerint a kiberhadviselés terén az egységes sztenderdek lefektetése kívánatos, melyet a sztenderdek betartása, illetve a közös szankcionálás követhetne. Azonban tisztában vagyunk azzal, hogy az elméleti optimum gyakorlati megvalósítása jelentős korlátokba ütközik az eltérő geopolitikai érdekek, a változó technológia, illetve a kibertámadások mögött álló támadó entitás egyértelmű beazonosításának lehetetlensége miatt.

A melléklet

A modell felépítése

Az országok az alábbi hasznosságfüggvénnyel szembesülnek minden egyes döntési pontban:

$$\max u_i = \Sigma_{k=1}^{2} (av_i^k - bx_i^k - cy_i - dz_i^k) \qquad (1)$$

Amennyiben az ország az előző döntési pontban kibertámadást hajtott végre (x_{i-1}^{k-1}), akkor hasznosságfüggvénye az alábbiak szerint változik:

$$\max u_i = \Sigma_{k=1}^{2} (av_i^k - bx_i^k - cy_i - dz_i^k - e_i) \qquad (2)$$

ahol „a" a sikeres kibertámadásokért járó jutalom nagysága, „b" egy kibertámadás költsége, „c" egy kritikus infrastruktúra kiberbiztosítási védelmi költsége, „d" pedig ha feltörik az egyik kritikus infrastruktúrájukat, „e" pedig a szankció nagysága. Az *i*-dik ország így dönt arról, hogy mennyi kibertámadást hajt végre a *k*-dik ország ellen (x_i^k), illetve a kritikus infrastruktúrái (I_i) közül hány darabot (y_i) szerel fel védelemmel.

Az *i*-dik országnak a *k*-dik ország ellen irányuló sikeres támadásainak (v_i^k) száma az összes *k*-dik ország ellen irányuló támadás (x_i^k), illetve az ellenség védett (y_k) és az összes (I_k) infrastruktúrájának aránya alapján áll elő: $v_i^k = x_i^{k*}(1-y_k/I_k)$. Az *i*-dik ország meghekkelt, feltört infrastruktúráinak száma (z_i^k) a kapott támadások (x_k^i), illetve a saját infrastruktúrájának száma (I_i), illetve védettsége (y_i) alapján számolódik: $z_i^k = x_k^{i*}(1-y_i/I_i)$. Így definíció szerint a $v_i^k == z_k^i$, hisz az i-dik ország sikeres támadásainak száma az összes k-dik ország ellen meg kell egyezzen a *k*-dik országban az *i*-dik ország által feltört infrastruktúrák számával.

Az országok két időszakra tekintenek vissza, és a támadáshoz, illetve védekezéshez kapcsolódó hasznosságváltozások alapján határozzák meg, hogy több vagy kevesebb támadást hajtsanak végre. Összességében amennyiben a korábbi döntési pontok során több támadás több hasznosságot generált, akkor relatíve növelik, ha kevesebbet akkor csökkentik a támadásaik számát. Ugyanígy a védekezés során, ha a védekezés a múltban kifizetődő volt, akkor továbbra is nagyobb erővel védekezik az adott ország, ha az elmúlt két időszak alapján nem érte meg védekezni, akkor a védett infrastruktúrák relatív száma csökkenő (pontos számításokat lásd a C. mellékletben).

Kezdeti paraméterek:

a = 100; b = 10; c = 10; d = 400 végig a szimuláció során

A modell két időszakra való visszatekintéssel modellezik, így az első két időszak értékei adottak, ezt követi 20 döntési pont, miután az országok maguk döntenek a stratégiájukról.

I. időszak értékei: $I_A = I_B = I_C = 5$; $y_A = y_B = y_C = 5$; $x_{AB} = x_{AC} = x_{BA} = x_{BC} = x_{CA} = x_{CB} = 0$

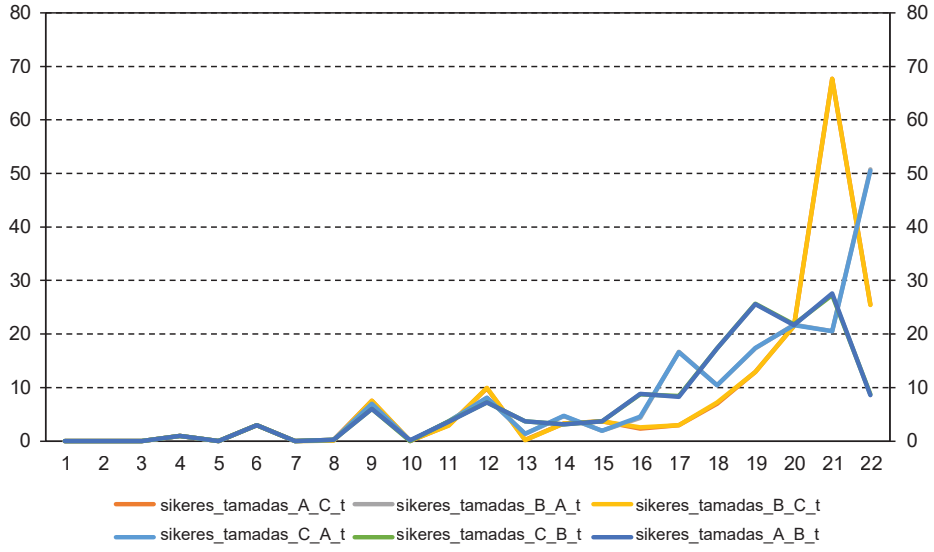
II. időszak értékei: $I_A = I_B = I_C = 10$; $y_A = y_B = y_C = 10$; $x_{AB} = x_{AC} = x_{BA} = x_{BC} = x_{CA} = x_{CB} = 10$

B melléklet

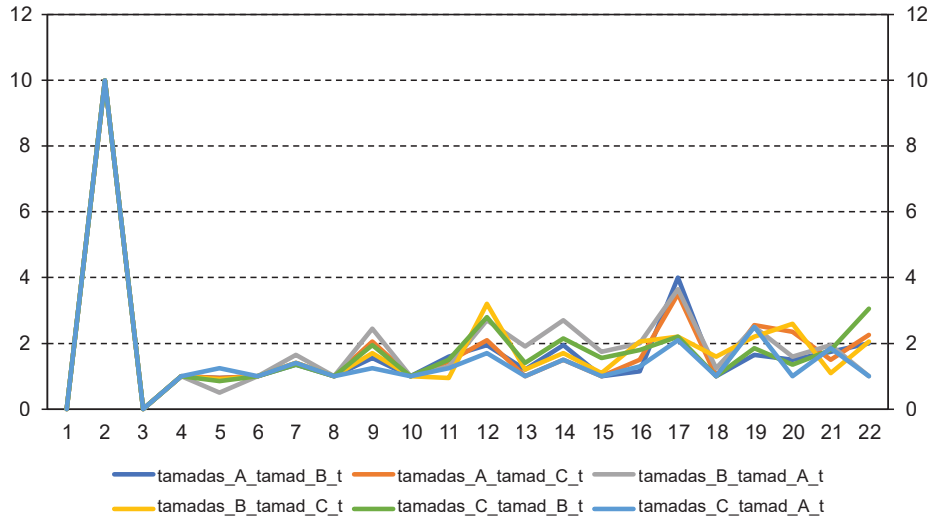
Ábrák és táblázatok

B.1. táblázat: A fogolydilemma egy lehetséges kifizetésfüggvénye

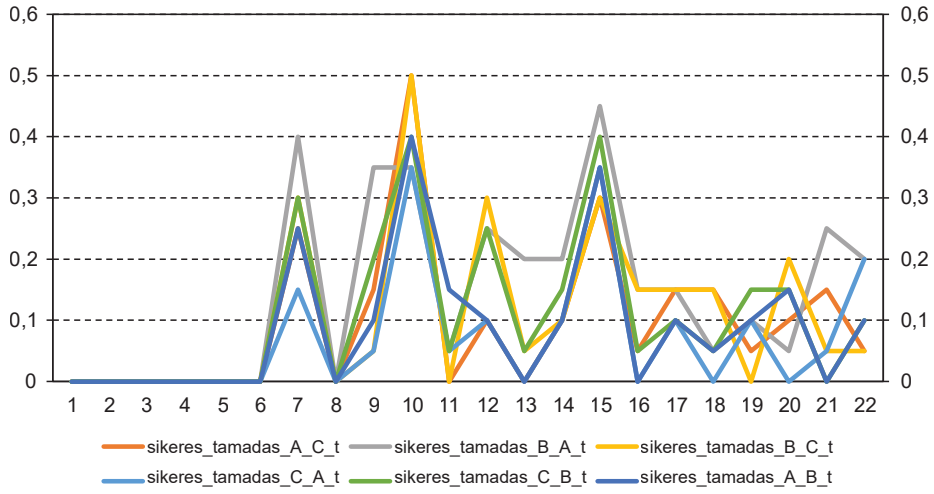
		„A" rabló	
		Tagad	Vall
„B" rabló	Tagad	(-1; -1)	(-10; 0)
	Vall	(0;-10)	(-5;-5)



B.1. ábra: Az egyes országok sikeres támadásainak alakulása 20 szimuláció átlagában



B.2. ábra: Az egyes országok összes támadásának alakulása 20 szimuláció átlagában, amennyiben kibertámadás esetén a „világkormány" e = 1000 szankcióval bünteti a támadó tagországokat



B.3. ábra: Az egyes országok sikeres támadásainak alakulása 20 szimuláció átlagában, amennyiben kibertámadás esetén a „világkormány" e = 1000 szankcióval bünteti a támadó tagországokat

C melléklet

A számítás során használt táblázatok, illetve VBA kód az alábbi dropbox mappából érhető el: https://www.dropbox.com/sh/eg0guodzwu1gg6s/AACMPzQI0o446V4rxnLkSVsBa?dl=0

Irodalomjegyzék

1. 1139/2013. (III. 21.) kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf (2020. június 15.)
2. 65/2013. (III. 8.) kormányrendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról. https://net.jogtar.hu/jogszabaly?docid=a1300065.kor (2020. június 15.)
3. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. https://net.jogtar.hu/jogszabaly?docid=a1200166.tv (2020. június 15.)
4. Bodine-Baron, E. – Helmus, T. C. – Radin, A. – Treyger, E. (2019): Countering Russian Social Media Influence. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR2740.html (2020. június 15.)
5. Bányi, B. (2019): Szemelvények a kiberhadviselés jelenéből. III. rész. Nemzetközi haditechnikai szemle. http://real.mtak.hu/98525/1/HT_2019-1_cikk-04.pdf (2020. június 15.)
6. Business Insider (2019): IoT Report: How Internet of Things technology growth is reaching mainstream companies and consumers. https://www.businessinsider.com/internet-of-things-report (2020. június 15.)
7. Capgemini Research Institute (2019): Reinventing Cybersecurity with Artificial Intelligence - The new frontier in digital security. https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf (2020. június 15.)
8. Columbus, L. (2019): 10 Predictions How AI Will Improve Cybersecurity In 2020. https://www.forbes.com/sites/louiscolumbus/2019/11/24/10-predictions-how-ai-will-improve-cybersecurity-in-2020/#56712eb96dd7 (2020. június 15.)
9. Cyber Security Intelligence (2019): The Future Of Cyber Security Is AI. https://www.cybersecurityintelligence.com/blog/the-future-of-cyber-security-is-ai-4550.html (2020. június 15.)
10. Dahlqvist, F. – Mark Patel, M. – Alexander Rajko, A. – Shulman, J. (2019): Growing opportunities in the Internet of Things. https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things# (2020. június 15.)
11. Descartes Lab (2020): https://www.descarteslabs.com/#overview (2020. június 15.)
12. Ericsson (2016): Ericsson Mobility Report (2016 November) – on the pulse of the networked society. https://www.ericsson.com/en/mobility-report/reports (2020. június 15.)
13. European Commission (2019): Cybersecurity industry. https://ec.europa.eu/digital-single-market/en/cybersecurity-industry?fbclid=IwAR27gK72s-_GNuMDBwwUYZ8rkQB5v2-_gl3I-pEKHysdimcu53SyEpJAknM (2020. június 15.)

14. Feledy, B. (2018): A kibertér mindent felfalhat. https://index.hu/tech/2018/07/03/kiberter_cyber_kiberhadviseles/ (2020. június 15.)
15. FT (2019): India confirms cyber attack on nuclear power plant. https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6 (2020. június 15.)
16. Gilmore, C. K. – Chaykowsky, M. – Thomas, B. (2019): Autonomous Unmanned Aerial Vehicles for Blood Delivery: A UAV Fleet Design Tool and Case Study. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR3047.html (2020. június 15.)
17. HelpNetSecurity (2019): European cybersecurity market to exceed $65 billion by 2025. https://www.helpnetsecurity.com/2019/12/03/european-cybersecurity-market/?fbclid=IwAR3GcwGwXvd_zA1OKgHvJ3hsDTSdKNileHefuDVCGl0X0nJ2etqd9xK9eWk (2020. június 15.)
18. IMF (2020): https://www.imf.org/external/index.htm (2020. június 15.)
19. ITU (2008): X.1205: Overview of Cybersecurity. https://www.itu.int/rec/T-REC-X.1205-200804-I (2020. június 15.)
20. Kovács, L. (2018): A kibertér védelme. Dialóg Capmus Kiadó, Budapest. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf (2020. június 15.)
21. Lewis, J. (2018): Economic impact of cybercrime. https://www.csis.org/analysis/economic-impact-cybercrime (2020. június 15.)
22. Milkovich, D. (2019): 15 Alarming Cyber Security Facts and Stats. https://www.cybintsolutions.com/cyber-security-facts-stats/ (2020. június 15.)
23. Our World in Data (2020): Technological progress. https://ourworldindata.org/technological-progress (2020. június 15.)
24. Porche, I. R. III (2019): Fighting and Winning the Undeclared Cyber War. https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html (2020. június 15.)
25. Ramachandran, R. (2019): How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks https://www.entrepreneur.com/article/339509 (2020. június 15.)
26. Szepesi, A. (2019): Holnaptól borul a fél világ? Mit jelent a kvantumfölény, mire számíthatunk ezután?
27. https://hvg.hu/tudomany/20191028_google_sycamore_kvantumfoleny_jelentese_hogyan_mukodik_kvantumszamitogep_mukodese_egyszeruen_qubit_kubit_ibm_summit_szuperszamitogep (2020. június 15.)
28. Takahashi, D. (2017): https://venturebeat.com/2017/03/28/intel-moores-law-isnt-slowing-down/ (2020. június 15.)
29. Tálas, P. (2016): A varsói NATO-csúcs legfontosabb döntéseiről. http://www.nemzetesbiztonsag.hu/cikkek/nb_2016_2_09_talas_peter_-_a_varsoi_nato-csucs_legfontosabb_donteseirol.pdf (2020. június 15.)
30. WEF (2015): Global Risk 2015 – Insight Report. http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf (2020. június 15.)

31. WEF (2019): Global Risk 2019 – Insight Report. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf (2020. június 15.)
32. Varian, H. (2010): Intermediate Microeconomics – A modern approach. New York :W.W. Norton & Company.
33. Wired (2016): Everything We Know About Ukraine's Power Plant Hack. https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ (2020. június 15.)

Hegyi Henrietta

Modernizáció és iparbiztonság a COVID-19-járvány után Magyarországon

Rezümé

Az értekezés célja, hogy bizonyítékokat keressen arra nézve, hogy a koronavírus okozta válság hosszútávon pozitív hatással lehet az ipari technológiák fejlődésére. A vizsgálat a különböző történelmi folyamatok áttekintése mellett egy ipari szereplők bevonásával végzett kérdőíves kutatással igyekszik alátámasztani ezt a hipotézist. Az áttekintés és a kutatási eredmények elemzése mellett a tanulmány arra is kísérletet tesz, hogy javaslatokat fogalmazzon meg a pozitív változások támogatása érdekében, illetve felhívja a figyelmet a várható kihívásokra.

Resume

The aim of this thesis is to look for evidence suggesting that the coronavirus crisis can have a positive long-term impact on the development of industrial technologies. In addition to reviewing various historical processes, the study seeks to support this hypothesis through a questionnaire survey involving industrial actors. Moreover, it provides an overview and analysis of the research findings, as well as attempting to make recommendations to support positive change and to draw attention to the challenges ahead.

Vezetői összefoglaló

A koronavírus-járvány olyan folyamatokat indított el világszerte, melyek egy ipari modernizációs hullám kialakulásának irányába hatnak. Magyarország ipari vállalatainak döntéshozói a dolgozatban foglalt kérdőíves kutatás alapján érzékelik ezt a trendet, ám digitális biztonsági felkészültségük még korlátozott. Ennek oka az új technológiákkal kapcsolatos hiteles információk hiányában keresendő. A dolgozat javaslatot tesz a probléma kiküszöbölésére az állami szerepvállalás fontosságát hangsúlyozva.

Bevezetés

A válságokról általánosan kialakult kép, hogy a gazdaságra kedvezőtlen hatást gyakorolnak, a társadalomban feszültséget szítanak, mivel reorganizáló erejük miatt sokan elvesztik megélhetésüket vagy nehéz helyzetbe kerülnek. Amellett, hogy ez igaz, a válságoknak hosszútávra nézve előnyeik is lehetnek, hiszen kedveznek bizonyos folyamatoknak, melyek szükségesek a fejlődéshez.

Dolgozatom célja annak bizonyítása, hogy a SARS-COV (COVID-19) világjárványnak hosszútávon várhatóan kedvező hatása lesz az ipari – különös tekintettel a gyáripari – digitalizációs folyamatokra nézve, másrészt felhívni a figyelmet a jelenlegi modernizációs, digitalizációs hullám biztonságpolitikai vetületeire hazánk iparában. Módszertani szempontból a vizsgálatot geopolitikai kitekintéssel végzem azzal a céllal, hogy keretrendszerbe helyezzem a lokális viszonyokat. Célom nem a folyamatok részletekbe menő magyarázata, hanem az átfogó strukturális változások és az ezekkel járó fenyegetettségek áttekintése, összegzése. Mindezeket hazai tapasztalatokkal egy exploratív jellegű empirikus kutatás útján egészítem ki, amely pilotkutatásként, iránymutatásként szolgálhat nagyobb erőforrásokat megmozgató későbbi kutatásokhoz.

Első tézisem: A koronavírus által okozott recesszió modernizációs hullámhoz vezet a magyar iparban. A megfogalmazott tézis alátámasztásához egyrészt megvizsgálom, hogy van-e összefüggés általában a válságok és az innováció között, illetve hogy modernizációs szempontból a válság hatása értelmezhető-e pozitívumként. Másrészt a koronavírus-járvány által előidézett válsággal kapcsolatos hírekből kiindulva igyekszem konkrét jeleket azonosítani, melyek utalhatnak a későbbi modernizációs hullámra.

Második tézisem: A várható digitalizációs – vagy általában a modernizációs – hullámban a magyar ipar bizonyos biztonsági kockázatoknak van kitéve. Ezt a feltevést főként az empirikus tapasztalatokra alapozva vizsgálom meg.

A 2020-as évekre a mesterséges intelligencián alapuló új technológiák szerepe – különösen a mélytanulás – megkérdőjelezhetetlenné vált, ráadásul megfigyelhető, hogy az alapmodellek egyre szélesebb körben válnak elérhetővé, ami kedvező hatással van a megfelelő szaktudású szakemberek képzésére. Világszerte beindulnak az adatpiacok, amelyek alapvetően átalakítják az államok és a nemzetközi szervezetek működési módját. Nem vitatott, hogy jelenleg egy paradigmaváltás tanúi vagyunk.

A dolgozat tárgyát tekintve elengedhetetlen a modernizáció és a digitalizáció szavak egymástól való elhatárolása. Bár a modernizáció tágabb fogalom, melynek részeként beszélhetünk a digitalizációról, és nem ugyanazt jelenti, a két fogalmat mégis szinonimaként használom, mert jelenlegi évszázadunkban ez a két folyamat szorosan összefonódik: 4. (és 5.) ipari forradalomban – egyes kutatók már az 5. ipari forradalom létéről beszélnek – a digitalizációs folyamatok főszerepet játszanak a modernizálás során.

Az elemzés során többnyire a modernizáció szót használom, mivel a modernizáció magába foglalja az átalakítás minden fajtáját, amik a jelen kor kihívásaihoz illeszkedő eszközök használatára, a célok leghatékonyabb elérésére irányulnak. Ezek a változtatások azonban nem szükségképpen innovatívak, hiszen sokszor egyszerűen csak felzárkózási célzattal hajtják végre őket.

A kibertér és a geopolitika kapcsolata

Mielőtt mélyebben sorra venném a bevezetésben megfogalmazott két tézist alátámasztó vagy cáfoló információkat, elengedhetetlen a digitális iparbiztonság és a kibertér biztonságának geopolitikai vetületének áttekintése, hiszen ezáltal jobban megérthetjük, miért is olyan fontos az ipari vállalatok digitális védelmével és az őket fenyegető kibertámadások témakörével foglalkozni.

A geopolitika a világ nemzeteinek hatalmi pozíciójával foglalkozó tudományág, amely erősen alapoz a földrajztudományra és a térbeliségre. A geopolitikai elemzések célja többnyire az erőfölény megállapítása, az ezt megváltoztató folyamatok vizsgálata, illetve javaslattétel az állami szintű vezetés számára. A kibertérrel kapcsolatos elemzések azért képezhetik a geopolitika részét, mert egyrészt maga a kibertér is értelmezhető egyfajta ötödik területként a klasszikus geopolitika által vizsgált területek – szárazföld, tengerek, légtér, világűr[1] – mellett, másrészt a kibertérnek vannak olyan konkrét fizikai infrastruktúrái, melyek védelme kiemelt fontossággal bír az állam számára.

A fizikai és elméleti terek mellett az ezekben zajló hatalmi verseny különböző szintjei, az egyes államok „viselkedése" és a konfliktusok dinamikája mind a geopolitika vizsgálati tárgyát képezik, ugyanakkor a geopolitika földrajzközpontúsága és a kibertér vizsgálata között a mai napig érzékelhető a feszültség. Nem véletlen tehát, hogy a kibertér geopolitikai vizsgálata számos kérdést vet fel. Frederick Douzet francia geopolitikai szakértő tette fel azt a kérdést, hogy vajon a kibertér tényleg egy új helymeghatározási forma lenne-e. A kibertérnek sok meghatározása van, bár egyes államok – ideértve a nagyhatalmakat, mint például Kína vagy Oroszország – még csak nem is használják ezt a kifejezést, mert azt sugallja, hogy a kibertér egy konkrét „terület", ami így más jogi megítélés alá esne, mintha egy szellemi produktumként értelmeznénk azt. Ezek az államok kommunikációjukban ezért egyszerűen „internetre" hivatkoznak.[2] A geopolitika segítségével kiemelhetjük a kibertér térbeli elemeit – nemcsak a konkrét adattároláshoz és telekommunikációhoz szükséges infrastruktúrára kell gondolnunk, hanem a szervezetekre és intézményi rendszerekre is, amelyek relevánsak lehetnek a különféle biztonságpolitikai témák elemzésében. Ilyen elemeknek számítanak többek között a nagyhatalmak helyzete, motivációik vagy befolyásuk növelésének eszközei. A geopolitika Gearóid Ó Tuathail meghatározása szerint éppen ezért úgy értelmezhető, mint a hatalom, a történelem, a földrajz, a jelen és a jövő szintetikus tanulmányozása, amelynek célja a változások tudományos „előrejelzése".[3]

Douzet rámutat arra, hogy a kibertér rétegekre bontható.[4] Ezt azért lényeges kiemelni, mert sok meghatározásbeli probléma kerülhető el azzal, hogy ha ezt a komplex fogalmat nem egy az egyben próbáljuk meg értelmezni, hanem szem előtt tartjuk, hogy egy olyan konstruált fogalomról van szó, mely sok különféle elemet foglal magába. Douzet egyúttal emlékeztet rá, hogy ezeknek a rétegeknek a száma nem egyértelmű és nincs egységes megállapodás a

1 Szilágyi, 2018, pp. 184-185.
2 Douzet, 2016, p. 23.
3 Ó Tuathail, 2003. p. 3-6.
4 Douzet, 2016, pp. 14-17.

felosztás mikéntjéről sem. Ő maga négy vizsgálandó területet emel ki elemzése során, melyek a következők: gerinc (fizikai infrastruktúra), logisztika (protokollok és tartományok), felhasználóbarát alkalmazások, valamint társadalmi és információs hálózat, más néven kognitív vagy szemantikus réteg.[5] Ez utóbbi első hallásra úgy tűnhet, hogy messze esik a geopolitikától és közelebb áll a nyelvészethez, így talán magyarázatra szorul, hogy miért szerepel mégis a vizsgálandó szegmensek között. Az információs-társadalmi réteg a geopolitika számára azért lehet érdekes, mert elősegíti a társadalmi konfliktusok megértését, vagyis például azt, hogy miért lépnek fel az emberek bizonyos régiókban a helyi hatalom ellen, vagy mi jellemzi a kormányt támogató vagy kormányellenes csoportokat egy adott országban.

A geopolitikának másrészt befolyásoló ereje is van, hiszen olyan objektív információkat nyújthat a kibertérről, amelyek egyúttal befolyásolhatják a kormányok vagy a nemzetközi politika más szereplőinek gondolkodását és cselekedeteit. A klasszikus geopolitika, mely a hidegháborús időszakig határozta meg a geopolitikai gondolkodást, inkább preskriptív irányvonalat követett, míg a mai geopolitikai elemzések, a kritikai geopolitikai megközelítés miatt a deskriptív elemzések irányába hajlanak – bár ezek szerepe sem elhanyagolható a döntéshozatal számára nyújtott információk szempontjából.

Douzet a rétegek említésekor nem tér ki külön az intézményi rétegre, amely a rendeleteknek megfelelően vagy azoknak ellenszegülve biztosítja a „gerinc" működését és adminisztrációját ezt azonban fontos szempont lehet egy elemzés során. Ez az intézményi réteg valahol a „gerinc" és a „logisztika" vagy az „alkalmazások" között jelenik meg és befolyásolja az infrastruktúra kiépítésének módját, hatással van az innovációs folyamatokra és a versenyképességre. Példa lehet erre a General Data Protection Regulation (a továbbiakban: GDPR) szerepe az európai adatgazdaság beindításában. A GDPR már megjelenésekor is vitát generált az unió tagjai között, egyes nézőpontok alapján pedig erősen befolyásolja az Unió globális versenyképességét az adatkereskedelemben.

A kibertér eredeti meghatározása William Gibson regényéből[6] származik, melyben Gibson egy olyan „térről" ír, ahol az internethasználók hozzáférhetnek a világ összes számítógépes rendszerén található adatok összességéhez. Igaz, Gibson könyve tudományos-fantasztikus regény, de munkájának köszönhetően lépett át az internetes hálózatok térbeli értelmezése a hétköznapi felfogásba, és műve hatással volt az internetszabályozásra is. Munkája nyomán alakult meg például 1990-ben az első, digitális jogokkal foglalkozó nemzetközi nonprofit szervezet, az Electronic Frontier Foundation.[7] Az alapítvány nevében a „határ" szó megfeleltethető az amerikai kontinens „vadnyugat" fogalmának, azaz az ország nem kolonizált részeit leíró fogalomnak, ami egyben az amerikai demokrácia bölcsője is.

5 Douzet, 2016 pp. 15-26.
6 Neuromancer, 1984.
7 Lásd: www.eff.org

Iparbiztonság, kritikus rendszerek és geopolitikai érdekérvényesítés

A kibertámadások kiötlőinek és végrehajtóinak motivációja igen sokszínűek mondható. A támadás kiindulópontja lehet egy aktivista hackercsoport, egy magányos, figyelemre vágyó hacker vagy akár egy állami entitás is. Jelen fejezetben a kibertámadásokat, mint a geopolitikai érdekérvényesítés eszközét vizsgálom, hogy szélesebb képet kaphassak arról, mi történhet akkor, ha egy vállalatot vagy iparágat külpolitikai hátterű támadás ér.

2019. október 9-én adta ki az Európai Bizottság azt az egész Európai Unióra kiterjedő kockázatértékelési riportot, melyet az Európai Kiberbiztonsági Ügynökség (ENISA) állított össze a tagállamok megbízott szerveinek adatai alapján. A jelentés egyebek mellett megállapítja, hogy az 5G-s hálózatok a jövőben ideális támadási felületet nyújthatnak majd a különböző érdekek mentén működő hackereknek és hackercsoportoknak, emellett az infrastruktúra bizonyos elemei a jelenleginél is érzékenyebbek lehetnek a támadásokra. A tanulmány külön kiemeli azokat a háttér- és távmenedzsment-funkciókat, melyek távoli hozzáférést nyújthatnak kritikus hálózati erőforrásokhoz. Ezenkívül a jelentés arra is rámutat, hogy a mobilszolgáltatók azon jellemző gyakorlata, mely szerint egyetlen beszállítótól vásárolják a hálózati infrastruktúrát, növelheti a kitettségét az adott hálózatnak.[8]

Egy, az Egyesült Nemzetek Szervezete (ENSZ) által elfogadott Agenda 2030 célkitűzéseinek megvalósításán dolgozó szervezet, a 5th Element Group rövid publikációjában arra figyelmeztetett, hogy a 4. ipari forradalomnak és a technológiának, illetve kereskedelemnek köszönhető lendület elvakítja az emberiséget. Emiatt pedig az olyan innovatív üzletemberek, mint például Elon Musk, rengeteg olyan információt publikussá tesznek, melyek hatásaiért így a későbbiekben nem kell felelősséget vállalniuk. Mindezt annak ellenére teszik, hogy az új technológiákban benne rejlik az a kapacitás, ami miatt akár az emberek „orwelli ellenségévé" is válhatnak."[9]

Tény, hogy napjainkban a mesterséges intelligencia, a robotika, az automatizációs folyamatok sokakban azt az érzetet keltik, hogy az irányítás kicsúszik az emberiség kezéből és így – főként a sajtóban – könnyen találkozhatunk utópisztikus, fenyegető hangvételű jóslatokkal. Az ilyen, erősen hatáskeltő megnyilvánulások szubjektív rétegével ugyan nem érdemes sokat foglalkozni, érdekes azonban elgondolkozni azon, miért tesz ilyen kijelentést egy fenntartható fejlődéssel foglalkozó globális társaság.

Világszinten az Egyesült Államok ellen indított 2001. szeptember 11-i terrortámadás jelentett olyan fordulópontot, melynek köszönhetően a kibertérből származó információk szerepe felértékelődött. Miután a globális szempontból is sokkoló terrortámadás körülményeit sikerült tisztázni, az Egyesült Államok lassan megkezdte a tömeges adatgyűjtési programjának elindítását, amelyről az Edward Snowden által nyilvánosságra hozott adatokból értesült a világ. Snowden és más, kevésbé ismert aktivisták és hackerek csoportjai rámutattak az átfogó programmal kapcsolatos szabályozási hiányosságokra.[10]

8 EU coordinated risk assessment of the cybersecurity of 5G networks, ENISA, 2019.
9 Gauri – Van Erdeem, 2019.
10 Deibert, 2020. és Snowden, 2019, p. 96-103.

Az iparbiztonság mindig fontos részét képezte a nemzetbiztonságnak, de Európában igazán nagy figyelmet akkor kapott ez a kérdéskör, amikor 2007-ben Észtországot, a kis méretű, de erősen digitalizált balti államot érte olyan orosz eredetű DDoS-támadás, mely megbénította a bankrendszert, a parlament és minisztériumok weboldalait és több médiumot is.[11] Ezt követően az állami és nemzetközi szintű kibervédelem fontosságának a 2010-es Stuxnet-támadás adott további nyomatékot, mivel a vírusról kiderült, hogy nem egyszerű féregvírus, hanem valójában állami szintű szervezetek nemzetközi összefogásának eredményeként életre hívott kiberfegyver.[12] A Krím-félsziget körül kialakult konfliktus során 2017-ben az Ukrajna létfontosságú rendszereit ért NotPetya zsarolóvírus által okozott károk jelentették a következő mérföldkövet. Az észtországi és krími támadások olyan kritikus infrastruktúrák működését lehetetlenítették el, amik leállása kihatással volt az egész országra, a NotPetya esetében pedig súlyos következményekkel járt az egész világ számára.[13] A vírus láncreakciót váltott ki a globális kibertérben, az ukrán határokon túlterjedve fennakadást okozott az Egyesült Államokban, valamint Európa-szerte több államban, főként Németországban. Az egyik, a vírus által különösen súlyosan érintett vállalat az A. P. Moller-Maersk hajózási társaság volt, amely a világ tengeri teherfuvarozásának körülbelül egyötödéért felel és a rendszerszervezési kommunikációs eszközök megbénulása miatt több hetes késést halmozott fel. A támadásról Andy Greenberg, a Wired oknyomozó újságírója úgy nyilatkozott, mint „a világ első igazi kiberháborúja", mivel az az Oroszország és Ukrajna közötti, 2014 óta tartó konfliktus egy kicsúcsosodó elemének tekinthető, amely a Krím megszállásával folytatódott.[14]

A fenti konfliktusok és a belőlük levont tanulságok, illetve a nemzetbiztonsági szolgálatok kibertérrel kapcsolatos fokozódó figyelme olyan trendeknek tekinthetők, melyek erősen befolyásolják a nemzetközi szabályozás jövőbeli fejlődését és mind geopolitikai megfigyelés tárgyát képezhetik. Ugyanakkor ezeket a globális eseményeket és az azokból kiinduló trendeket nagyon nehéz elemezni az ismeretlen részletek sokasága miatt. A kibertámadások egyre gyakoribb megjelenése és a kivédésükkel kapcsolatos problémák miatt joggal vetődik fel a szigorúbb szabályozásokra és a digitalizációs folyamatokra irányuló ellenőrzés igénye.

Ezek után a példák után nem kérdés, hogy a kibertér és azon belül az ipari folyamatokhoz tartozó kibertér védelme fontos a nemzetbiztonság, az állam megóvása szempontjából. A felkészülés érdekében szükségessé vált a szakosított intézmények (CSIRT-ek és információbiztonsági hatóságok) létrehozása mind állami, mind nemzetközi szinten. A kiberbiztonság mindazonáltal egy rendkívül összetett feladat, melynek részét képezik az államok kiberbiztonsági stratégiái, a nemzetközi és nemzeti jogi keretek, a különböző biztonsági szabványok, melyek alapján elvégezhető a sérülékenységek vizsgálata és az előírások elkészítése is. Mindemellett ki kell alakítani számos kapcsolódó szolgáltatást, például biztosítani kell a bejelentéshez szükséges információt és a bejelentések fogadásához szükséges szervezeti hátteret. Fontos továbbá a tájékoztatás, az együttműködés szorgalmazása is. Éppen ezért a feladat nem kizárólagosan az operatív szervezetek hatásköre, azok kifejezetten az incidenskezelésre jönnek létre.[15]

11 Kovács, 2018, pp. 145-148.
12 Kovács 2018, pp. 155-165.; Kovács-Sipos, 2010.
13 Kovács, 2018, pp. 131-140.
14 Rhysider, 2019, 30m35s.
15 Tikos, 2018, pp. 200-201.

Milyen folyamatok vezetnek el a modernizációs hullám kialakulásához?

Ahhoz, hogy megértsük, milyen hatással lehet a SARS-COV az ipari modernizációra, érdemes előzetesen megvizsgálni a korábbi ipari forradalmak kialakulásának körülményeit, illetve az ipari fejlődés és a válságok között fenálló kapcsolatot. Jelen fejezet tehát a bevezetőben kijelölt első tézishez tartozó első altézissel foglalkozik, vagyis azt mutatom be, hogy a koronavírus által okozott recesszió modernizációs hullámhoz vezet-e a magyar iparban, és hogy van-e összefüggés általában a válságok és az innováció között, illetve, hogy modernizációs szempontból a válság hatása értelmezhető-e pozitívumként. Ehhez először is górcső alá veszem a korábbi válságok, a biztonság kérdésének és az ipari fejlődésnek a kapcsolatát, másodszor pedig a különböző hazai és nemzetközi hírek alapján igyekszem következtetni arra, hogy a SARS-COV-járvány után várhatóan kialakul-e egyfajta ipari modernizációs hullám.

Az ipari forradalmak olyan hosszú éveken vagy évtizedeken átívelő folyamatok, amelyek teljesen átalakítják először magát a termelést (vagy azt, ahogyan a szolgáltatások elérhetővé válnak), majd ezen keresztül a társadalmat, ami önmagában is destabilizációs hatással jár a gazdasági folyamatokra nézve, azonban ezt a hatást általában egy pozitív irányba tartó strukturális fejlődés követi. Ez részben annak tudható be, hogy az emberi társadalom folyamatosan az életminőség javításán dolgozik, az ipar pedig igyekszik lépést tartani ezekkel az igényekkel.

Az ipari forradalmak a gazdaságtörténet azon pontjai, melyek során gyors ütemű változások mentek végbe. A kommunikáció, az energiahasznosítás és a mobilitás fejlődése egybeesett, aminek következtében az életszínvonal emelkedett, az üzleti modellek pedig tartós, mély strukturális változáson mentek keresztül.[16] Bár a tudomány és a technológia fejlődése folyamatosan támogatta az iparosodás fejlődését az egész világon, és az évek során finomodott az ipari forradalom kifejezés jelentése, ugyanakkor még egyetemes megállapodás nincs a definícióról. Ezért leginkább a folyamat értelmezésén keresztül alakítható ki kép arról, hogy mit is jelent az ipari forradalom.

Az ipari forradalmaknak a hagyományos megközelítés szerint[17] három szakasza különíthető el:

1. Egy konkrét gazdasági ágazatban rövid idő alatt történő változás.
2. Az ágazatban bekövetkezett változás, mely az első szakasz folytatásának tudható be és ami miatt a teljes ágazat dinamikusabb növekedésnek indul, mint a gazdaság más iparágai, megváltoztatva ezzel a szerkezeti arányokat. Ebben a szakaszban nő a kibocsátás és a foglalkoztatási részaránya az érintett ágazatnak.
3. A harmadik szakaszban a fejlődés hatásai átterjednek a többi ágazatba is.

Az első ipari forradalmat az emberiség fontos fordulópontjának tekintik, amely a 18. század végén a víz- és gőzüzemű mechanikus gyártóberendezések használatával kezdődött. Később, a 20. század elején, az elektromos meghajtású tömegtermelési technológiák alkalmazása a munkamegosztás révén a második ipari forradalom is elérkezett. Ezt követően a gyártás

16 Holodny, 2017.
17 Mokyr, 1985.

további automatizálásával az 1970-es évek közepén kezdődött a harmadik ipari forradalom, melyben már fontos szerep jutott az elektronika és az informatika széleskörű alkalmazásának és népszerűsítésének a gyárakban és a hétköznapokban egyaránt.[18] Összességében ennek a három korábbi ipari forradalomnak körülbelül két évszázadra volt szüksége a teljes kibontakozáshoz, ami elég időt biztosított az ipari létesítmények védelmére és a geopolitikai stabilitás megőrzésére. Az elmúlt években, a Dolgok Internete (azaz az Internet of Things, vagy IoT)[19] és a kiberfizikai (Cyber-physical systems, CPS) rendszerek[20] iránti fokozott figyelem mellett viharos gyorsasággal terjed a negyedik ipari forradalom. A Dolgok Internete olyan hálózatba kapcsolt hagyományos eszközöket jelent, amiknek kommunikációjára korábban nem volt igény, sem megfelelő technológia. Ilyenek például az „okos" berendezési tárgyak, mint az okoshűtő, amelyen egy kijelző segítségével azonnal lehetséges az élelmiszer-rendelés. Az ipari felhasználású eszközök esetében az IoT helyett egyre inkább szokás IIoT-ről, (Industrial Internet of Things) az Ipari Dolgok Internetéről beszélni, azonban ez a kifejezés az általános szakirodalomban még kevésbé elterjedt.

A válságok okozta innovációs hullámok különböző fajtáit több tudós és kutatóintézet is vizsgálja, vizsgálta már. A 70-es évekbeli olajválságokkal kapcsolatosan a Rapid Transition Alliance klímapolitikával és fenntartható energiagazdasággal foglalkozó intézet a következőket írja: *„A nagy innováció a válság közvetlen következményeként merülhet fel. A Kőolaj Exportáló Országok Szervezetének (OPEC) olajválságának esete megmutatja, hogy a válság eredményeként hogyan alakulhat ki a kormány által irányított energiatakarékosság és egy teljesen új, megújuló energián alapuló ipar. Az 1970-es évek elején a fosszilis tüzelőanyag-fogyasztás ugrásszerűen növekedett, és az ipar virágzott - mindaddig, amíg a közel-keleti olajtermelők sokkoló manőverben ki nem állították az ellátó csapot. Az ez által okozott mély recesszió ellenére a gazdaságok fennmaradtak és az ipar alkalmazkodott. Az olaj hirtelen hiányával szembesülve az energiatakarékosság és a hatékonyság kiemelt prioritássá vált. A megújuló energiákkal kapcsolatos kutatás szintén fokozódott. Az 1973. évi olajválság, amelynek hangos visszhangja 1979-ben volt, egyértelmű történelmi példa a gyors átmenetre, és arra, amit az emberek, a közösségek és a kormányok tehetnek, ha mozgósítják őket."*[21]

Az OECD egy 2012-es tanulmánya[22] alapján a 2008-as gazdasági válság negatív hatással volt az innovációra és a nemzeti K+F programokra. Emellett a kutatók arra is felhívják a figyelmet, hogy a válság felfedte néhány ország (például Görögország és Délkelet- és Kelet-Európa országai), az ágazatok (például az autóipar) és az innováció típusainak (például pénzügyi innovációk) a válság előtti gyengeségeit. Sok ország az innováció támogatására irányuló politikát hajtott végre a válság idején, ezzel új hangsúlyt kapott az innováció a politikai menetrendben. A válsághelyzetre adott kormányzati válaszok elsősorban az innovációra irányuló infrastrukturális beruházásokra és a vállalkozások pénzügyi forrásainak biztosítására irányultak. A válság kialakulásával számos kormány a közelmúltban kezdte csökkenteni az

18 Klingenberg-do Vale Antunes, 2017.
19 Atzori et al., 2010.
20 Monostori, 2014.
21 Rapid Transition Alliance, 2019.
22 OECD, 2012.

innovációra szánt kiadását.[23] A kutatók azonban nem a válság egyenes következményeként írják le az innováció visszaesését, azt sokkal inkább a téves helyzetértékelésből adódó hibás válságkezelés okozta, nem pedig maga a pénzügyi helyzet. A tanulmány kijelenti, hogy voltak olyan, a válság idején bevezetett politikák, melyek kedvezően hatottak az innovációra. A legtöbb ország azonban a hagyományos infrastrukturális és pénzügyi támogatási eszközökre támaszkodott, hogy a kereslet bizonytalanságának csökkentését célzó eszközökkel felgyorsíthassák a helyreállítási folyamatot. A sikertelen ágazatokat támogató helyreállítási politikák tévesnek bizonyultak, a piaci erők továbbra is gyengítik őket, mivel a válság felerősítette az amúgy is érvényes trendeket, és végül hasonló nehézségekkel kellett szembenézniük, mint a válság előtt. Az OECD-tanulmány szerint e helyett erőforrásokat kell biztosítani a növekedési potenciállal rendelkező ágazatok számára, párhuzamosan az erőforrások átcsoportosítását elősegítő iparpolitikákkal, például átképzési programok és K+F vállalkozási programok révén, amelyek csökkentik a szerkezetátalakítás költségeit. A foglalkoztatás csökkenésének elkerülésére és a képzés támogatására irányuló politikai döntések alapvető fontosságúak az innovációs rendszerek károsodásának elkerülése érdekében. A kutatók felhívják a figyelmet arra, hogy az ilyen politikák nemcsak társadalmi szempontból fontosak, hanem azért is, mert az új vállalkozások alapításának hiányából következően nincs elegendő új munkahely, ami elnyelné az azonos képzettségű munkaerőt, illetve azért is szükségesek, hogy az innovációt a megfelelően képzett munkaerő bevonásával lehessen végrehajtani.[24]

Az okos vállalkozók és cégvezetők tudják, hogy a válság nem tart örökké, és addig kell a tartalékokból gazdálkodni, amíg a fellendülés el nem érkezik. Az új gazdasági ciklus ugyanakkor valószínűleg strukturális változásokat is hoz a kibocsátás és a kereslet összetételében. Annak érdekében, hogy kihasználhassák a változó gazdasági környezetben rejlő lehetőségeket, a sikeres vállalatoknak fel kell készülniük új és továbbfejlesztett áruk és szolgáltatások nyújtására.

Joseph Alois Schumpeter elméletéből kiindulva – mely szerint a válságokból nem csak vesztesek kerülnek ki hosszú távon – olasz és brit kutatók kimutatták, hogy hosszú távon azok a cégek kerülnek ki győztesen a válságból, akik nem az innovációs kiadásokból faragnak le. Az elméletet bemutató tanulmányuk két eshetőséggel foglalkozik, a kreatív pusztítás és a kreatív felhalmozás kategóriájával. A kreatív pusztítás során a leginnovatívabb vállalatok kerülnek ki győztesen a válságból, míg a többiek elbuknak. A kreatív felhalmozás során egy lassabb és sokkal stabilabb innovációs folyamat alakul ki. A kutatók a két kategóriát egy olyan modell kidolgozására használták fel, amely segítségével képessé váltak európai vállalatok stratégiáinak elemzésére abból a szempontból, hogy hogyan teljesítettek a 2008-as pénzügyi válság előtt, közben és után.[25]

Az elemzés első jelentős eredménye összesített szinten az, hogy a válság jelentősen csökkentette azon vállalkozások számát, amelyek 38%-ról 9%-ra kívánják növelni innovációs beruházásaikat. Nem kétséges, hogy a válság – legalábbis a kezdeti szakaszában – „megsemmisítette" az innovációs beruházásokat. Az elvárásokkal ellentétben a válság vége felé a modernizációs és K+F tevékenységeiket nem a nagy tartalékkal rendelkező cégek folytatták, hanem azok, amelyek flexibilisek voltak és képesek voltak maguknak új ügyfeleket, új piacot találni.[26]

23 OECD, 2012.
24 Uo.
25 Archibugi et al., 2012, pp. 2-8.
26 Archibugi et al., 2012, pp. 26-28.

A válságok tehát amellett, hogy számos dologban különböznek egymástól, és típusuktól függetlenül a visszaesés mellett lehetőséget is rejtenek magukban. Nem tönkreteszik, hanem átalakítják a meglévő struktúrákat és oly módon rostálják meg a vállalatokat, hogy ne csak az adott korszak trendjeinek, gazdasági követelményeinek és szempontjainak megfelelőek legyenek képesek fennmaradni. Ez az átrendeződés a fennmaradó cégek esetében kedvez a fejlődésnek. Az alapján pedig, amit a korábbi ipari forradalmak vizsgálatából megtudhatunk, megállapítható, hogy az élre törő vállalatok innovációs tevékenységei befolyással vannak a versenytársaikra, valamint áttételesen az egész szektorra és iparágra nézve. A sikereket látva az innovációk egy részét tehát vélhetően egyre több piaci szereplő veszi át hullámszerűen.

Egy gyár átalakítása oly módon, hogy a munkaerő egy részét vagy egészét automatizált rendszerek helyettesíthessék, gyökeres változásokat követel. Minél elavultabb a gyár technológiai szempontból, annál nagyobb kihívás lehet megszakítani a már zajló karbantartási, fejlesztési folyamatokat és teljesen új rendszert felépíteni, hiszen meglehet, hogy minden elemet – IT-rendszerek, biztonság, belső kommunikáció, vállalatszervezés – alá kell rendelni, meg kell feleltetni az innovációnak. A válságok alapvetően azért tesznek jót az automatizálásnak, mert a leállással, a gyártósor kiürítésével és az elbocsátások magas számával olyan környezetet teremtenek, amik kedveznek egy régóta halogatott vagy éppen korábbról elhúzódó átalakításnak. Bár a kiadások magasak lehetnek, ami nem szerencsés egy kezdődő gazdasági válság idején, ugyanakkor az átalakítással járó rövidtávú hátrány olyan „szükséges rossz", amit idővel minden gyártónak vállalnia kell ahhoz, hogy alkalmazkodni tudjon a modern ipar elvárásaihoz. Ez azt jelenti, hogy ha a megfelelően végrehajtott modernizáció mellett minél előbb lép valaki, annál nagyobb hosszútávú megtérülést érhet el.

Az is egyre valószínűbbnek tűnik, hogy nem csak a rutinszerű feladatokat végző munkások félthetik a munkahelyeiket, annak ellenére, hogy ez az elgondolás szembe megy a korábbi tapasztalatokkal. Egy sokat idézett 2017-es kutatás, melyet a McKinsey Intézet készített, rávilágított arra, hogy korábban főleg az ipari, rutinszerű feladatok automatizálására volt példa az új technológiákra történő átállások esetén, most viszont több középvezetői szintű munkafolyamatot is „fenyeget" az átalakulás. A McKinsey forgatókönyv-modellezése alapján becslések szerint az automatizálás világszerte évente 0,8–1,4 százalékkal növelheti a termelékenység növekedését, annak köszönhetően, hogy 15 billió dollárnyi heti bérköltséget takarít meg a vállalatoknak.[27] Ezzel a becsléssel azonban nem árt óvatosan bánni. Egyrészt a feladatok automatizálása – főként a menedzsment szintjén – még hosszú évekbe telik majd, elsőként csak bizonyos részfeladatok robotizálására lehet számítani, ami mellett a menedzserek munkája nem veszik el, csak átalakul, például több idejük jut az ügyfelekkel való egyeztetésre. Másrészt az átalakulás számos előre nem látható tényezőt rejt magában. Fontos kérdés például, hogy vajon kell-e majd járulékot fizetni a robotok után. Elsőre ez talán futurisztikus felvetésnek tűnhet, de a nagymértékű automatizálás okán a jövőben valószínűleg szükség lesz a kiesett munkaerő után fizetett járulékok pótlására.

Bár a válságok pontos hatása előre megjósolhatatlan, ugyanakkor az kétségtelen, hogy hatásuk erősen befolyásolja az ipari modernizációt. Kérdés, hogy egy hirtelen modernizációs

27 McKinsey, 2017.

hullámra vagy egy elhúzódó, stabilabb folyamatra kell számítani. Ezt több külső tényező is erősen befolyásolja, például az, hogy milyen trendek hatása érvényesült a válságot közvetlenül megelőző időszakban.

William I. Robinson, a Californiai Egyetem professzorának kissé talán merész, de annál érdekesebb elemzése[28] alapján a világban jelenleg zajló folyamatok sebessége és átfogó jellege semmihez sem fogható. A tizennyolcadik századi ipari forradalom óta nem volt ugyanis példa olyan mélyreható változásokra, mint a kapitalista, globális átalakulás kezdetén, az 1980-as években. A professzor szerint ennek a gazdasági, strukturális átalakulásnak a következménye az, amit ma digitalizációs átalakulásnak hívunk. Állítása szerint főként azok a gazdasági szereplők igyekeztek meggyőzni a közvéleményt arról, hogy a 2008-as gazdasági válság véget ért, akik számára hasznos a fennálló kapitalista rendszer. A destabilizációs folyamatok azonban mélyen a rendszer struktúrájában gyökereznek, így előbb-utóbb mindenképpen számolni kell egy újabb, súlyos válság kialakulásával. Ez alapján elmondható, hogy a 30-as évektől számított legsúlyosabb, 2008-as gazdasági válságot kiváltó mögöttes strukturális körülmények továbbra is fennállnak, és a globális gazdaságban jelenleg zajló új szerkezetátalakítás, amely a digitalizáción és a militarizáción alapul, valószínűleg tovább súlyosbítja ezeket. A növekedés elmélete szerint azért haladhatott előre, mivel a kormányok maximálisan kihasználták a monetáris eszközöket a rendszer fenntartása érdekében. Ez az adósságvezérelt fogyasztás azonban hosszú távon további válsághullámokat gerjeszt majd.[29] Amennyiben Robinson elmélete beigazolódik, az alapvető átrendeződést okoz a nemzetközi status quo-ban.

Több tanulmányból is olyan kép tűnik ki, hogy az új digitalizációs korszakba való áttérés sebessége és összetettsége a globalizált környezetben még nem teszi lehetővé a különféle országokban és régiókban végrehajtott intézkedések hatásainak összehangolását és mély megértését. A legtöbb politika a német Industrie 4.0 politikára hivatkozik, második helyen a Made in China 2025-ös stratégia áll három hivatkozással, a harmadik helyen pedig a Factories of the Future európai terv.[30]

Az Industrie 4.0-val kapcsolatos konferenciák és tudományos dolgozatok száma 2013-tól 2015-ig fokozatosan huszonnégyszeresére nőtt. Figyelembe véve a negyedik ipari forradalom iránti növekvő érdeklődést az egész világon, felmerül a kérdés, hogy vajon mennyire tud lépést tartani ezzel a trenddel a kibervédelem.

A 2000-es években zajló digitalizációs folyamatok révén a kibertér mind fizikai (infrastrukturális), mind pedig infokommunikációs értelemben kibővül az új rácsatlakoztatott belső hálózatokkal és iparban használatos digitális eszközökkel. Geopolitikai szempontból ez a következő okok miatt érdekes:

1. Az infrastruktúra gyakran nem annak az államnak a területén található, ahol a szolgáltatást igénybe veszik. Ez a probléma már korábban is fennállt, azonban a bővülés miatt most sokkal nagyobb kockázatot rejt magában.
2. A gyors bővüléssel jogi és védelmi szempontból nehéz lépést tartani, ami sebezhetővé teszi az újonnan implementált rendszereket.

28 Robinson, 2018.
29 Robinson, 2018. pp. 78-80.
30 Liao et al., 2017.

3. A folyamat lassítása elősegíti a megfelelő védelem kialakítását, de gazdasági lemaradást eredményez.
4. A legversenyképesebb technológiák a nagyhatalmak részleges vagy teljes irányítása alatt állnak, akik érdekeik szerint képesek felhasználni azokat.

A fenti szempontok fontos szerepet játszanak a megfelelő biztonságpolitikai döntések meghozatalában. Az ENISA a Dolgok Internetét a vonatkozó weboldal első bekezdésében úgy definiálja mint *„összekapcsolt érzékelők és az azokat működtető vezérlők kiberfizikai ökoszisztémája, amelyek lehetővé teszik az intelligens döntéshozatalt"*. A meghatározásból látszik, hogy az információ az IoT-hálózatokban központi szerepet tölt be egy folyamatos érzékelési, feldolgozási és döntéshozatali ciklusba illeszkedve.[31]

Az IoT szorosan kötődik a kiberfizikai rendszerekhez, és e tekintetben lehetővé teszi az intelligens infrastruktúrák kialakítását (például: intelligens hálózatok vagy intelligens közlekedés). Az IoT-eszközökkel, rendszerekkel és szolgáltatásokkal kapcsolatos veszélyek és kockázatok sokrétűek, és gyorsan fejlődnek. A Dolgok Internetét érintő biztonsági kockázatok, amelyek nagy hatással vannak a polgárok biztonságára, védelmére és magánéletére, rendkívül széles területet ölelnek fel. Ezért fontos megérteni, hogy pontosan mit kell biztosítani és milyen operatív biztonsági intézkedéseket kell kidolgozni, amelyek segítenek megvédeni az ipari eszközöket az internetes fenyegetésektől. Az IoT biztonsági intézkedéseinek meghatározásakor nagy kihívást jelent a bonyolultság, amelyet a technológia alkalmazási területeinek sokfélesége okoz. Alapvető fontosságú az egyensúly megteremtése az egyes területek sajátosságai között, ezért fontos figyelembe venni a különféle környezetekre eső kockázatok megosztásának különbségeit.[32]

A 2008-as gazdasági válság után sokakban felmerült a kérdés, hogy vajon elérhető-e egy olyan állapot, amikor az emberiségnek már nem kell félni egy következő, hasonló helyzettől. A jelenlegi járványügyi helyzet azonban ismételten egy olyan környezetet alakított ki, amiben a gazdasági folyamatok meginognak. Bár a történések pontos láncolata megjósolhatatlan volt, a járvány kialakulására, elterjedésére és pusztítására sok szakértő figyelmeztetett. Nouriel Roubini, közgazdász és geostratégia kutató, a New Yorki Egyetem Stern School of Business professzora a Guardianban megjelent cikkében kifejti, hogy amíg a korábbi válságoknak évekre volt szükségük a kibontakozáshoz, a SARS-COV-járvánnyal járó válság gyakorlatilag egy hónap alatt alakult ki, és sokkal mélyebben megrázta a világgazdaságot.[33] Éppen emiatt a bankoknak már most engedményeket kell tenniük, hogy lassítsák a gazdasági szétesést. Ez az átalakulás kedvez a 4. (és az 5.) ipari forradalom kibontakozásának, mivel a járványügyi helyzet megmutatta, hogy mekkora szükség van a robotmunkaerőre egy egészségügyi krízishelyzetben.

Milyen élet vár ránk a SARS-COV-járvány lecsengése után? Átveszik-e a termelő személyzet munkáját a robotok? Ezek a kérdések joggal foglalkoztatják a munkavállalókat és munkaadókat, hiszen minden gazdasági válság kedvez az automatizált berendezések bevezetésének és az eddigi megfigyelések szerint a SARS-COV által okozott recesszióra ez fokozottan érvényes lesz.

31 ENISA, 2020.
32 Uo.
33 Roubini, 2020.

Az új koronavírus-járvány sok szempontból káros a munkaerőpiacra nézve. Az elmúlt hetekben a munkanélküliségi kérelmek száma világszerte rekordokat döntött, hiszen egész iparágak kényszerültek bezárni kapuikat, hogy megállítsák a SARS-COV terjedését vagy a válságban szükséges eszközök gyártására álljanak át.[34] Ennek eredményeként a gazdaság nagyot zuhant: a Dow Jones ipari átlag és az S&P 500 több mint 20%-kal esett vissza a februári legmagasabb értékekről.

Noha a karanténnal kapcsolatos intézkedések ideiglenesek, ennek a gazdasági visszaesésnek a munkaerőpiacra gyakorolt hatása hosszútávú lesz. Mark Muro, a Brookings Intézet Metropolitan Policy Programjának vezető munkatársa és politikai igazgatója a közelmúltban kollégái elemzésére[35] hivatkozva arról írt,[36] hogy a koronavírus okozta visszaesések hosszútávon ugyanúgy lendületet adnak az automata berendezések elterjedésének, mint a korábbi válságok.

Az amerikai Nemzetgazdasági Kutatóiroda két elemzője, Nir Jaimovich és Henry Siu egy kutatás során arra a következtetésre jutott[37], hogy az elmúlt harminc év három vizsgált válsága során az elvesztett munkahelyek 88%-a az automatizálható munkakörök kategóriájába esett. Egy másik kutatás alapján pedig, melyet Brad Hershbein és Lisa Kahn, a Rochesteri Egyetem kutatói végeztek több mint 100 millió álláshirdetés vizsgálatával, azt mutatja, hogy az elvesztett alacsonyan képzett munkaerőt a cégek hatékonyan tudták új technológiák különböző kombinációival helyettesíteni.[38]

Februárban több olyan cikk is megjelent az online sajtóban, ami a jelenséget úgynevezett „Fekete Hattyúként" írta le utalva Nassim Taleb világhírű könyvére.[39] Taleb azonban később egy interjúban elmondta, szó sincs hasonlóságról, hiszen a járvány és az általa okozott következmények előreláthatóak voltak.[40] Ezt a megállapítást a továbbiakban ismertetett, közelmúltban megjelent hírek bemutatásával támasztom alá.

Chris Hansen, a Valiant Capital Management vezetője már januárban reagált a koronavírus-járvány előjeleire, és a várakozásokhoz igazított stratégiájával magas hozamra tett szert bizonyos részvények shortolásával. A Valiant hajótársaságokat, repülőtársaságokat, utazási cégeket kezdett el shortolni februárban, aminek köszönhetően március végére 36%-os hozamot értek el az év elejétől számolva. A teljesítmény azért is szembeötlő, mert eközben az S&P 500 19,6%-ot, az MSCI All World Index pedig 21,3%-ot esett.[41]

Egy kínai és amerikai kutatókból álló csapat (köztük a bulvármédiában vuhani denevérhölgyként is emlegetett Zheng-Li Shi) 2015-ben publikálta azt a kutatását a Nature folyóiratban, melyben leírják, hogy a korábbi SARS-CoV-járvány mérföldkövet jelentett a fajok között terjedő vírusok kutatásában, és kijelentették, hogy több hasonló járványra lehet számítani a jövőben.[42]

34 Taylor-Schwartz, 2020.
35 Muro-Maxim-Whiton, 2020.
36 Muro, 2020.
37 Jaimovich-Siu, 2012.
38 Hershbein-Kahn, 2016.
39 Eredeti: The Black Swan, 2007.
40 Avishai, 2020.
41 Chung, 2020.
42 Menachery-Yount-Debbink, 2015.

A járvány kialakulásának lehetőségével és a terjedés módjával a hálózatkutatás tudományában tevékenykedő szakemberek közül is többen foglalkoztak[43], köztük Alessandro Vespignani és munkatársai.[44] Barabási Albert-László 2015-ben a Spektrum egy műsorában tett kijelentése a következő: *„Azt hiszem, még nem láttunk mindent. A 21. században nem az a kérdés, hogy lesz-e világméretű járvány, hanem az, hogy mikor és hogy mennyire lesz pusztító."*[45]

Egy fertőző betegségekre és közegészségügyre specializálódott doktor, Kamran Khan is kénytelen volt testközelből átélni a 2002-2004-es SARS-járványt. Khan végignézte, ahogy a várost legyűrő vírus megbénítja a kórházakat, a dolog pedig mély nyomot hagyott benne, ezért elhatározta, hogy kitalál egy módszert, amivel hatékonyabban lehet nyomon követni a betegségeket. Ennek nyomán 2008-ban létrehozott egy tudományos kutatóprogramot BioDiaspora néven, és elkezdte vizsgálni, hogyan köti össze a világ lakosságát a kereskedelmi repülés. A projekt keretében sikerült előre jeleznie a 21. század első nagy influenzajárványának terjedését, 2012-ben pedig az angol hatóságokkal közösen keresték és azonosították be a londoni olimpia járványügyi kockázatait.[46]

Az igazi áttörés végül 2014-ben jött el, amikor a cég egy nagyobb tőkeinjekciót követően felvette a BlueDot nevet, majd nem sokkal később több milliárd útiterv elemzésével sikeresen jósolta meg, hogy az Ebola-vírus hogyan és mikor fog kijutni Nyugat-Afrikából. Később a Brazíliából kiinduló Zika-vírus esetében sem fogtak mellé, és a kockázatelemzési modelljeikkel fél évvel azelőtt figyelmeztettek egy floridai járványra, hogy az kitört volna.

Larry Brilliant epidemiológus már 14 évvel korábban beszélt arról a TED globális konferencia sorozat keretében, hogy ha kitör egy világjárvány, annak milyen következményei lehetnek. Bár eddig úgy tűnik, a fertőzés mértékét jelentősen túlbecsülte – 100 millió áldozattal számolt –, ugyanakkor a gazdasági hatások tekintetében valószínűleg nem tévedett: recesszió és munkanélküliség követi a vírus által okozott járványügyi vészhelyzetet.[47]

A fent idézett kutatások arra is felhívják a figyelmet, hogy a SARS-COV-járvány nem egyedi eset, hanem az egyre gyakoribbá váló újfajta betegségek egyike, melyet a jövőben több hasonló követ majd. Ezek a felismerések nem azt jelentik, hogy a járvány felbukkanása és terjedése teljes egészében megjósolható lett volna, hanem azt, hogy más típusú válság kialakulása mellett a világjárvány eshetőségével is régóta számoltak a kutatók. Ennek a ténynek a tudatában nem csodálkozhatunk azon, ha egyes vállalattulajdonosok már a vírus terjedésének korai időszakában megkezdték a felkészülést a nehezebb gazdasági helyzettel járó vírus utáni időszakra.

43 Carey, 2020.
44 Chinazzi-Davis-Ajelli, 2020.
45 Portfolio, 2020.
46 Niiler, 2020.
47 Levy, 2020.

1. táblázat: A modernizációs hullámot erősítő folyamatok
Forrás: saját szerkesztés

A SARS-COV előtt is fennálló folyamatok	A SARS-COV miatt kibontakozó folyamatok
A 4. ipari forradalom jelenleg is zajló folyamat, mely egyre kiterjedtebb digitalizációs ökoszisztéma kiépítését követeli meg a különböző iparágakban.	A SARS-COV megmutatta, hogy az iparnak szüksége van a magasabb fokú robotizációra az egészségügyi krízissel szemben kevésbé ellenálló emberi munkaerő mellett vagy helyett.
Az elmúlt évtizedekben erősödő terrorizmusveszély és a kritikus infrastruktúrákat érő egyre gyakoribb kibertámadásokkal szemben erősebb védelemre, szigorúbb fellépésre van szükség.	A SARS-COV okozta válságban nagyobb szerepet kap a nemzetbiztonság, ami szigorúbb ellenőrzéssel is jár.
Az elmúlt két évtizedben a fejlett gazdaságokban megkezdődött az állami szintű digitalizáció, és ezzel együtt nagyobb szerepet kapott a kibervédelem. (Az Amerikai Egyesült Államokban a tömeges megfigyelés, Kínában az egyre széleskörűbben használt kamerarendszerek figyelmeztetnek erre).	A SARS-COV-járvány okot adott arra, hogy a globális technológiai vállalatok mint a Facebook, a Google, az Alibaba vagy a Tencent a nagyhatalmak kormányaival együttműködve több adatot gyűjthessenek a felhasználók készülékein keresztül (például tartózkodási helyüket illetően).

A járvánnyal kapcsolatos híreket olvasva az a benyomásunk támadhat, hogy viszonylag magas azoknak a szakembereknek a száma, akik valamilyen módon számoltak egy lehetséges válság kialakulásával. Ahhoz, hogy pontosan megállapítható legyen, mennyivel volt kiszámíthatóbb a jelenlegi válság a korábbiakhoz képest, jelen megfigyeléseknél jóval mélyebb elemzésre lenne szükség – ám esetünkben elegendő ez az információ ahhoz, hogy megállapíthassuk, a szakemberek, tanácsadók és így a vállalatok egy része tisztában volt azzal, hogy a közeljövőben kialakul egy újabb válság. Ezt feltételezve pedig megállapítható, hogy ezek a gazdasági szereplők – bár eltérő szinten – de felkészülhettek a visszaesésre.

A COVID-19 utáni modernizációs folyamatok és azok kockázatai Magyarországon

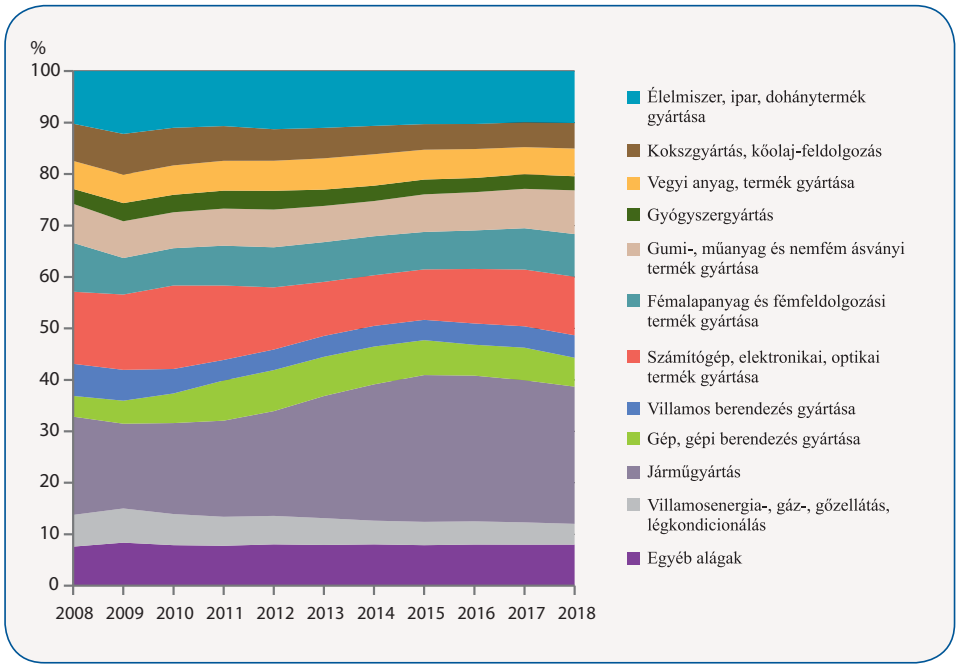
Jelen fejezetben mindkét tézis alátámasztását megkísérlem, azonban a korábbi fejezetektől eltérő szempontok alapján. Egyrészt kifejezetten a magyar iparra koncentrálok, másrészt a bevezető, témakijelölő bekezdések kivételével primer kutatáson alapuló megállapításokat teszek.

Az Nemzeti Innovációs Hivatal Kutatás-Fejlesztési Megfigyelőközpontja által közölt, a KSH által biztosított adatok alapján elkészített tanulmány szerint a GDP-arányos K+F ráfordítások nagy része a feldolgozóiparhoz kötődik, mindemellett a szakmai, tudományos és műszaki tevékenységek, valamint az oktatás hozzájárulása is jelentős. A magyar Ipar 4.0 Nemzeti Technológiai Platform alapító okiratát magyarországi telephellyel rendelkező magyar kutatóintézetek, oktatási intézmények, vállalatok és szakmai szövetségek 2016. május 6-án írták alá annak érdekében, hogy a termelés és a K+F folyamatok szabályozásának alapjait lefektessék, működési szabályzatában meghatározott küldetésének teljesítése érdekében pedig kijelölték a feladatokat ellátó munkacsoportokat.[48]

48 Lazaro, 2017.

„Az Európai Unió országai ipari versenyképességének megőrzése és fejlesztése a célja a Digitising European Industry Strategy-nak, amely az uniós „Digitális Egységes Piac" stratégia kiemelkedően fontos része. A stratégia sikere megköveteli a digitális innováció integrálását a gazdaság teljes keresztmetszetében."[49]

A KSH adatai szerint *„2018-ban Magyarország vásárlóerő-paritáson számolt egy főre jutó GDP-je az EU-28 átlagának 71%-át érte el, ami 3 százalékponttal magasabb az egy évvel korábbinál. A folyó áron számított GDP értéke 2018-ban hazánkban az uniós átlagnál erőteljesebben, 9,9%-kal növekedett."*[50] A magyar termelőiparral kapcsolatosan a következő megállapítások szolgálhatnak információval: *„A feldolgozóipar 2018-ban 3,7%-kal bővült. A három legnagyobb alág közül a legjelentősebb járműgyártás kibocsátása gyakorlatilag stagnált, ugyanakkor a számítógép, elektronikai, optikai termék gyártásáé 6,8, az élelmiszer, ital és dohánytermék gyártásáé 4,9%-kal nőtt."*[51] A 2019-es évben a GDP volumene 4,9%-kal bővült. A GDP bővüléséhez a szolgáltatások 2,3, az ipar és az építőipar 1-1 százalékponttal járultak hozzá ebben az évben.[52]



1. ábra: Az ipar termelési értékének megoszlása a jelentősebb alágak szerint
Forrás: KSH, 2018b, 14. oldal.

49 Redaktor, 2018.
50 KSH, 2019. p 1.
51 KSH, 2018a. p. 3.
52 KSH, 2020.

Az adatok alapján az ipari termelés emelkedése minden régióra érvényes volt, de legnagyobb mértékben Pest régióban volt tapasztalható a növekedés. Az ipari beruházások értéke a KSH szerint 2018-ban 2607 milliárd forint volt, ami az előző évhez képest összehasonlító áron 10%-kal több.[53] A GDP-növekedés legfőbb mozgatórugója mindkét említett évben a szolgáltatószektor volt: a villamosenergia-, gáz-, gőzellátás és légkondicionálás területén 2018-ban 39%-kal[54] nőttek a beruházások. Az energiaipari beruházásokon belül a villamosenergia-termelés területén történtek számottevő invesztíciók.[55]

A KSH adatai alapján tehát látható, hogy közvetlenül a járvány kitörését megelőző években a magyar ipari termelés – és néhány területen az iparba való beruházások – növekedtek. Jelen dolgozat vizsgálatának szempontjából kiemelt ágazatnak a gyáriparon belül a járműgyártás, a számítógépek, az elektronikai és optikai termékek gyártása, az élelmiszer, ipari és dohánytermékek előállítása, a fémgyártás és -feldolgozás, illetve a gumi-, műanyag és nemfém ásványi termékek gyártása számít. Ezenfelül a vizsgálat tárgyát képezheti a szolgáltatóipar is, bár ez egy igen összetett kategória, melybe sokféle szolgáltatás beletartozik.

A statisztikai adatok bemutatásán túl a válság utáni modernizáció magyar viszonylataival kapcsolatban érdemes megemlíteni Szalavecz Andrea munkáját, melyben a globális szervezetek reorganizációjának magyarországi leányvállalataira gyakorolt hatását vizsgálta 2016-ban. A tizenhárom autóipari, elektronikai és más gépipari céggel készített interjú alapján arra a következtetésre jutott, hogy a 2008-as válság során és azt követően végrehajtott szervezeti reorganizációs lépések egyértelműen kedvezően érintették az interjúalanyokat (egy cég kivételével). Az anyavállalatok a fejlett országokban működő leányvállalataiktól további termelési feladatokat telepítettek hazánkba. Szalavecz rámutat arra is, hogy a tudásigényes támogató funkciók helyi vagy regionális felelősségét is elnyerték, ezzel pedig bővült és mélyült a leányvállalatok fejlesztési feladatköre.[56]

A digitalizációs folyamattal és annak elemeivel kapcsolatos mérőszám, a Digitális Gazdaság és Társadalom Index (DESI) alapján 2019-ben Magyarország hátulról a 6. a sorban. Ebből nemcsak arra következtethetünk, hogy további fejlesztésekre van szükség, hanem arra is, hogy a hazai piac még telítetlen, ami kedvezhet a befektetők bevonzása szempontjából. Mint minden új informatikai modernizáció esetében, ha a bevezetés túl rövid idő alatt történik meg, akkor sokkal nagyobb az esély arra, hogy egy rendszer ki lesz téve a rosszindulatú betolakodók jelentette fenyegetettségeknek.

Modernizáció és iparbiztonság – kérdőíves kutatás

Annak érdekében, hogy megvizsgálható legyen, hogy a 2020-as járványügyi vészhelyzet során mit gondoltak a Magyarországon tevékenykedő cégvezetők az ipar digitalizálásáról és saját vállalatuk modernizációjáról, saját kérdőíves kutatást készítettem. A kérdőív 30 kérdést tartalmazott és két fő szakaszból állt. Az első szakasz a megkérdezettek véleményét volt hivatott felmérni azzal kapcsolatban, hogy számítanak-e saját iparágukon belül fejlesztési hullámra a

53 KSH, 2018a .p. 3.
54 KSH, 2018a .p. 8.
55 KSH, 2018a .p. 8,
56 Szalavecz, 2016. p. 2.

következő években, illetve terveikkel kapcsolatos kérdések is szerepeltek köztük, például hogy ők maguk terveznek-e a következő 5-10 évben nagyobb modernizációra irányuló beruházást. A második szakasz a biztonsággal kapcsolatos kérdésköröket tartalmazta.

A kitöltési időszak 2020. április 21-től április 27-ig tartott. A GKI Digital által készített, főként az e-kereskedelemre fókuszáló jelentés alapján ez az időszak a járványügyi vészhelyzet 4. szakaszába esett, melyet az ellátási láncok normalizálódása, a készlethiányok megszűnése jellemez.[57] A védekezés szempontjából a késő áprilisi időintervallum az 1. hullám végét jelentette, hiszen a kormány május 1-től vezette be az új szabályokat.[58] Ez azt jelenti, hogy ebben az időszakban már láthatók voltak a járvány által okozott első hatások, illetve már életbe léphettek az első ipari üzletvezetési módosítások a 2020-as évre vonatkozóan. Mindazonáltal nem szabad megfeledkezni arról sem, hogy a rövid időszak csak egyfajta pillanatfelvételt jelent.

A kérdőívet egy ismert ipari magazin és egy hazai, negyedik ipari forradalmi folyamatokkal foglalkozó kutatóközpont segítségével juttattuk el a válaszadókhoz. A platformokat tekintve e-mailben (hírlevél, belső kör-e-mail formájában) és Facebookon is elérhető volt a kérdőív és 86 válasz érkezett rá. A kitöltési időszak után a válaszadók közül végül csak a középvezetői és annál magasabb szintű pozícióban lévő személyek kerültek kiválasztásra, mivel a kérdésekre adott válaszok alapján láthatóvá vált, hogy az alacsonyabb beosztásokban sok a félreértés az olyan technológiák kapcsán, mint a felhőszolgáltatások, az IoT, a mesterséges intelligencia vagy az 5G. Emellett az alacsonyabb beosztásban dolgozó szakemberek nem látják át teljességgel a vállalat terveit.

2. táblázat: A kérdőíves kutatás válaszadói (*Forrás: saját szerkesztés)*

Pozíció	Szakterület
Vezető, tulajdonos	Logisztika, szállítmányozás
Vezető, tulajdonos	Üzleti szolgáltatás
Vezető, tulajdonos	Ipari IT-szolgáltatás
Vezető, tulajdonos	Építőipar
Vezető, tulajdonos	Üzleti szolgáltatás
Vezető, tulajdonos	Élelmiszeripar
Vezető, tulajdonos	Ipari IT-szolgáltatás
Vezető, tulajdonos	Robotika
Vezető, tulajdonos	Fémmegmunkálás
Vezető, tulajdonos	Egyéb gyáripar
Középvezető	Fémmegmunkálás
Középvezető	Egyéb gyáripar
Középvezető	Ipari IT-szolgáltatás
Középvezető	Egyéb gyáripar
Középvezető	Fémmegmunkálás
Középvezető	Építőipar

57 GKI Digital, 2020.
58 MTI, 2020.

A megkérdezett szakértők közül hárman nem tudták, mit jelent az IoT (sem az Internet of Things, sem a Dolgok Internete megfogalmazást nem értették), a többi válaszadó a kérdőív következő pontján szabad szöveges mezőben megadhatta, mit ért IoT-eszköz alatt. A legtöbb megkérdezett a hálózatot, az azonnali elérhetőséget, a szabályozhatóságot emelte ki definíciójában. Egy válaszadó „ismeretlen dologra való keresésként" határozta meg az IoT fogalmát.

A válaszadók közül hatan nyilatkozták, hogy vállalatuk használ valamilyen IoT-alapú eszközt, azonban arra a kérdésre, hogy milyen formában használja az eszközt egy válaszadó azzal válaszolt, hogy a „telefon és nyomtató" az, amire gondolt. Mivel ezek – a kérdőív esetében alkalmazott definíció szerint – nem tartoznak az IoT-kategóriába, így összesen öt pozitív választ fogadtam el. A megnevezett IoT-eszközök között szerepeltek okos mérőeszközök, RFID-eszközök, munkaterületek ellenőrzésére szolgáló eszközök, videórendszerekhez kapcsolt vagyonvédelmi eszközök, illetve a gyártáshoz használt gépek irányítására és működésük monitorozására használt eszközök.

A mesterséges intelligencia alkalmazásával kapcsolatban két pozitív válasz érkezett, de mivel itt is felmerült az a probléma, hogy az egyik válaszadó nem „valódi" MI-alapú rendszereket említett, csak egy választ fogadható el. Az egy pozitív válasz esetében a vállalat előrejelzésekhez, gépek optimalizálásához használja a technológiát.

A kérdőív következő része arra vonatkozott, hogy milyen változásokra készülnek a hazai ipari vezetők saját iparágukban a következő 5-10 évre vonatkozóan. Arra a kérdésre, hogy „Ön szerint saját iparágában lehet számítani modernizációs hullámra az elkövetkező 5 éven belül?" 12 pozitív válasz (igen, szinte biztosan) érkezett, ketten a „lehetséges" választ adták, illetve egy válaszadó válaszolt nemmel – ő fémmegmunkálási területen tevékenykedik.

Ezután ugyanezt a kérdést tettük fel, de a következő 10 évre vonatkozóan – itt a válaszokban csak annyi eltérés mutatkozott, hogy az előző kérdésre nemmel válaszoló kitöltő ebben az esetben a „lehetséges" pontot választotta.

3. táblázat: Milyen mértékben lehet modernizációs hullámra számítani az adott iparágban?
Forrás: Saját szerkesztés

Adható válaszok	Ön szerint saját iparágában lehet számítani modernizációs hullámra az elkövetkező 5 éven belül?	Ön szerint saját iparágában lehet számítani modernizációs hullámra az elkövetkező 10 éven belül?
Lehetséges	2	3
Igen, szinte biztosan	13	13
Nem	1	0

Érdekes a fenti elképzeléseket összehasonlítani a következő két kérdéssel, melyek lényege az volt, hogy ugyanígy az öt-, illetve tízéves időtáv tekintetében felmérje, tervez-e modernizációt az adott vállalat. Míg a fenti, az iparágakra vonatkozó kérdések során szinte alig született nemleges válasz, ebben az esetben az ötéves időtávra vonatkozóan csak nyolcan, a tízéves időtávra vonatkozóan csak tízen válaszoltak egyértelmű igennel.

4. táblázat: Lehet-e modernizációra számítani az adott vállalatnál?
Forrás: saját szerkesztés

Adható válaszok	Az Ön vállalata tudomása szerint tervez-e valamilyen modernizációt az elkövetkező 5 éven belül?	Az Ön vállalata tudomása szerint tervez-e valamilyen modernizációt az elkövetkező 10 éven belül?
Lehetséges	6	5
Igen, szinte biztosan	8	10
Nem	2	1

Külön kérdés vonatkozott arra az eshetőségre, ha az adott vállalaton belül már zajlik valamilyen modernizáció, amit a közelmúltban kezdtek el megvalósítani. A kapott válaszokat az alábbi táblázat szemlélteti.

5. táblázat: Modernizációs folyamat az adott vállalatoknál
Forrás: saját szerkesztés

Adható válaszok	Az Ön vállalatánál az elmúlt EGY évben elkezdődött valamilyen modernizáció?
Igen, több területen is	6
Igen, de csak csekélyebb mértékben	7
Egyáltalán nem	3

A kérdőív következő részében a fenti folyamatok részletesebb kifejtésére is lehetősége volt a válaszadóknak. A kérdéssor azt volt hivatott feltérképezni, hogy a következő öt-tíz éven belül pontosan milyen területeken számítanak modernizációra a vállalatvezetők és középvezetők saját iparágukban és saját vállalatukban. Az alábbi táblázatokban 1-4-es skálát alkalmaztam, melyben az 1-es jelölte, ha valaki egyáltalán nem számít modernizációra, míg a 4-es jelölte azt, ha az tervben van és biztosan be fog következni.

6. táblázat: Iparági modernizációval kapcsolatos válaszok összegző bemutatása
Forrás: saját szerkesztés

Az Ön iparágában mely területen milyen mértékű modernizációra lehet számítani Ön szerint a következő 5-10 éven belül?																
	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16
a. gyártósorok modernizációja	3	3	4	2	1	3	2	3	4	4	3	3	4	4	3	3
b. gyártósori munkaerő gépekkel történő helyettesítése	3	3	4	1	1	3	2	3	4	3	2	4	3	3	3	3
c. biztonsági személyzet gépekkel/IT-rendszerekkel való helyettesítése	2	2	3	2	2	4	3	4	4	3	2	3	1	3	2	2
d. biztonsági rendszerek modernizációja	3	3	3	3	2	4	3	4	4	4	2	3	3	3	2	3
e. kisebb elektronikai eszközök modernizációja	3	3	4	3	3	3	4	2	4	3	4	2	2	3	3	3
f. gyártóberendezések, gyártóegységek modernizációja	3	3	4	2	2	3	4	4	4	4	3	2	3	4	3	3
g. szállítmányozási eszközök modernizációja	3	3	4	3	2	2	3	3	4	3	3	2	4	3	3	3
h. szállítmányozási informatikai és kommunikációs rendszerek modernizációja	3	3	4	3	3	3	4	3	4	4	3	3	3	4	3	4
i. irodai ügyintézéssel kapcsolatos repetitív feladatok	2	3	3	3	3	2	3	4	4	3	4	2	1	3	3	4
j. irodai informatikai rendszerek, szoftverek modernizációja	2	3	3	3	3	2	4	3	4	4	3	1	3	3	3	4
k. IoT-eszközök beszerzése, modernizálása	3	2	3	3	3	3	3	3	4	3	3	1	2	3	1	3
l. Mesterséges intelligencián alapuló eszközök beszerzése, modernizálása	2	2	3	2	2	3	3	4	4	3	3	1	4	3	2	3
m. Felhőalapú rendszer kiépítése/fejlesztése	3	3	3	3	2	4	4	4	4	4	3	2	2	3	2	4

A válaszok alapján a válaszadók saját iparágukban elsősorban a következő területek modernizálására számítanak: gyártóberendezések, gyártóegységek modernizációja, kommunikációs rendszerek modernizációja, illetve a felhőalapú rendszerek bevezetése, fejlesztése.

7. táblázat: A vállalat modernizációs területei az elkövetkező öt évben
Forrás: saját szerkesztés

Ön szerint mely területeken milyen mértékű modernizációra lehet számítani az Ön vállalata esetében a következő 5 évben?																
	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16
a. gyártósorok modernizációja	1	3	1	2	1	2	3	2	1	4	2	2	1	3	3	2
b. gyártósori munkaerő gépekkel történő helyettesítése	2	2	1	1	2	2	3	3	1	3	2	1	1	3	2	3
c. biztonsági személyzet gépekkel/IT-rendszerekkel való helyettesítése	2	2	1	2	2	4	3	3	1	3	2	1	1	2	1	2
d. biztonsági rendszerek modernizációja	2	3	1	3	2	4	3	3	1	4	3	1	1	3	1	3
e. kisebb elektronikai eszközök modernizációja	3	3	2	3	3	4	4	2	4	4	4	3	1	3	2	3
f. gyártóberendezések, gyártóegységek modernizációja	3	3	1	2	3	2	4	3	1	4	3	2	1	3	3	3
g. szállítmányozási eszközök modernizációja	3	3	1	3	3	2	3	3	1	4	2	1	1	2	3	4
h. szállítmányozási informatikai és kommunikációs rendszerek modernizációja	3	3	2	3	2	2	3	3	4	4	3	1	1	3	3	3
i. irodai ügyintézéssel kapcsolatos repetitív feladatok	2	3	2	3	2	4	3	4	4	4	3	1	1	3	3	3
j. irodai informatikai rendszerek, szoftverek modernizációja	2	3	2	3	2	4	3	3	4	4	3	2	1	3	3	3
k. IoT-eszközök beszerzése, modernizálása	2	2	2	3	2	4	4	3	4	4	3	1	1	3	1	3
l. Mesterséges intelligencián alapuló eszközök beszerzése, modernizálása	3	2	3	2	1	4	3	3	4	4	3	1	1	3	1	3
m. Felhőalapú rendszer kiépítése/fejlesztése	3	3	2	3	3	4	3	3	4	4	2	2	1	3	1	3

Saját vállalatukkal kapcsolatban a megkérdezettek már sokkal konzervatívabb válaszokat adtak. Érdekes információ, hogy az egyik válaszadó egyáltalán nem számít modernizációra saját vállalata esetében. A többiek leginkább a kisebb elektronikai eszközök modernizációjára,

az irodai ügyintézéssel kapcsolatos repetitív feladatok kiváltására, illetve IoT-eszközök beszerzésére és modernizálására számítanak. Ez azt jelenti, hogy bár a többségnek erős véleménye van a saját iparágát érintő trendekkel kapcsolatban, saját vállalata modernizációjával kapcsolatban valamilyen okokból kifolyólag nem ezeket a trendeket jelölte meg. Ezen okok mélyebb feltárását hivatott vizsgálni a következő kérdéssor, melyben a megkérdezettek súlyozhatták azokat a szempontokat, amik egy esetleges modernizációs beruházásnál felmerülnek.

8. táblázat: Főbb szempontok a modernizációs beruházások tervezésénél
Forrás: saját szerkesztés

Ha Ön vezetné vállalata modernizációs programját, milyen súllyal venné figyelembe a beruházás során az alábbi szempontokat?																
	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16
a. várható költségek	4	3	3	3	3	3	3	4	3	3	3	3	1	4	3	3
b. a folyamat minél gyorsabban kivitelezhető legyen	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2
c. információbiztonság (szoftverek, képzések stb.)	4	3	4	4	3	4	3	4	4	4	3	3	3	4	4	3
d. infrastruktúra biztonsága (megfelelő implementáció, beszállítók megbízhatósága stb.)	4	3	4	3	3	4	4	3	4	4	3	3	3	4	4	3
e. régi eszközök minél nagyobb arányú cseréje, felújítása	3	3	2	3	2	3	3	3	3	3	3	3	3	4	4	3
f. élő munkaerő minél nagyobb arányú helyettesítése gépi vagy szoftveres megoldásokkal	2	3	3	3	3	3	3	3	4	2	3	1	1	3	3	3
g. meglévő élő munkaerő munkájának minél nagyobb arányú támogatása gépekkel vagy szoftveres megoldásokkal	3	3	3	3	4	3	3	3	4	4	3	4	1	3	3	4

Érdekes megfigyelni, hogy a legtöbb válaszadó az összes szempontot hasonló súllyal venné figyelembe, illetve szembeötlő, hogy a „várható költségek” opciót csak három válaszadó jelölte kiemelt fontosságú szempontnak. A válaszok alapján meglehetősen sokak számára prioritás viszont az információbiztonság és az infrastruktúra biztonsága is. A megkérdezettek közül öt válaszadó számára az emberi munkaerő gépekkel vagy szoftverekkel való támogatása is a legfontosabb szempontok közé tartozik, aminek tényleges megvalósítása a fennálló világszintű innovációs trendek szempontjából fontos lépést jelentene. A kérdőív további része a biztonsággal kapcsolatos kérdésköröket foglalta magába.

9. táblázat: A vállalat biztonságával összefüggő kérdésekre adott válaszok
Forrás: saját szerkesztés

Igazak az alábbi állítások az Ön cégére?																
	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16
a. Rendelkezik jól működő beléptetőrendszerrel	I	I	N	I	N	I	I	N	N	N	N	N	N	I	I	I
b. Rendelkezik megfelelő szoftveres védelemmel (egységes rendszer, vírusirtó stb.)	I	I	N	I	I	I	I	I	I	I	I	I	N	I	I	N
c. Az irodai infrastruktúra megfelelően védett	I	I	N	I	I	I	I	N	N	I	I	I	N	I	I	I
d. A gyártósor vagy a termeléshez, szolgáltatáshoz használt eszközök biztonságosak	N	I	N	N	I	N	I	N	N	I	I	I	N	I	I	N
e. Az Ön személyes munkaeszközein a munka biztonságosan végezhető	I	I	I	I	I	I	I	N	I	I	I	I	N	I	I	N
f. Az IT-eszközöket (laptop, mobiltelefon stb.) a munkavállalók hazavihetik	I	I	N	N	I	I	I	I	I	I	I	N	N	N	I	N
g. Az IT-eszközökön a munkavállalók a feladataikhoz nem köthető (személyes) tevékenységet is végeznek (személyes fájlok tárolása az eszközökön, Facebook, saját e-mail-cím használata, szabadidős tevékenység stb.)	I	I	N	I	I	I	I	I	I	N	I	N	N	N	I	I

Annak ellenére, hogy az előző kérdések alapján a biztonság kiemelten fontos a vállalatok vezetői számára, a következő kérdéssor alapján az alábbi következtetések vonhatók le:

- A megkérdezettek fele nem tartja biztonságosnak a gyártósor vagy a termeléshez, szolgáltatáshoz használt eszközöket.
- Három megkérdezett szerint a vállalat eszközein végzett munka nem végezhető biztonságosan.
- Tizenhatból tíz vállalat esetében a munkavállalók hazavihetik az IT-eszközeiket és tizenegy esetben megszokott, hogy azokon személyes kommunikációt folytatnak beleértve a közösségi média használatát és e-mailek küldését.

A következő kérdéssorok a biztonsággal kapcsolatos szűkebb kérdéskörökre is kiterjedtek, például az 5G-hálózat kiépítésével kapcsolatos aggályokra és elképzelésekre. IT-biztonság szempontjából főként azért lényeges, mert olyan eszközök képesek csak az 5G-hálózatra csatlakozni, amelyekben erre alkalmas chipek vannak. Az 5G technológia fejlettségi szintjét illetően pedig néhány belföldi, koreai és amerikai versenytársa mellett a kínai Huawei jár élen, így a piacszerzésnek geopolitikai, biztonságpolitikai vetületei is vannak.

Amerika kitiltotta a Huawei-t: a Huawei 2017-ben 33%-ot emelkedett a piacon, ami óriási növekedést jelent. Amerika számára az Apple pozíciójának megtartása gazdasági szempontból is fontos kérdés. De mit is jelent az 5G és miért érdekes? Az 5G fő különlegessége két tényezőn alapul: az egyik a sebessége, a másik pedig az, hogy teljesen új infrastruktúrát igényel, új eszközöket új chipekkel.[59] Az ipart három tényező befolyásolja jelentősen az elmúlt években, ezeket az alábbi táblázat foglalja össze.

10. táblázat: Az egyes technológiák hatása az iparra
Forrás: saját szerkesztés

Technológia	Hatása az iparra
IoT-eszközök	5G kommunikációra képes eszközök megjelenése
Mesterséges intelligencia, gépi tanulás	Gyors és hatékony adatfeldolgozás
Felhőalapú rendszerek	Olcsó és hatékony adattárolás
5G	Nagy adatok gyors átvitele

Ezek a folyamatok azt jelzik előre, hogy a jövőben már nem csak az olyan adatokkal lesz könnyű és olcsó dolgozni, mint amiket a mikroelektronikai eszközökbe épített egyszerű szenzorok képesek érzékelni – többek között ilyen adat a páratartalom, a rezgés vagy a fényerősség –, hanem akár nagyfelbontású videófelvételek továbbítására is lehetőség lesz, méghozzá gyorsan és hatékonyan.

Az átállás természetesen nem történhet meg azonnal, mivel a szükséges infrastruktúrának ki kell épülnie ahhoz, hogy megfelelő lefedettséget lehessen elérni az adat nagy távolságokba való továbbításához. Az átmeneti időszakban azonban fokozott veszélyeknek vannak kitéve az olyan létesítmények, ahol még nincsen kiépítve a technológiának megfelelő szintű biztonsági rendszer.

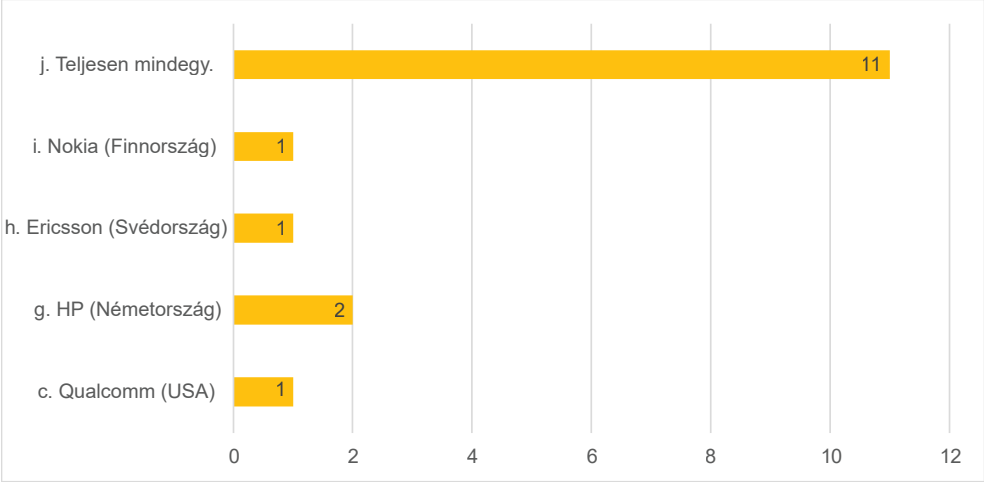
59 Index, 2020.

2. ábra: Az 5G hálózat magyarországi bevezetésével kapcsolatosan beérkező válaszok összegzése
Forrás: saját szerkesztés

Az 5G hálózattal kapcsolatos általános vélemények megoszlanak, de a megkérdezettek nagy része pozitívan áll a változáshoz. Az általános vélemény kifejtésére a következő nyitott kérdés adott lehetőséget, mely a válasz mögött megbúvó okokra vonatkozott. A válaszadók közül öten hangsúlyozták ki azt a tényt, hogy az 5G pontos természeti és egészségügyi kockázatairól nem találtak „meggyőző információt, leírást", nem ismernek „tárgyilagos forrást". Hét válaszadó kiemelte, hogy a fejlődéshez mindenképpen elengedhetetlen az 5G kiépítése, „a modernizáció igényli a nagy kapacitású, gyors és akadozásmentes kapcsolat kiépítését". Három válaszadó konkrét negatív hatás említésével válaszolt, melyek a következők: „növekszik a környezet sugárzásterhelése", „természeti pusztítás", „hosszú távú egészségügyi hatás az emberre". Egy válaszadó szerint pedig a jelenlegi sebesség is elég lenne a vállalkozás igényeihez. Véleményalkotásában csak két válaszadót befolyásol az, hogy milyen gyártó építi ki az 5G infrastruktúrát.

A következő kérdésben a válaszadóknak el kellett dönteniük, melyik vállalattal építtetnék ki legszívesebben az 5G hálózatot. A válaszlehetőségek a következők voltak: a) Huawei (Kína), b) ZTE (Kína), c) Qualcomm (USA), f) Samsung Electronics (Dél-Korea), g) HPE (Németország), h) Ericsson (Svédország), i) Nokia (Finnország), j) Teljesen mindegy.

Ha döntenie kellene, melyik vállalatra bízná inkább az 5G hálózat infrastruktúrájának kialakítását?



3. ábra: Az 5G hálózat infrastruktúrájának kiépíttetése kapcsán beérkező válaszok összegzése
Forrás: saját szerkesztés

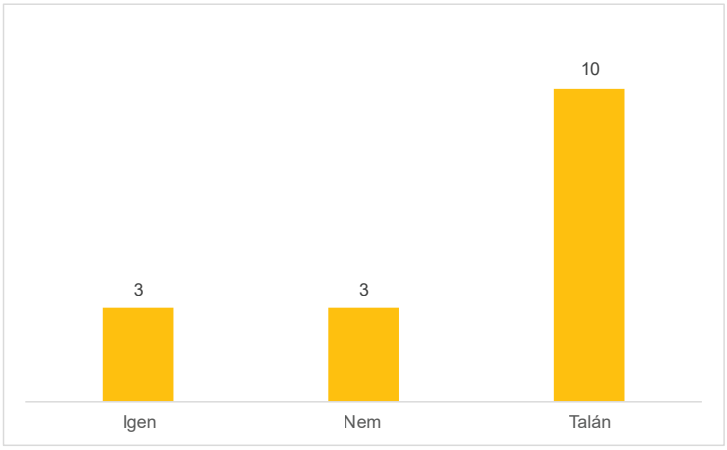
A beérkező válaszok alapján látható, hogy 16 válaszadóból 11 válaszadó az 5G hálózat infrastruktúrájának kiépíttetése kapcsán nem köteleződött el egy vállalat mellett sem, aminek több oka is lehet: például nem rendelkeznek elég információval az adott szolgáltatókról vagy nem szempont számukra a szolgáltató kiléte.

A válasz után arra kértem a kitöltőket, hogy indokolják meg, hogy miért az adott lehetőség mellett döntöttek. Akik azt a választ adták, miszerint teljesen mindegy, hogy melyik vállalat építi ki az 5G infrastruktúrát, válaszukat többnyire azzal indokolták, hogy kevés ismerettel rendelkeznek a technológiát illetően. Mindemellett abból kiindulva, hogy a felsorolásban megadott vállalat egyike sem hazai cég, mindegy melyiket választják, inkább az árajánlatok tartalma alapján döntenének a kérdésben. Akik az európai vállalatok mellett döntöttek, jellemzően biztonsági okok miatt tették ezt, vagy mert az adott vállalat olyan társadalomhoz köthető, ahol kiemelt értéket képvisel a „stabilitás, átláthatóság" és az adott nemzet „megfelelő fékekkel és felelősségtudattal rendelkezik". Az amerikai vállalatra szavazó megkérdezett csak azért döntött a Qualcomm mellett, mert szerinte az esélyesek közül ez a döntés a kisebbik rossz.

A következő két kérdés szintén az 5G-vel kapcsolatos, azonban eltérő szempontból hivatott vizsgálni a megkérdezettek véleményét. Mivel az 5G-vel kapcsolatos egészségügyi kockázatok hangsúlyozásának geopolitikai jelentősége van (emiatt akadozik a hálózat kiépítése Svájcban[60]) releváns, hogy mit gondolnak a hazai vezetők erről a kérdésről.

60 E&T, 2020.; Reuters, 2020.

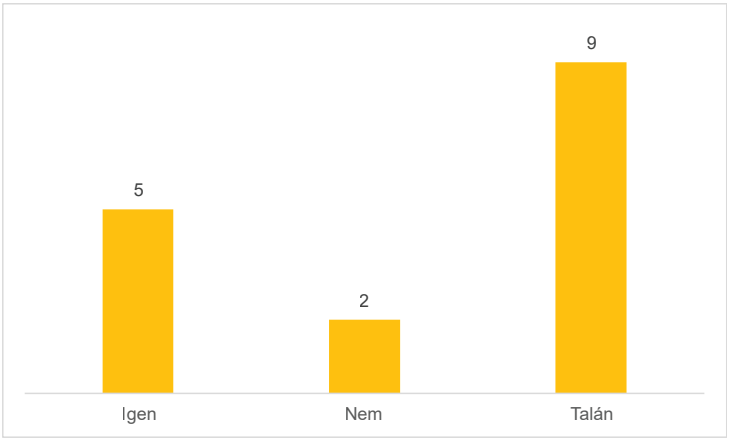
Ön szerint rejt magában egészségügyi kockázatokat az 5G?



4. ábra: Az 5G egészségügyi kockázataival kapcsolatos elképzelések
Forrás: saját szerkesztés

A fenti diagram alapján látható, hogy a legtöbb megkérdezett bizonytalan az egészségügyi kockázatokkal kapcsolatban, míg 3-3 biztos saját véleményében a technológia káros vagy veszélytelen mivoltát illetően.

Ön szerint rejt magában információbiztonsági kockázatot az 5G bevezetése?

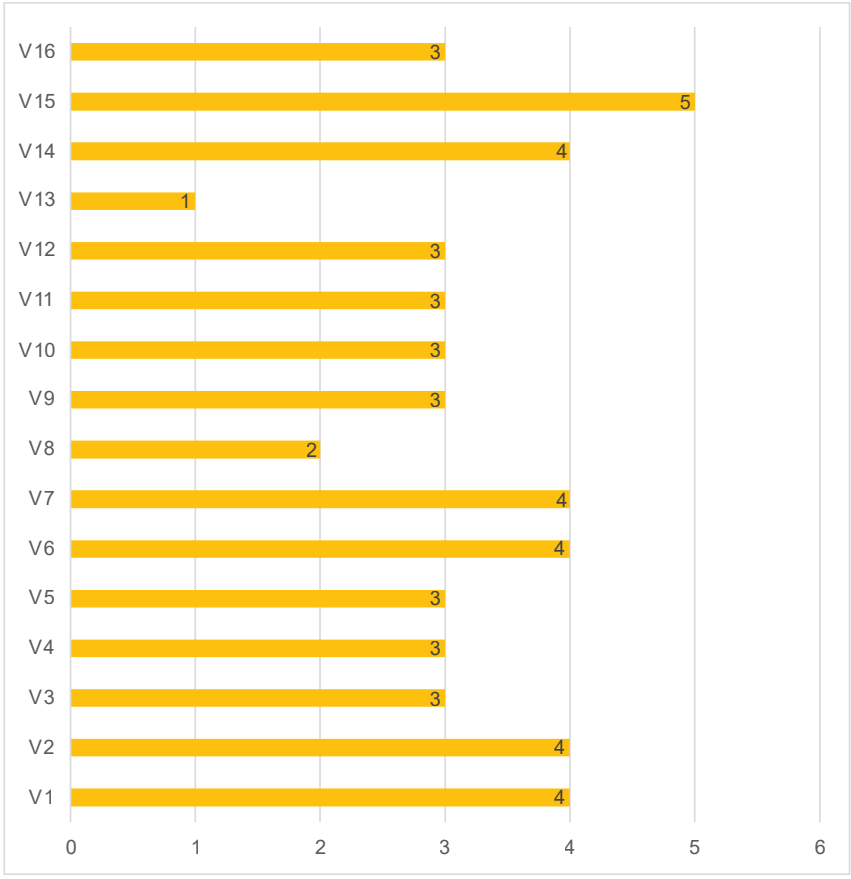


5. ábra: Az 5G információbiztonsági kockázataival kapcsolatos kérdések
Forrás: saját szerkesztés

Érdekes az a tény, hogy kilenc válaszadó bizonytalan az 5G hálózat kiépítésének információbiztonsági kockázatával kapcsolatban, öten pedig biztosak benne, hogy az új technológia rejt magában ilyen kockázatot. Továbbá az is, hogy a válaszadók szerint fontos az információbiztonság kérdése, azonban az 5G hálózatot kiépítő cég választását a vezetők nem eszerint, hanem egyéb szempontok, például árajánlat alapján kívánják eldönteni.

A kérdőív utolsó kérdése a vállalatvezetők és középvezetők biztonsággal kapcsolatos szubjektív megítélését vizsgálta a saját vállalatukra vonatkozóan, átfogó jelleggel.

Összességében hányasra értékeli a saját vállalatának biztonságát?



6. ábra: A kérdésre beérkező válaszok összegzése
Forrás: saját szerkesztés

Látványos, hogy csupán egy válaszadó értékelte a legmagasabb pontszámmal vállalata biztonsági rendszerét, míg a legtöbben a közepes osztályzat mellett döntöttek. Fontos megjegyezni, hogy ezek az értékek a válaszadók véleményét mutatják, nem pedig azt, hogy valójában

milyen erős biztonsági rendszerrel rendelkeznek. Ezt azért érdemes kiemelni, mert ebből a szempontból a közepes osztályzatok száma akár pozitív is lehet – hiszen ez arra enged következtetni, hogy a legtöbb válaszadó tisztában van az esetleges kockázatokkal és ezért meggyőzhetőbb lehet egy a vállalat biztonságának fejlesztését célzó esetleges ajánlattal kapcsolatban.

A magyarországi ipari modernizáció lehetséges jövőképei, fenyegetettségi pontjai

A kérdőíves kutatás részletezése után jelen fejezetben röviden összefoglalom a kapott eredményeket, különös tekintettel azokra a pontokra, melyek kockázati tényezőt jelenthetnek.

Az előző fejezetben közölt eredmények azt támasztják alá, hogy Magyarország vállalati szempontból is a viszonylag alacsonyan digitalizált országok közé tartozik.[61] A már meglévő trendek és tendenciák miatt a jövőben számítani lehet a digitalizáció mértékének növekedésére, főként akkor, ha a külföldi befektetők között lesznek olyan vállalatok, akik a válságból győztesen kerülnek ki. Ha azonban a vállalatok és az állam nem fordít elég hangsúlyt az innováció és modernizáció támogatására, illetve az ahhoz szorosan kapcsolódó oktatási programokra, akkor ez a jövőben nagyobb lemaradáshoz is vezethet, hiszen az adatok alapján hosszú távon a trendek erősödése várható.

Az elméleti elemzés és empirikus kutatás alapján a magyarországi ipar digitalizációjával kapcsolatban összességében a következő geopolitikai és gazdasági kockázati tényezők fedezhetők fel:

- A digitalizációs folyamat lassúsága miatt fennáll a gazdasági lemaradás veszélye.
- Az 5G bevezetése kapcsán a Huawei lehet a legesélyesebb az európai szabályozás, a vállalatvezetők általi elfogadottsága és a versenyképessége miatt.
- A dolgozók eszközhasználati szokásai (kiemelten az árnyék-IT) miatt a potenciális támadás (behatolás) kockázata növekszik.
- A biztonsággal és az 5G hálózattal kapcsolatos objektív információk hiánya miatt magasabb a helytelen döntések esélye.
- A hirtelen modernizációs hullám olyan viszonyokat teremthet, amelyek még inkább megnehezítik a komplex kibervédelmi feladatok ellátását és a sérülékenységek vizsgálatát, illetve a problémák elhárítását.

Mivel a kérdőíves kutatás alapján a vállalatvezetők egy részének nem reálisak az elképzelései saját vállalatának információbiztonsági védettségét illetően (például mert láthatóan az eszközökön végzett személyes kommunikáció lehetősége és a biztonságról kialakított kép nem áll összhangban egymással vagy mert az 5G kommunikációs hálózatok tekintetében nem állnak rendelkezésre megfelelő források), a tájékoztatás és figyelemfelkeltés kulcsfontosságú lehet a biztonságérzékelés kialakításában.

A fenti információk birtokában hasznos lehet egy információmegosztó platform létrehozása, melyen a magyar ipari szereplők a legújabb technológiákkal kapcsolatban szűrt, magyar nyelvű, hiteles tájékoztatást kaphatnak, akár több különböző forrásból is.

61 DESI, 2020.

Már léteznek Magyarországon olyan kezdeményezések, melyek tartalmait fogyasztva az érdeklődők tájékozódhatnak a modern technológiai megoldások bevezetésének folyamatáról, a szükséges tényezőkről, de ezek vagy profitorientáltak (magazinok, vállalatok híroldalai, blogjai) vagy csak egy-egy kiemelt technológia köré fonódnak (pl. mesterséges intelligenciát használó magyar vállalatokat tömörítő információs oldal).

Szükséges lenne továbbá megvizsgálni a kkv-szektor és a nagyvállalatok közötti különbségeket és a két szektor közötti kiberbiztonság szempontjából jelentős összefonódásokat. Ezt feltérképezve tisztább kép alakítható ki az olyan kockázati tényezőkről, melyek pusztán az ipari vállalatok döntéshozóinak általános válaszaiból nem következtethetők ki.

Külön figyelmet érdemel a hiteles információk terjesztése gyakorlati szempontból, hiszen ehhez fel kell térképezni, honnan tájékozódnak az ipari döntéshozók, miért pont azokat a forrásokat jelölik meg, illetve, hogy mi lenne számukra a legmegfelelőbb tájékozódási forma. Ebben a kérdéskörben vélhetően erős különbségek is lehetnek, hiszen egy elfoglalt felsővezető valószínűleg könnyebben elérhető egy iparági konferencián, ahol előad vagy kapcsolatépítés céljából részt vesz, mint egy középvezető, aki az ebédszünetben elolvassa a legfontosabb iparági híreket vagy vállalata partnereinek hírlevelét olvasva jut friss információkhoz.

Összefoglalás

A korábbi válságok és ipari forradalmak természetét vizsgáló tanulmányok alapján erős esély mutatkozik arra, hogy a koronavírus utáni válság hosszú távon felerősít bizonyos innovációs trendeket. Ez alapján a feltételezés alapján érdemes lehet megvizsgálni, hogy mely iparágakban, mely országokban, milyen technológiák kapcsán várható nagyobb eséllyel innovációs hullám, és a későbbiekben ezekre kiemelt figyelmet fordítva kidolgozhatók a megfelelő politikai döntések.

A tanulmányban szereplő kérdőíves kutatás csak néhány vállalatvezető véleményét és felkészültségét tükrözi, teljes képet nem ad a piaci helyzetről, így a kutatást érdemes lehet kiterjeszteni egy nagyobb mintára – különös tekintettel az ellentmondásos válaszokat eredményező kérdéskörökre.

Az államnak, az ipar szereplőinek és az Európai Uniónak egyszerre kell dolgoznia a biztonságos ipari digitalizáción. A feladat összetettségéből és a válság miatt kialakuló helyzetből adódóan nem lehet a megoldást csupán az egyik vagy a másik félre bízni.

Az 5G hálózatokkal kapcsolatban a fenti kutatás kiegészítéseként egy tartalomelemzés adhat átfogóbb képet arra vonatkozóan, hogy pontosan milyen információk terjedtek el a hazai médiában az egészségügyi és információbiztonsági kockázatokról. Ez segítene pontosabb képet kapni arról, hogy milyen tájékoztatási stratégiát érdemes kialakítani a vállalatok számára, milyen információkkal lehet segíteni a biztonságos átállást az új technológiákra.

Geopolitikai szempontból Magyarország számára az egyik legfontosabb kérdés a külpolitikai egyensúly keresése, a technológiai szabványok és a külföldi vállalatok beengedése a piacra, hiszen a kelet-közép európai térség részeként saját érdekeinek érvényesítését így képes megoldani. A kibervédelmi politika kialakításánál emiatt kiemelten fontos mind az Európai Unió keretrendszeréhez való illeszkedés, mind pedig a technológiai lemaradás gátlása és az új

lehetőségek keresése a megfelelő biztonsági intézkedések mellett. Az egyensúly megtartására különösen abban az esetben lesz nagy szükség, ha a kutatásunkban bemutatott tanulmányok alapján előrevetített forgatókönyv következik be, azaz a SARS-COV-járvány utáni válság mélyebb átalakulást is eredményez, felgyorsítja a geopolitikai átrendeződést és emellett szigorúbb ellenőrzést eredményez.

Irodalomjegyzék

1. Archibugi, D. - Filippetti, A. - Frenz, M. (2012): *The Impact of the Economic Crisis on Innovation: Evidence from Europe. Technological Forecasting and Social Change.* URL:https://www.researchgate.net/publication/238048698_The_Impact_of_the_Economic_Crisis_on_Innovation_Evidence_from_Europe (Utoljára letöltve: 2020. 04. 28.).
2. Avishai, Bernard (2020): *The pandemic isn't a black swan but a portent of a more fragile global system*, in: New Yorker. 2020.04.21. URL: https://www.newyorker.com/news/daily-comment/the-pandemic-isnt-a-black-swan-but-a-portent-of-a-more-fragile-global-system (Utoljára letöltve: 2020. 04. 28.).
3. Carey, Benedict (2020): *Mapping the Social Network of Coronavirus*, in: New York Times. 2020.03.13. URL: https://www.nytimes.com/2020/03/13/science/coronavirus-social-networks-data.html (Utoljára letöltve: 2020. 04. 28.).
4. Chinazzi, M. – Davis, Jessica T. - Ajelli, M. et al. (2020): *The effect of travel restrictions on the spread of the 2019 novel coronavirus (SARS-COV) outbrea*k, in: Science, Vol 368, Issue 6489. 2020.04.24. URL: https://science.sciencemag.org/content/368/6489/395 (Utoljára letöltve: 2020. 04. 29.).
5. Chung, Juliet (2020): *This Hedge Fund Saw Risks of Coronavirus Early. Now It's Up 36%*, in: Wall Street Journal 2020. 04. 02. URL: https://www.wsj.com/articles/this-hedge-fund-saw-risks-of-coronavirus-early-now-its-up-36-11585819802 (Utoljára letöltve: 2020. 04. 28.).
6. Deák Veronika (szerk.) (2018): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Nemzeti Közszolgálati Egyetem. URL: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/11181/EIB2018_50_C%C3%A9lzott%20kibert%C3%A1mad%C3%A1sok_imprim%C3%A1lt.pdf?sequence=1&isAllowed=y (Utoljára letöltve: 2020. 04. 28.).
7. Deibert, Ron: *The Geopolitics of Cyberspace after Snowden*. URL: http://currenthistory.com/Deibert_CurrentHistory.pdf (Utoljára letöltve: 2020. 04. 28.).
8. DESI (2020) Europe.ec Connectivity - Broadband market developments in the EU, Digital Economy and Society Index Report 2019. URL: https://ec.europa.eu/digital-single-market/desi (Utoljára letöltve: 2020. 04. 29.).
9. Douzet, Frédérick (2016): *Geopolitika a kibertér megértéséhez*, in: Műhelymunkák A virtuális tér geopolitikája, 2016/I. URL: http://mek.oszk.hu/16100/16182/16182.pdf (Utoljára letöltve: 2020. 04. 27.).

10. E&T (2020): *Swiss refuse to back down on 5G radiation standards, hampering rollout.* 2020.04.23. URL: https://eandt.theiet.org/content/articles/2020/04/swiss-refuse-to-back-down-on-5g-radiation-standards-hampering-rollout/ (Utoljára letöltve: 2020. 04. 29.).
11. ENISA (2019): *EU coordinated risk assessment of the cybersecurity of 5G networks.* URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049 (Utoljára letöltve: 2020. 06. 14.).
12. ENISA (2020): *IoT*. URL: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot (Utoljára letöltve: 2020. 04. 29.).
13. Gauri, P. – Van Erdeen, J. (2019): *A 5th Industrial revolution? What it is, and why it matters.* URL: https://5thelement.group/wp-content/uploads/2019/05/A-5th-Industrial-Revolution_-What-It-Is-And-Why-It-Matters_05.03.19_vX.pdf (Utoljára letöltve: 2020. 04. 29.).
14. Gibson, William (1984): Neuromancer. Ace Science Fiction Books, New York. ISBN: 9780441569595
15. GKI Digital (2020): *A koronavírus nyertese?! – lendületben az e-kereskedelem.* 2020. 05. 07. URL: https://gkidigital.hu/2020/05/07/koronavirus/ (Utoljára letöltve: 2020. 06. 21.).
16. Hershbein, Brad J. – Kahn, Lisa B. (2016): *Do Recessions Accelerate Routine-Biased Technological Change? Do Recessions Accelerate Routine-Biased Technological Change? Evidence from Vacancy Postings Evidence from Vacancy Posting.* Upjohn Institute. 2016. 10. 17. URL: https://research.upjohn.org/cgi/viewcontent.cgi?article=1272&context=up_workingpapers (Utoljára letöltve: 2020.06.29.).
17. Holodny, E. (2017): *A keyplayer in China and the EU's „third industrial revolution" decribes the economy of tomorrow*, in: Business Insider. 2017.07.16. URL: http://www.businessinsider.com/jeremy-rifkin-interview-2017-6 (Utoljára letöltve: 2020. 04. 29.).
18. Index (2020): Amerika kitiltja a Huaweit. URL: https://index.hu/aktak/huawei_kitiltas_egyesult_allamok_kina_kereskedelmi_haboru_kemkedes_nemzetbiztonsagi_kockazat_szankciok_android/ (Utoljára letöltve: 2021. 03. 09.).
19. Jaimovich, Nir – Siu, Henry E. (2012): Job Polarization And Jobless Recoveries. NBER paper series. URL: https://www.nber.org/system/files/working_papers/w18334/w18334.pdf (Utoljára letöltve: 2021. 03. 09.).
20. Klingenberg, Cristina Orsolin - do Vale Antunes, José Antônio Jr. (2017): Industry 4.0: what makes it a revolution? URL: https://www.researchgate.net/profile/Cristina-Klingenberg/publication/319127784_Industry_40_what_makes_it_a_revolution/links/5993035e458515c0ce61eb5e/Industry-40-what-makes-it-a-revolution.pdf (Utoljára letöltve: 2021. 03. 09.)
21. Kovács László (2018): *A kibertér védelme.* Nemzetközi Közszolgálati Egyetem. URL: https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf (Utoljára letöltve: 2020. 04. 29.).
22. Kovács L. - Sipos M. (2010): *A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala*, in: Hadmérnök, 5. évfolyam, 4. szám. URL: http://hadmernok.hu/2010_4_kovacs_sipos.pdf (Utoljára letöltve: 2020. 04. 29.).

23. Kralovánszky Kristóf (2019): *A kibertér fejlődése*. Hadmérnök, 14. évfolyam 4. szám, URL: http://real.mtak.hu/108269/1/HM_2019_4_Kralovanszky_Kristof.pdf (Utoljára letöltve: 2020. 04. 29.).
24. KSH (2018a): *Helyzetkép az iparról.* URL: http://www.ksh.hu/docs/hun/xftp/idoszaki/jelipar/jelipar18.pdf (Utoljára letöltve: 2020. 04. 29.).
25. KSH (2018b): *Digitális gazdaság és társadalom.* URL: http://www.ksh.hu/docs/hun/xftp/idoszaki/ikt/ikt18.pdf (Utoljára letöltve: 2020. 04. 29.).
26. KSH (2019): Statisztikai tükör. URL: http://www.ksh.hu/docs/hun/xftp/stattukor/gdp_eu/gdp_eu18.pdf (Utoljára letöltve: 2020. 04. 29.).
27. KSH (2020): *Gyorstájékoztató. Bruttó hazai termék (GDP), 2019. IV. negyedév (második becslés)* URL: http://www.ksh.hu/docs/hun/xftp/gyor/gdp/gdp1912.html (Utoljára letöltve: 2020. 06. 21.).
28. Lazaro, O. (2017): *Analysis of National Initiatives for Digitising Industry. Hungary: IPAR 4.0.* URL: https://ec.europa.eu/futurium/en/system/files/ged/hu_country_analysis.pdf (Utoljára letöltve: 2020. 04. 29.).
29. Levy, Steven (2020): *The Doctor Who Helped Defeat Smallpox Explains What's Coming*, in: Wired 2020.3.19. URL: https://www.wired.com/story/coronavirus-interview-larry-brilliant-smallpox-epidemiologist (Utoljára letöltve: 2020. 04. 29.).
30. Liao, Y., Loures, E. R., Deschamps, F., Brezinski, G., & Venâncio, A. (2018): *The impact of the fourth industrial revolution: a cross-country/region comparison.* 2018. 01. 28. URL: https://www.researchgate.net/publication/322507266_The_impact_of_the_fourth_industrial_revolution_A_cross-countryregion_comparison (Utoljára letöltve: 2020. 04. 28.).
31. McKinsey Institute (2017): *A future that works: automation, employment and productivity.* URL: https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Digital%20Disruption/Harnessing%20automation%20for%20a%20future%20that%20works/MGI-A-future-that-works_Full-report.ashx (Utoljára letöltve: 2020. 04. 29.).
32. Menachery, V., Yount, B., Debbink, K. et al. (2015): *A SARS-like cluster of circulating bat coronaviruses shows potential for human emergence.* 2015.11.09. URL: https://www.nature.com/articles/nm.3985 (Utoljára letöltve: 2020. 04. 29.).
33. Monostori, L. (2014): *Cyber-physical production systems: Roots, expectations and R&D challenges.* URL: https://www.researchgate.net/publication/263857376_Cyber-physical_Production_Systems_Roots_Expectations_and_RD_Challenges (Utoljára letöltve: 2020. 04. 27.).
34. Mokyr, J.I. (ed.) (1985): *The economics of the industrial revolution.* Rowman & Littlefield Publishers Inc., USA.
35. MTI (2020): *Hétfőtől kezdődik a védekezés új szakasza.* 2020.05.01. URL: https://koronavirus.gov.hu/cikkek/hetfotol-kezdodik-vedekezes-uj-szakasza (Utoljára letöltve: 2020. 06. 21.).

36. Muro, Mark (2020): How COVID-19 will change the nation's long-term economic trends, according to Brookings Metro scholars. URL: https://www.brookings.edu/research/how-covid-19-will-change-the-nations-long-term-economic-trends-brookings-metro/ (Utoljára letöltve: 2021. 03. 09.)
37. Muro, Mark - Maxim, Robert – Whiton, Jacob (2020): The robots are ready as the COVID-19 recession spreads. URL: https://www.brookings.edu/blog/the-avenue/2020/03/24/the-robots-are-ready-as-the-covid-19-recession-spreads/ (Utoljára letöltve: 2021. 03. 09.)
38. Niiler, Eric (2020): *An AI Epidemiologist Sent the First Warnings of the Wuhan Virus.* 2020.01.25. URL: https://www.wired.com/story/ai-epidemiologist-wuhan-public-health-warnings/ (Utoljára letöltve: 2020. 04. 29.).
39. OECD (2012): *OECD Science, Technology and Industry Outlook 2012.* URL: https://www.oecd.org/sti/sti-outlook-2012-chapter-1-innovation-in-the-crisis-and-beyond.pdf (Utoljára letöltve: 2020. 04. 29.).
40. Ó Tuathail, Gearóid (2003): *Introduction. Thinking critically about geopolitics.* in: The Geopolitics Reader, Routledge, London and New York. ISBN: 0203444930. URL: https://frenndw.files.wordpress.com/2011/03/geopol-the-geopolitics-reader.pdf (Utoljára letöltve: 2021. 03. 09.).
41. Portfolio (2020): *Itt egy videó arról, amikor a világhírű magyar tudós 5 évvel ezelőtt megjósolja a világjárványt*, in: Portfolio. 2020.03.22. URL: https://www.portfolio.hu/gazdasag/20200322/itt-egy-video-arrol-amikor-a-vilaghiru-magyar-tudos-5-evvel-ezelott-megjosolja-a-vilagjarvanyt-421126 (Utoljára letöltve: 2020. 04. 29.).
42. Rapid Transition Alliance (2019): *From oil crisis to energy revolution. How nations once before planned to kick the oil habit.* 2019.04.26. URL: https://www.rapidtransition.org/stories/from-oil-crisis-to-energy-revolution-how-nations-once-before-planned-to-kick-the-oil-habit/ (Utoljára letöltve: 2020. 04. 29.).
43. Redaktor (2018): Digitális Egységes Piac: a Digitális Innovációs Központok Munkacsoportjának harmadik találkozója az európai ipar digitális átalakításáért. in: eGov Hírlevél. URL: https://hirlevel.egov.hu/2018/06/03/digitalis-egyseges-piac-a-digitalis-innovacios-kozpontok-munkacsoportjanak-harmadik-talalkozoja-az-europai-ipar-digitalis-atalakitasaert/ (Utoljára letöltve: 2021. 03. 09.).
44. Reuters (2020): *Swiss maintain 5G emission standards amid safety concerns.* 2020. 04. 22. URL: https://www.reuters.com/article/us-swiss-5g/swiss-maintain-5g-emission-standards-amid-safety-concerns-idUSKCN22420H (Utoljára letöltve: 2020. 04. 29.).
45. Robinson I. William (2018): *The next economic crisis: digital capitalism and global police state. in: Sage.* URL: https://journals.sagepub.com/doi/pdf/10.1177/0306396818769016 (Utoljára letöltve: 2020. 04. 29.).
46. Roubini, Nouriel (2020): *Coronavirus pandemic has delivered the fastest, deepest economic shock in history.* in: Guardian. 2020. 03. 25. URL: https://www.theguardian.com/business/2020/mar/25/coronavirus-

pandemic-has-delivered-the-fastest-deepest-economic-shock-in-history?CMP=Share_iOSApp_Other&fbclid=IwAR1xiYWqB0xx3antvltQ_G0BhavbU2bbmF0guVhjQNtvhqxBwoku1KWWmc4 (Utoljára letöltve: 2020. 04. 29.).
47. Rhysider, Jack (2019): EP 54: NotPetya. URL: https://darknetdiaries.com/episode/54/ (Utoljára letöltve: 2021. 03. 09.).
48. Schwab, Klaus (2015) The Fourth Industrial Revolution. What It Means and How to Respond. in: Foreign Affairs. URL: https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution (Utoljára letöltve: 2021. 03. 09.).
49. Snowden, Edward (2019): Rendszerhiba. XXI. Század Kiadó. Budapest. ISBN 978 615 5955 69 3
50. Szalavetz Andrea (2016): *Az ipar 4.0 technológiák gazdasági hatásai –Egy induló kutatás kérdései.* in: Külgazdaság, 60. URL: http://real.mtak.hu/39363/1/Ipar40.pdf (Utoljára letöltve: 2020. 04. 29.).
51. Szilágyi István (2018): *A geopolitika elmélete* (Második, bővített kiadás). PAIGEO Alapítvány. Budapest. ISBN 978 615 80951 0 5
52. Taylor, Edward – Schwartz, Jan (2020): *Volkswagen suspends production as coronavirus hits sales.* in: Reuters. URL: https://www.reuters.com/article/us-volkswagen-results-2019-idUSKBN2140OF (Utoljára letöltve: 2021. 03. 09.).
53. Tikos Anita (2018): *Információmegosztás szervezetek és államok között célzott kiberbiztonsági incidensek esetén* in: Deák Veronika (szerk.) (2018): *Célzott kibertámadások Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára,* Nemzeti Közszolgálati Egyetem. URL: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/11181/EIB2018_50_C%C3%A9lzott%20kibert%C3%A1mad%C3%A1sok_imprim%C3%A1lt.pdf?sequence=1&isAllowed=y (Utoljára letöltve: 2020. 04. 28.)

Paráda István

Katonai kibergyakorlatok a biztonságpolitikai stratégiák és a digitalizáció célkitűzéseinek elérése érdekében

Rezümé

A NATO és az Amerikai Egyesült Államok kiberstratégiájának kialakulásából és kezeléséből tisztán következik a technológiai és informatikai fejlődésnek jelentős hatása a biztonságpolitikára nézve. Egyik jelentős eszköz – nemzetközi szinten – a biztonságpolitkiai stratégiákban meghatározott célkitűzések elérésére a katonai kibergyakorlatok végrehajtása. Ennek érdekében javaslom Magyarországon is technikai kiberbiztonsági gyakorlatokat szervezését és végrehajtását, mind biztonságpolitikai, közigazgatási szinten mind katonai vonatkozásban is.

Resume

The development and management of the cyber strategy of NATO and the United States clearly shows that technological and IT developments have a significant impact on security policy. One of the important tools, at the international level, for achieving the objectives set out in security policy strategies is the implementation of military cyber exercises. To this end, I propose the organization and implementation of technical cyber security exercises in Hungary, both at the security policy, administrative level and in the military context.

Vezetői összefoglaló

A technológiai és információs fejlődésnek és forradalomnak köszönhetően a biztonságpolitika is jelentős változásokon ment keresztül az évek folyamán. A biztonságpolitikai stratégiákban megjelentek a kibertérrel és kiberműveletekkel kapcsolatos törekvések. Ezen törekvések teljesítésének egyik módja a katonai kibergyakorlatok végrehajtása. Biztonságpolitikai és katonai összefüggésben egyaránt javaslom Magyarországon végrehajtott technikai kiberműveleti gyakorlatok szervezését.

Bevezetés

A technika folyamatos fejlődésének köszönhetően újabb biztonsági kihívások és fenyegetések megjelenésével a kiberműveletek a katonai tevékenységek mindennapi részévé váltak. Ezen képesség létjogosultságát, az Észak-atlanti Szerződés Szervezete (North Atlantic Treaty Organisation – továbbiakban: NATO), az Amerikai Egyesült Államok, valamint Magyarország is felismerte. Egyértelműen látszik, hogy szinte valamennyi ország biztonságpolitikai szempontból nemzeti szinten törekszik kibertérrel kapcsolatos biztonsági kérdésekre megoldásokat találni. A kibertér a „felhasználók, eszközök, szoftverek, folyamatok, tárolt vagy átvitel alatt lévő információk, szolgáltatások és rendszerek gyűjtőfogalma, amelyek közvetlenül vagy közvetett módon számítógép-hálózathoz vannak kapcsolva".[1]

Amennyiben magáról a biztonságról vagy a kiberműveletek nemzeti léptékű kezeléséről beszélünk, az azt jelenti, hogy stratégiai szinten kell annak értelmezését végrehajtani. Kérdésként merül fel, hogy a nemzeti stratégiák milyen módon kezelik az informatikai revolúciót és a vele járó lendületes ütemű információs és technológiai fejlődést. Figyelmen kívül hagyják őket, vagy beépítődnek a folyamatokba, esetleg kihasználják a bennük rejlő lehetőségeket?

A nemzeti biztonsági és nemzeti katonai stratégiák szemszögéből hazánk és a Magyar Honvédség is jelentős kihívásokkal áll szemben a kiberműveleti képességek fejlesztése terén. Az ezzel kapcsolatos munkának rengeteg eredményét látni, mint például a Magyar Honvédség Kibervédelmi Akadémiájának[2] létrehozását Szentendrén. A Magyar Honvédség számos kibervédelmi elvárásnak kíván eleget tenni mind állami, nemzeti és katonai oldalról, összhangban hazánk jelenlegi Nemzeti Biztonsági Stratégiájával[3], Nemzeti Katonai Stratégiájával[4], valamint a Nemzeti Kiberbiztonsági Stratégiájával[5]. Ezenfelül meghatározható, hogy Magyarországon a biztonságpolitikai és katonai kiberműveleti törekvések a 2013. évi L. az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvénnyel[6] összhangban valósulnak meg.

A stratégiákban meghatározott képességek kialakítása, fejlesztése és elérése érdekében számos szövetséges és szomszédos nemzet is jelentős hangsúlyt fektet az informatikai biztonsági, illetve kiberműveleti gyakorlati képzésre és oktatásra. Ennek egyik módszere a katonai kibergyakorlatok tervezése és végrehajtása, melyek készség szinten segítik elsajátítani az adott tudást. Ezek a gyakorlatok több szinten, többek között stratégiai – vezetői és döntéshozói – valamint technikai, szakmai szinten is megvalósulnak. A katonai kibergyakorlatok nagymértékben hozzájárulnak a nemzeti biztonsági, a nemzeti katonai, valamint a nemzeti kiberbiztonsági startégiák célkitűzéseinek eléréséhez.

Mindezért rendkívül fontosnak tartom a nemzeti biztonsági, katonai és nemzetbiztonsági stratégiákon belül a kiberstratégiák szerepét, valamint azok kapcsolatát a katonai

1 Kovács László, A kibertér védelme, Budapest: Dialóg Campus Kiadó, 2018. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf (letöltve és megtekintve: 2020. 03. 30.)
2 Draveczki-Ury Ádám, Átadták a Magyar Honvédség Kiber Képzési Központját 2019. 06. 13. 12:00 https://honvedelem.hu/galeriak/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat/ (letöltve és megtekintve: 2020. 03. 30.)
3 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
4 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról
5 1139/2013. (III. 21.) Korm. határozat
6 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

kibergyakorlatokkal, hisz ezek mind katonai, mind biztonságpolitikai szempontból előnyös helyzetet, és folyamatos fejlődési és előnyös digitális pozíciót eredményeznek az ilyen gyakorlatokat megszervezni és lebonyolítani képes nemzeteknek.

A NATO kibervédelmi irányelveinek fejlődése

Napjainkban az információs és az infokommunikációs technológia használata alapszolgáltatásnak minősül. Életünk szinte valamennyi szegmensére hatást gyakorol a pénzügyi ügyletektől kezdődően a munkahelyi kötelezettségeinken keresztül az egyszerű tevékenységeinkkel bezárólag. Amennyiben katonai oldalról vizsgáljuk meg a kérdéskört, akkor egyértelművé válik, hogy az informatikai, távközlési és elektronikai technológia rohamos fejlődése kikerülhetetlenül elérte a biztonságpolitika területét is. E fejlődés és ennek nyomán a kiberműveletek megjelenése hatással van a politikai és a gazdasági szektorra, valamint a fegyveres erőkre is.[7] Magyarország NATO-tagállamként betartja és teljesíti a Szövetség alapokmányában foglaltakat.

A kiberirányelvekkel kapcsolatos folyamatok bemutatása előtt fontos rögzíteni a kiberbiztonság meghatározását. A kiberbiztonság meghatározása a Nemzetközi Távközlési Egyesület (International Telecommunication Union) ITU-T X.1205 jelzésű dokumentuma alapján a következő: *„A kiberbiztonság az eszközök, a politikák, a biztonsági koncepciók, a biztonsági garanciák, az iránymutatások, a kockázatkezelési megközelítések, a cselekvések, a képzés, a legjobb gyakorlatok, a biztosítékok és a technológiák gyűjteményét jelenti, amelyek a kiberkörnyezet, a szervezet és a felhasználói eszközök védelmére használhatók. A szervezet és a felhasználói eszközök közé tartoznak a számítástechnikai eszközök, a személyzet, az infrastruktúra, az alkalmazások, a szolgáltatások, a telekommunikációs rendszerek, valamint a továbbított és/vagy tárolt információk összessége a kiberkörnyezetben. A kiberbiztonság célja a szervezet és a felhasználók eszközei biztonsági tulajdonságainak elérése és fenntartása a kiberkörnyezetben meglévő biztonsági kockázatokkal szemben.”*[8]

A NATO 2007 óta kiemelten kezeli a kibervédelem és a kiberhadviselés kérdéskörét. Számos adat van a 2007-ben Észtország ellen indított kiberműveletekről, amikor meghatározó jelentőségű szolgáltatásmegtagadást (Denial of Service – DOS) kiváltó támadássorozat történt. 2007 áprilisában Tallinnban egy második világháborús szovjet emlékmű eltávolítását az észtországi orosz lakosság nagy felháborodással fogadta. Ezzel egy időben internetes támadások érték az észt informatikai és távközlési infrastruktúrát, főként az országon kívülről. A valószínűsíthető orosz támadások az Észtország és Oroszország közötti nézeteltéréseknek tulajdoníthatók. Az incidens a hadviselés teljesen új formáira irányította a figyelmet. Az esemény jelzésértékű példa arra, hogy az infokommunikáció milyen fontos szerepet játszik a társadalomban. Az eseménysorozat egyértelművé tette, hogy a NATO-nak az új kihívásokra reagálnia kell, és fel kell ismernie a megfelelő képességek fejlesztésének szükségességét.

7 Jobbágy Szabolcs, Az információs társadalom, az informatika és a távközlés konvergenciája. Múlt, jelen, jövő. Hadmérnök IV. évfolyam 1. szám, 2009. március, 185–188. http://www.hadmernok.hu/2009_1_ jobbagy.pdf (letöltve és megtekintve: 2020. 03. 30.)

8 ITU-T X.1205 telecommunication standardization sector of ITU (04/2008) series x: data networks, open system communications and security telecommunication security overview of cybersecurity. 8. https://www.itu.int/rec/T-REC-X.1205-200804-I (letöltve és megtekintve:2020. 03. 30.)

Különösképpen azért is, mert – az Észak-atlanti Szerződés Szervezete megalakulásakor, Washingtonban, 1949. április 4-én aláírt Alapokmány 5. cikkelye, azaz a kollektív védelem értelmében – egy NATO-tagországot ért támadás a szervezet elleni támadásnak tekintendő. A NATO Alapokmány 5. cikkelye erről a következőképpen rendelkezik: „*A Felek megegyeznek abban, hogy egyikük vagy többjük ellen, Európában vagy Észak-Amerikában intézett fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek; és ennélfogva megegyeznek abban, hogy ha ilyen támadás bekövetkezik, mindegyikük az Egyesült Nemzetek Alapokmányának 51. cikke által elismert jogos egyéni vagy kollektív védelem jogát gyakorolva támogatni fogja az ekként megtámadott Felet vagy Feleket azzal, hogy egyénileg és a többi Féllel egyetértésben azonnal megteszi azokat az intézkedéseket – ideértve a fegyveres erő alkalmazását is – amelyeket a békének és biztonságnak az észak-atlanti térségben való helyreállítása és fenntartása érdekében szükségesnek tart.*”[9] Az észt informatikai és távközlési infrastruktúra megbénítását eredményező támadást felismerve a NATO szükségszerűnek látta kiberbiztonsággal és kiberműveletekkel kapcsolatos intézkedések bevezetését.

A Szövetség 2008-ban megalapította a Kooperatív Kibervédelmi Kiválósági Központot (Cooperative Cyber Defence Centre of Excellence – továbbiakban: CCDCOE). Az intézmény a kiberműveletek és a kiberbiztonság oktatásával, kutatásával és fejlesztésével foglalkozik, továbbá a műszaki-technológiai nézőpontokon kívül vizsgálja az erkölcsi, illetve a jogi kérdésköröket is. A CCDCOE alapításának elgondolását a szövetséges erők transzformációs főparancsnoka 2006-ban hagyta jóvá. A támogatónemzetek tárgyalásai 2007-ben kezdődtek, végül az egyetértési megállapodást 2008-ban írták alá. Az alapító tagokon kívül folyamatosan csatlakoznak a NATO-tagállamok közül a támogatónemzetek, köztük 2010-ben Magyarország is.[10] A 2007-es események következményeként a nyilatkozatokban is egyre nagyobb hangsúlyt kaptak a kiberbiztonságról és a kiberműveletekről alkotott elképzelések, ahogyan az már jól látható a 2008-as bukaresti csúcstalálkozó nyilatkozatán is.[11]

A lisszaboni csúcstalálkozón 2010-ben elfogadtak egy új stratégiai tervezetet, amelyben az Észak-atlanti Tanácsnak (North Atlantic Council – NAC) feladata volt egy alapos, új NATO kibervédelmi politika kidolgozása és egy végrehajtási terv elkészítése. Az Alapokmány 5. cikke értelmében a fegyveres támadások körét bővítették a kollektív védelem vonatkozásában.[12] A lisszaboni csúcstalálkozó nyilatkozata az előzőekhez képest részletesebb információkat tartalmazott a kiberbiztonság kérdéskörével kapcsolatban. Megjelent a kibertér fogalma és fontossá vált a kibervédelem a konfliktusok kezelésében. Jelentős szerepet kapott a képességek elérésének felgyorsítása, valamint a tervezési folyamatok szükségessége a szövetségesek segítésére.[13]

9 Az Észak-atlanti Szerződés, Washington DC, 1949. április 4., 1. 5. cikk https://www.nato.int/cps/ic/natohq/official_texts_17120.htm?Selectedlocale=hu (letöltve és megtekintve:2020. 03. 30.)

10 Kovács László–Szentgáli Gergely, National Cyber Security Organization: Hungary. 11. Tallinn, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_HUNGARY_2015-10-12.pdf (letöltve és megtekintve: 2020. 03. 30.)

11 Bucharest Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008. https://www.nato.int/cps/en/natolive/official_texts_8443.htm (letöltve és megtekintve: 2020. 03. 30.)

12 Szentgáli Gergely, A NATO kibervédelmi politikájának fejlődése. Bolyai Szemle XXI. évf. 2. szám, 2012, 80–85. http://archiv.uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf (letöltve és megtekintve: 2020. 03. 30.)

13 Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon 19–20. November 2010. https://www.nato.int/cps/ua/natohq/official_texts_68580.htm (letöltve és megtekintve: 2020. 03. 30.)

A 2012. májusi chicagói csúcstalálkozón a szövetségesek vezetői megerősítették elkötelezettségüket, hogy javítsák a Szövetség kibervédelmét oly módon, hogy valamennyi NATO-hálózatot központi védelem alá helyezték, és jelentős fejlesztéseket hajtottak végre a számítógépes incidenskezelő képesség (NATO Computer Incident Response Capability – továbbiakban: NCIRC) területén. A Lisszabon utáni kibervédelmi elgondolás, -politika és cselekvési terv elfogadásával integrálták az újabb kibervédelmi intézkedéseket a Szövetség rendszereibe és eljárásaiba.

2014 májusában a NCIRC elérte teljes működőképességét, ami fokozott védelmet biztosított a NATO-hálózatok és -felhasználók számára. A 2016. szeptemberi walesi csúcstalálkozón a szövetségesek támogatták az új kibervédelmi politikát, és jóváhagytak egy új cselekvési tervet, amely a politikával együtt hozzájárul a Szövetség alapvető feladatainak teljesítéséhez. A politikát és végrehajtását a Szövetségen belül mind politikai, mind technikai szinten szoros felülvizsgálat alatt tartották, és a kiberfenyegetésnek megfelelően frissítették. A NATO és az Európai Unió (a továbbiakban: EU) 2016. február 10-én megkötötte a kibervédelemről szóló technikai megállapodást, miszerint mindkét szervezet megfelelő segítséget nyújt a kibertámadások megelőzéséhez és a reagáláshoz. Ez a technikai megállapodás az NCIRC és az EU számítógépes vészhelyzeti reagáló csoport (Computer Emergency Response Team EU – CERT-EU) között keretet biztosít az információcseréhez és a legjobb gyakorlatok megosztásához a válságkezelő csoportok között.

2016. június 14-én a védelmi miniszterek megállapodtak abban, hogy a varsói csúcstalálkozón dimenzióként ismerik el a kiberteret. Ez a Szövetség jelenlegi működési területeinek – levegő, víz, szárazföld és világűr – a kiegészítése egy újabbal. A kiberteret illetően számos meghatározással találkozhatunk, a sok közül egyet emelnék ki. Az Amerikai Egyesült Államok Védelmi Minisztériumának hivatalos szótára alapján a kibertér *„az információs környezetben az egymással kölcsönös függőségben lévő információs infrastruktúrák hálózata és a bennük lévő adatok által létrehozott globális tartomány, amely magában foglalja az internetet, a távközlési hálózatokat, a számítógépes rendszereket, valamint a beépített feldolgozó és vezérlő elemeket”*.[14] Ez a felismerés nem változtatja meg a NATO küldetését vagy megbízását, amely egyértelműen védekező. Akárcsak a cselekvés minden területén, a NATO a nemzetközi joggal összhangban jár el. A Szövetség elismerte az egyéb nemzetközi fórumokon tett erőfeszítéseket is, melyek arra irányultak, hogy kidolgozzák a felelősségteljes állami magatartás normáit és a bizalomépítő intézkedéseket, és elősegítsék a nemzetközi közösség átláthatóbb és stabilabb kiberterének létrehozását. A 2016. júliusban rendezett varsói csúcstalálkozón a szövetséges állam- és kormányfők ismét megerősítették a NATO védekező megbízatását és a már elismert kiberteret a műveletek egyik területeként, amelyben a NATO-nak hatékonyan meg kell védenie magát, mint ahogyan azt teszi a többi négy dimenzióban. A szövetségesek is kötelezettséget vállaltak arra, hogy nemzeti hálózataik és infrastruktúráik kibervédelmét előtérbe helyezzék. A NATO és az EU 2016. december 6-án több mint 40 olyan intézkedést fogadott el, amelyek elősegítik a két szervezet együttműködését, beleértve a hibrid fenyegetések[15] elleni küzdelmet,

14 Joint Publication 3-12 (R) Cyberspace Operations. 5. Feb 2013, 69. http://www.dtic.mil/doctrine/new_ pubs/jp3_12R.pdf (letöltve és megtekintve: 2020. 03. 30.)

15 Babos Tibor, Hibrid hadviselés a NATO-ban, Honvédségi Szemle 6. évfolyam 6. szám 2010. november, HU ISSN 2060-1506 http://193.22Ő.76.Ő/download/konyvtar/digitgy/tartalomjegyz/honv_szemle_2010_6.pdf (letöltve és megtekintve: 2020. 03. 30.)
(„Hibrid fenyegetéseknek azon képességeket nevezzük, amelyek révén az ellenfelek hagyományos és nem hagyományos eszközöket egyidejűleg, adaptívan tudnak alkalmazni saját céljaik elérése érekében.”)

a kibervédekezést és a közös szomszédságuk stabilabbá, illetve biztonságosabbá tételét. A kibervédelem területén a NATO és az EU közös gyakorlatokat tart, elősegítik a kutatást, a képzést és az információk megosztását.

„(70.) A kibertámadások egyértelműen kihívást jelentenek a Szövetség biztonsága szempontjából, és ugyanolyan károsak lehetnek a modern társadalmak számára, mint a hagyományos támadások. Walesben megállapodtunk abban, hogy a kibervédelem része a NATO kollektív védelmi feladatainak. Most Varsóban megerősítjük a NATO védelmi mandátumát, és elismerjük a kiberteret olyan műveleti területnek, amelyben a NATO-nak olyan hatékonyan kell megvédenie magát, mint a levegőben, a szárazföldön és a tengeren. Ez javítani fogja a NATO azon képességét, hogy ezeken a területeken védje és végezze műveleteit, és minden körülmények között megőrizze cselekvési és döntéshozatali szabadságát. Továbbá támogatja a NATO szélesebb körű elrettentését és védelmét: a kibervédelem továbbra is beépül a működési tervezésbe és a Szövetség műveleteibe és küldetéseibe, és együtt fogunk dolgozni, hogy hozzájáruljanak a sikerhez. Ezenkívül biztosítja a NATO-kibervédelem hatékonyabb megszervezését és az erőforrások, készségek és képességek jobb kezelését. Ez a NATO hosszú távú alkalmazkodásának része. Továbbra is végrehajtjuk a NATO-nak a kibervédelemre vonatkozó továbbfejlesztett politikáját, és megerősítjük a NATO kibervédelmi képességeit, kihasználva a legújabb élvonalbeli technológiákat. (71.) Biztosítjuk, hogy a szövetségesek megfeleljenek a 21. századra szabott követelményeknek. Napjainkban a Kibervédelmi Vállaláson (Cyber Defence Pledge) keresztül elköteleztük magunkat nemzeti hálózataink és infrastruktúráink kibervédelmének növelése mellett. Támogatjuk a NATO kibervédelmi gyakorlat (Cyber Range) képességét és hatókörét, ahol a szövetségesek készségeket építhetnek, növelhetik a szakértelmet és megismerhetik a legjobb gyakorlatokat.”[16]

A védelmi miniszterek egy frissített kibervédelmi és egy cselekvési tervet fogadtak el 2017. február 16-án a kibertér műveleti területként történő elismerésére. Ez növeli a szövetségesek együttműködési képességét, képességeinek fejlesztését és az információk megosztását. A védelmi miniszterek 2017. november 8-án elvben egyetértésüket fejezték ki egy új Kiberműveleti Központ (Cyber Operations Center) létrehozásáról az adaptált NATO-parancsnoki struktúra körvonalazásának részeként. Ez erősíti a NATO kibervédelmét, és segít a kiberintegrációs tervezésben és működésben. A miniszterek megállapodtak abban is, hogy integrálják a szövetségesek nemzeti kiberképességeit a NATO-missziókba és műveletekbe. A szövetségesek fenntartják a hozzájárulások teljes tulajdonjogát, ahogyan a szövetségesek a NATO-missziókban a tankok, a hajók és a repülőgépek tulajdonjogait.

Összegzés

A NATO mindig is védte kommunikációs és információs rendszereit, de először a 2002-es prágai csúcstalálkozó vette napirendre a kibervédelmet. A szövetséges vezetők 2006-ban a rigai csúcstalálkozón felismerték, hogy további védelmet kell biztosítani ezeknek az információs rendszereknek. Az Észtország állami és magánintézményei ellen 2007-ben végrehajtott

16 NATO Summit Guide Warsaw, 8–9. July 2016, 124–128. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf (letöltve és megtekintve:2020.03.30)

kibertámadások nyomán a szövetséges védelmi miniszterek ugyanezen év júniusában megállapodtak abban, hogy e területen jelentős munkára van szükség.

Egyértelműen látszik, hogy a NATO felismerte az új biztonsági kihívásokat, és lépéseivel reagálni kíván a bekövetkezett eseményekre és a folyamatosan változó helyzetre. Ezen túlmenően fejleszteni akarja az eddig elért és alkalmazott képességeit a kérdéskörrel kapcsolatban, illetve támogatni kívánja az oktatási, gyakorlatorientált ismeretterjesztési, a tudományos és a kutatási irányvonalakat. Továbbra is alapvető a NATO védelmi jellege, és elismerték a kiberteret a műveletek egyik dimenziójaként, amelyben a NATO-nak olyan hatékonyan kell megvédenie magát, mint a levegőben, a szárazföldön és a tengeren. A NATO megerősíti a kiberoktatásra, -képzésre és -gyakorlatokra vonatkozó képességeit. A NATO kibergyakorlatokat is szervez, és végre is hajt a tagállamok bevonásával, mint például a Locked Shields. A gyakorlatot a Nemzetközi katonai kibergyakorlatok című fejezetben részletesen bemutatom.

Véleményem szerint a NATO időben felismerte a kibervédelem és a kiberműveletek fontosságát. Jelentős erőfeszítéseket tett és fog tenni az ehhez kapcsolódó képességek kialakítására és fejlesztésére, így Magyarországnak és a Magyar Honvédségnek is hasonlóképpen kell eljárnia. A Magyar Honvédségen belül a kiberbiztonsági stratégiával összhangban a kiberbiztonsági képességek fejlesztése létfontosságú lehet a jövőben elvégzendő feladatok szempontjából, melynek egyik alappillére kell, hogy legyen egy hazai katonai kiberbiztonsági gyakorlat.

Az Amerikai Egyesült Államok kibervédelmi irányelveinek fejlődése

Az Egyesült Államok világviszonylatban élvonalban jár a kiberbiztonsági politikák és stratégiák megvalósításában. A szövetségi kormány már 2003-ban kiadta az első nemzeti számítógépes biztonsági stratégiát.[17] A dokumentum három stratégiai célkitűzést fogalmazott meg:

- a kritikus infrastruktúrák elleni kibertámadások megelőzését;
- az internetes támadásokkal szembeni sebezhetőségek minimalizálását;
- az internetes támadások által okozott károk és a helyreállítási idő csökkentését.

E célok elérése érdekében öt nemzeti prioritást határoztak meg:

- szövetségi számítógépes rendszerek és hálózatok biztosítása;
- a reakcióképesség fejlesztése;
- fenyegetéseket és sebezhetőséget csökkentő program létrehozása;
- tudatosságnövelő és képzési program a kiberbiztonságról;
- a nemzetközi együttműködés rendszere.

A következő szakaszban időrendben áttekintem a legfontosabb stratégiai okmányokat és a szövetségi törvényeket, beleértve az amerikai elnökök végrehajtható végzéseit a kiberbiztonságról.

17 The White House, 'The National Strategy to Secure Cyberspace', 2003 https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (letöltve és megtekintve: 2020. 03. 30.)

Ezek a dokumentumok magukban foglalják:

- a nemzeti kritikus infrastruktúrák védelmét, valamint a szövetségi számítógépes rendszerek és hálózatok biztonságát;
- a szövetségi, állami, helyi, területi és magánpartnerek szerepének és felelősségének meghatározását;
- a nemzetközi és a nemzetbiztonsági, a védelemi és a kémelhárítási kiberbiztonságának szempontjait.

A kilencvenes évek eleji kiberbiztonság kellemetlen problémává vált a létfontosságú nemzeti biztonság szempontjából. Az amerikai kiberbiztonsági irányelv a kritikus infrastrukturális védelmi erőfeszítésekben gyökerezik. 1996-ban Bill Clinton elnök kiadta a „Kritikus infrastruktúra védelme" című 13010. számú végrehajtási rendeletet.[18] A határozat létrehozta a Kritikus Infrastruktúra Elnökségi Bizottságát, amely felhívta a figyelmet az internetes támadásokra és a nemzetbiztonsági fenyegetésekre. Az 1998. évi 63. elnöki határozati irányelv (Presidential Decision Directive – a továbbiakban: PDD)[19] létrehozott egy struktúrát a Fehér Ház vezetése alatt a szövetségi kormány tevékenységének összehangolására a kritikus infrastruktúrák védelme érdekében az internetes támadásokkal szemben. A PDD 63 a kormányon belül számos kiberbiztonsággal kapcsolatos szervezetet hozott létre, köztük a Nemzeti Biztonsági, Infrastruktúravédelmi és Terrorizmusellenes Koordinátort, a Kritikus Infrastruktúra Hivatalával, ami támogatja a koordinátort és a Nemzeti Infrastruktúravédelmi Központot.[20]

A szövetségi információbiztonsági gazdálkodási törvény (Federal Information Security Management Act – a továbbiakban: FISMA)[21], a 2002. évi e-kormányzati törvény részeként a Nemzeti Szabványügyi és Technológiai Intézet által kidolgozott kockázatkezelési keretet alkalmazta (National Institute of Standards and Technology – a továbbiakban: NIST) a kiberbiztonsági folyamatok szabványosítása érdekében az amerikai kormányzati szervezetek között. Ezen esemény eredményeként, a szövetségi információs vezérigazgató-helyettes (Federal Chief Information Officer – a továbbiakban: FCIO) felelős a kormány technológiai alkalmazásának felügyeletéért, mind a kiadások, mind a stratégia szempontjából. Ez tisztázta és megerősítette a NIST felelősségét a szövetségi számítógépes rendszerek (a védelmi és hírszerzési rendszerek kivételével) biztonsági szabványainak kidolgozásáért, létrehozott egy központi szövetségi incidens központot és az OMB-t tette felelőssé a szövetségi kiberbiztonsági szabványok közzétételéért.

2002-ben a belbiztonsági törvény értelmében létrehozták a belbiztonsági osztályt (Department of Homeland Security – a továbbiakban: DHS), többek között azért, hogy összehangolja a kritikus infrastruktúra védelmének nemzeti infrastruktúráját az informatikai és kommunikációs ágazatokban.

18 Executive Order 13025 - Amendment to Executive Order 13010, the President's Commission on Critical Infrastructure Protection November 13, 1996, https://www.gpo.gov/fdsys/pkg/WCPD-1996-11-18/pdf/WCPD-1996-11-18-Pg2390-3.pdf (letöltve és megtekintve:2020. 03. 30.)

19 Presidential DecisionDirective/NSC-63 The White House Washington May 22, 1998 https://fas.org/irp/offdocs/pdd/pdd-63.pdf (letöltve és megtekintve: 2020. 03. 30.)

20 Kevin P. Newmeyer, Who Should Lead U.S. Cybersecurity Efforts? 2012,. 118-119 http://cco.ndu.edu/Portals/96/Documents/prism/prism_3-2/prism115-126_newmeyer.pdf (letöltve és megtekintve: 2020. 03. 30.)

21 The United States Congress, 'H.R.2458 –E-Government Act of 2002. 107th Congress (2001-2002)', 2002 https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf (letöltve és megtekintve: 2020.03.30)

A szárazföldi biztonságról szóló, 2003. évi 7. elnöki irányelv[22] meghatározta a kritikus infrastruktúrák azonosítását és rangsorolását a fizikai világban és a kibertérben, a terroristatámadásokkal szembeni védelem érdekében. Az irányelv naprakésszé tette a különféle ügynökségek szerepét és felelősségét a 2002. évi belbiztonsági törvényben és más okmányokban. Megerősítette a DHS felelősségét a teljes kritikus infrastruktúra védelmére irányuló erőfeszítések irányításában, és kinevezte az osztályt az informatikai és kommunikációs iparág vezető ügynökségének, amely megosztja a fenyegetéssel kapcsolatos információkat, értékeli a sebezhetőségeket, és elkészíti a megfelelő biztonsági és vészhelyzeti intézkedéseket, terveket. Ezen kívül arra utasította a DHS-t, hogy hozzon létre egy nemzeti infrastruktúravédelmei tervet (National Infrastructure Protection Plan – továbbiakban: NIPP), ezért 2006-ban közzétették a Nemzeti Infrastruktúra Védelmi Tervet.[23]

A Bush-kormányzat alatt a kiberbiztonság bonyolult volt, korlátozott vezetéssel és felelősségmegosztással a Fehér Ház és a védelmi minisztérium (Department of Defense – következőkben: DoD) között. A belbiztonság átfogó koordinációs szerepet kapott, de a felelősség továbbra is az egyes ügynökségekre hárult. 2006-ban a Legfelsőbb Parancsnokság által kiadott, a kibertérműveletekre vonatkozó nemzeti katonai stratégia az első átfogó okmány[24], amely leírja az amerikai katonaság megközelítését a kibertérműveletekben. A dokumentum felvázolta az amerikai fegyveres erők szerepét az amerikai érdekek védelme szempontjából a kibertérben végrehajtott katonai műveletek végrehajtásában. A DoD stratégia szerint a „katonai, hírszerzési és üzleti műveletek a kibertérből támaszkodnak a nemzeti katonai célok elérésére".

George W. Bush elnök 2008 januárjában aláírta a nemzetbiztonsági elnöki irányelvet és a 23-as belbiztonsági elnöki irányelvet[25] a DHS-re és az OMB-re, hogy minimális működési szabványokat állítson fel a szövetségi kormány polgári hálózatai részére. Mindkét irányelv hangsúlyozta a teljes irányítási megközelítést, amelyet az Átfogó Nemzeti Kiberbiztonsági Kezdeményezés (Comprehensive National Cybersecurity Initiative – a továbbiakban: CNCI)[26] követ iránymutatásokkal. A CNCI kijelenti, hogy védelmet nyújt a fenyegetések legközvetlenebb és legteljesebb spektruma ellen, és megerősíti a jövőbeli biztonsági környezetet egy átfogó megközelítés biztosításával, amely magában foglalja a bűnüldözést, hírszerzést/kémelhárítást és katonai képességeket. 2009-ben Obama elnök a CNCI megfelelő integrációjának, finanszírozásának és a kongresszussal, illetve a magánszektorral való megfelelő integrációjának, finanszírozásának, valamint összehangolásának biztosítása érdekében egy 60 napos kiberűr-politikai áttekintés elnevezésű cyber-kormányzati felülvizsgálatot indított.[27] A felülvizsgálat egy erősebb Fehér Házra, valamint a szövetségi vezetés és az internetes biztonság

22 U.S. Department of Homeland Security, 'Homeland Security Presidential Directive 7: Critical Infra-structure Identification, Prioritization, and Protection', 2003 http://www.dhs.gov/homeland-security-presidential-directive-7 (letöltve és megtekintve: 2020. 03. 30.)

23 National Infrastructure Protection Plan 2006 https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf (letöltve és megtekintve: 2020. 03. 30.)

24 National Military Strategy for Cyberspace Operations Chairman of the Joint Chiefs of Staff, Washington, December 2006 https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf (letöltve és megtekintve: 2020. 03. 30.)

25 National Security Presidential Directive 54/Homeland Security Presidential Directive 23, The White House, Washington, 2008 https://fas.org/irp/offdocs/nspd/nspd-54.pdf (letöltve és megtekintve: 2020.03.30)

26 Comprehensive National Cybersecurity Initiative (CNCI) https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf (letöltve és megtekintve: 2020. 03. 30.)

27 Cyberspace Policy Review https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-028.pdf (letöltve és megtekintve: 2020. 03. 30.)

elszámoltathatóságának erősítésére tett javaslatot. 10 rövid távú intézkedést és 14 középtávú intézkedést határozott meg a CNCI általános célkitűzéseinek támogatására.

A szélesebb körű nemzetbiztonsági és védelmi stratégiák szintén körvonalazzák a kiberbiztonság céljait. A 2010. évi nemzetbiztonsági stratégia[28] volt az első amerikai nemzetbiztonsági stratégia, amely figyelmet fordított a kiberfenyegetésekre. A 2010. évi négyévenkénti honbiztonsági áttekintés kiemelte a „kibertér védelmét és biztonságát", mint az öt fő nemzetbiztonsági küldetés egyikét.[29] A kiberbiztonsági folyamatokhoz közeledő katonai védelmi megfontolások alapján az Amerikai Kiberparancsnokság (U.S. Cyber Command's – a továbbiakban: USCYBERCOM) 2010-ben jött létre, és ugyanabban az évben kezdte meg működését.[30] A nemzetbiztonsági stratégia végrehajtása és a Quadrennial Homeland Security Review[31] által kitűzött célok elérése érdekében a DHS dolgozott ki egy cselekvési tervet, amely 2011-ben a Blueprint for Secure Cyber Future[32] elnevezést kapta. A cselekvési terv a következő két területre terjed ki: a kritikus információs infrastruktúrára és a számítógépes környezetre. 2011 májusában a Fehér Ház kiadta a nemzetközi kibertér stratégiáját[33], amely tükrözi az Egyesült Államok megközelítését a nemzetközi kapcsolatokban és a nemzeti prioritások közlésében. A stratégia általános célja a következő: az Egyesült Államok olyan nemzetközi, nyitott, interoperábilis, biztonságos és megbízható információs és kommunikációs infrastruktúrát fog működtetni, amely támogatja a nemzetközi kereskedelmet, erősíti a nemzetközi biztonságot, előmozdítja a szabad véleménynyilvánítást és az innovációt. E cél elérése érdekében olyan környezetet építünk és tartunk fenn, amelyben a felelősségteljes magatartási normák szabályozzák az államok tevékenységét, fenntartják a partnerségeket és támogatják a jogállamiságot a kibertérben. A kibertér nemzetközi stratégiája miatt az Egyesült Államok Nemzeti Minisztérium Stratégiája (2011) elismerte, hogy a kibertér önmagában hadszíntérré alakult, és hogy az Egyesült Államok növeli a légi, az űrbéli és a kibertérre vonatkozó elrettentést és javítja azon képességét, hogy legyőzze a rendszerek vagy infrastruktúrák elleni támadásokat.

2012-ben az Obama-adminisztráció támogatta azt a jogszabályt, amely felhatalmazást adna a DHS-nek a kritikusinfrastruktúra-hálózatok védelmére, a törvényjavaslatot azonban kétszer nem fogadta el a Kongresszus. Válaszul Obama kiadta *A kritikus infrastruktúra kiberbiztonságának javítása (EO 13636)*[34] című kiadványt. Ez az elnökség számára kötelező érvényű dokumentum kiegészíti az összes korábbit, és jobb információcserét biztosít a szövetségi kormány és a magánszektor között. Ezen túl minimális kritériumokat is meghatároz a kritikus infrastruktúrák biztonságának javítása érdekében. Az EO 13636 szám alatt kiadott, a kritikus

28 National Security Strategy http://nssarchive.us/NSSR/2010.pdf (letöltve és megtekintve: 2020. 03. 30.)

29 Quadrennial Homeland Security Review https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf (letöltve és megtekintve: 2020. 03. 30.)

30 US Department of Defense U.S. Cyber Command Fact Sheet https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf (letöltve és megtekintve: 2020. 03. 30.)

31 The Quadrennial Homeland Security Review https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf (letöltve és megtekintve: 2020. 03. 30.)

32 Blueprint for Secure Cyber Future https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf (letöltve és megtekintve: 2020. 03. 30.)

33 International Strategy for Cyberspace https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (letöltve és megtekintve: 2020. 03. 30.)

34 Improving Critical Infrastructure CyberSecurity (EO 13636) https://www.dhs.gov/sites/default/files/publications/EO-13636-Improving-Critical-Infrastructure-Cybersecurity-508.pdf (letöltve és megtekintve: 2020. 03. 30.)

infrastruktúrák biztonságáról és ellenállóképességéről szóló elnöki irányelv (PPD-21)[35] nem tett jelentős változásokat a politikában, a szerepekben, a felelősségvállalásban és a programokban; ugyanakkor felszólította a meglévő köz- és magánszféra szereplőit a hatékony információcsere alapjául szolgáló adatok és rendszerkövetelmények, valamint a helyzettudatosság fejlesztésének értékelésére.[36] Felhívta a figyelmet a Nemzeti Infrastruktúra Védelmi Terv (NIPP) felülvizsgálatára, és végül a terv 2013-as harmadik felülvizsgálatának átdolgozására. A 2013. évi Nemzeti Kiberbiztonsági és Kritikus Infrastruktúra Védelem (National Cybersecurity and Critical Infrastructure Protection – a továbbiakban: NCCIP)[37] biztosítja a DHS szerepét a kiberbiztonság megelőzésében és reagálásában, és információcsere-partnerséget hoz létre a DHS és a kritikus infrastruktúra tulajdonosai és üzemeltetői között. A Quadrennial Homeland Security Review-et 2014-ben felülvizsgálták. A vizsgálat feltárta a DoD felelősségét az új és kibővített teljes spektrumú kibertér képesség;nek kifejlesztésében, hogy megvédjék országukat és támogassák a katonai missziókat világszerte. A DoD 2014. évi negyedéves védelmi áttekintése a következőképpen határozza meg a DoD legfontosabb szerepét a kibertérben: „Védje meg a DoD hálózatainak integritását, védje a legfontosabb rendszereinket és hálózatainkat, hajtson végre tengerentúli műveleteket, és védje meg a nemzetet a küszöbönálló, destruktív kibertámadások ellen". A kiber-elektromágneses tevékenységek (FM 3-38)[38], amelyeket az Egyesült Államok Hadserege 2014-ben tett közzé, útmutatást nyújt a kiber-elektromágneses tevékenységekhez, valamint taktikát és eljárásokat tervez, integrál és szinkronizál. A doktrína összehasonlítja a hadsereg műveleteit az elektronikus hadviselésel. Ezenkívül a közös kibertérműveletek (Joint Cyberspace Operations) (JP 3–12)[39] a katonai műveletek egyediségével foglalkoznak a kibertérben, és tisztázza a kibertérműveleteket. 2014-ben a szövetségi kormány létrehozott egy önkéntes kiberbiztonsági keretet, amelyet a Kritikus Infrastruktúra Fejlesztési Keretnek[40] hívtak, és amely iránymutatásokat, gyakorlatokat és önkéntes szabványokat tartalmaz a magánszektor számára a kritikus infrastruktúra védelmének biztosítása érdekében.

Katonai szempontból a jelenlegi nemzetbiztonsági stratégia, amelyet 2015 elején fogadtak el, a korábbi 2011-es kiadás frissített verziója, felismeri a pusztító kibertámadások növekvő veszélyét, és bejelenti az Egyesült Államok azon szándékát, hogy erősítse a kritikus infrastruktúrák kiberbiztonságát. A dokumentum elsősorban az Egyesült Államok azon szándékára összpontosít, hogy előmozdítsa a nemzetközi szabványokat a kibertérben. Az új stratégia nagyobb átláthatóságot biztosít a DoD saját támadó és operatív képességei tekintetében.

35 Presidential Policy Directive The Critical Infrastructure Security and Resilience 55 https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf (letöltve és megtekintve: 2020. 03. 30.)

36 Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity Presidential Policy Directive (PPD) 21 Critical Infrastructure Security and Resilience https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf (letöltve és megtekintve: 2020. 03. 30.)

37 National Cybersecurity and Critical Infrastructure Protection (NCCIP) https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (letöltve és megtekintve: 2020. 03. 30.)

38 U.S. Department of Army, 'Cyber Electromagnetic Activities', No. 3-38, Washington, 2014 http://fas.org/irp/doddir/army/fm3-38.pdf (letöltve és megtekintve: 2020. 03. 30.)

39 Joint Cyberspace Operations Cyberspace Operations http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf (letöltve és megtekintve: 2020. 03. 30.)

40 Framework for Improving Critical Infrastructure https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (letöltve és megtekintve: 2020. 03. 30.)

Összegzés

Az Egyesült Államokban a kiberbiztonsági irányelv manapság részleges intézkedésekből áll, hasonlóképpen a jogalkotásokhoz, melyek kevésbé átfogóak és inkább helyi, lokális jellegűek. Több mint 50 alapszabály foglalkozik a kiberbiztonság különféle szempontjaival. Mivel nincs átfogó keret, amely ezeket a dokumentumokat szintetizálja, vagy átfogóan leírja a jelenlegi stratégiát, a világos megértés, valamint az általános stratégiai célok és prioritások meghatározása bonyolult feladat. A legtöbb meglévő dokumentum a szűkebb kiberbiztonsági területek nemzeti prioritásaira vonatkozik, amelyek ugyanakkor elősegítik a prioritásoktól és a struktúrától való eltérést, és nem határozzák meg, hogy kapcsolódnak-e más politikai dokumentumokhoz, vagy felülírják-e azokat. Ezeknek a dokumentumoknak a többsége nem írja le, hogyan illeszkednek az átfogó nemzeti kiberbiztonsági stratégiához.[41]

Az Egyesült Államok kormánya már a 90-es évektől gyökerezteti a kiberstratégiára vonatkozó irányelvalkotást, és egyértelműen felismerte az új biztonsági kihívásokat, és reagálni akart a felmerült eseményekre és helyzetekre. Számos irányelve, direktívája, elnöki rendelete a startégiai szintű szabályozásra és útmutatásra utal, mely rendkívül fontos prioritással és naprakészséggel kerül kezelésre. Ezenkívül ez rámutat arra, hogy fejleszti képességeit és kompetenciáit, amelyeket eddig elért, és támogatja az oktatási, tudományos és kutatási irányokat. Ezen túlmenően technikai támogatást kíván nyújtani a tagállamoknak és saját szervezeteiknek a megfelelő készségek biztosításával. Ezek a technikai támogatások több katonai jellegű gyakorlatot is tartalmaznak, melyből van kiberbiztonsági gyakorlat is, mint példaául a Cyber Shield. Ezt a gyakorlatot a következő fejezetben részletesen kifejtem.

Nemzetközi katonai kibergyakorlatok

Több katonai gyakorlatnak is részét képezi már az informatikai biztonság, valamint a NATO által elfogadott kibertér mint műveleti hadszíntér. Ez figyelemfelhívás a kibertérből érkező fenyegetésekre, veszélyekre estleges támadásokra, valamint felkészülés is a C4ISR (Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance – Katonai felhasználású informatikai célrendszerek a vezetés, irányítás, kommunikáció, hírszerzés és felderítés támogatására) rendszerek megbízhatóságának tesztelésére.

41 National Cyber Security Organization, United States 2016 https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf (letöltve és megtekintve: 2020. 03. 30.)

A gyakorlatokat kimondottan az informatikai rendszereket üzemeltető szakállomány részére szervezik meg és bonyolítják le, amikbe sok esetben bevonják a civil szakértőket. Ilyen gyakorlatok többek között:

- Cyber defense exercise (CDX)[42]
- Cross swords[43]
- Cyber coalition[4445]
- Cyber perseu[46]
- Cyber czech[47]
- Cyber tesla[48]

A fentiekben felsoroltakon kívül két gyakorlatot szeretnék kiemleni, melyek véleményem és tapasztalatom szerint jelentős múlttal, megfelelő szervezéssel és szakmai, valamint technológiai és technikai jellemzőkkel rendelkeznek. A két gyakorlat kitűnő példája a kibergyakorlatok többrétegűségének és komplexitásának. Ezen felül zászlóshajói a Kiberbiztonsági Stratégiákban meghatározott oktatási célkitűzés megvalósításának, mely gyakorlatorienált és készségszintű ismereteket segít elsajátítani. Ez a két gyakorlat a Locked Shields és a Cyber Shiled.

Locked Shields

A NATO-tagállamok katonai híradó-informatikai rendszereinek szakállománya számára elérhető a Locked Shields[49] gyakorlatsorozat, melyet a NATO Kibervédelmi Kiválósági Központja évente megrendez. A 2010-ben megrendezett első gyakorlat folytatásaként évente növekszik a résztvevők száma, és bővül a feladatok összetettsége. A Magyar Honvédség 2014 óta szerepel a gyakorlaton. A gyakorlat állománya folyamatos leterheltség alatt van, hiszen a résztvevőknek egy ismeretlen, rosszul dokumentált, nagy kiterjedésű hálózatot kell felügyelniük, aminek felkészüléséhez és végrehajtásához csekély időintervallumot kapnak. Ezenfelül megfertőztek

42 Cyber Research Center – CDX Network https://www.usma.edu/centers-and-research/cyber-research-center/data-sets (letöltve és megtekintve: 2020. 03. 30.)

43 Cymmetria: The Crossed Swords wargame: Catching NATO red teams with cyber deception – 2017. május 25. https://cymmetria.com/blog/nato-crossed-swords-exercise/ (letöltve és megtekintve: 2020. 03. 30.)

44 NATO - NATO's flagship cyber exercise begins in Estonia (2017) https://www.nato.int/cps/ic/natohq/news_149233.htm (letöltve és megtekintve: 2020. 03. 30.)

45 Szűcs László, Sikeres volt a kibervédelmi gyakorlat (2011) https://honvedelem.hu/cikk/29471/sikeres-volt-a-kibervedelmi-gyakorlat (letöltve és megtekintve: 2020. 03. 30.)

46 INDRA - The Portuguese Armed Forces complete Cyber Perseu, the National Cyberdefense exercise, using Indra's Minsait Cyber Range platform https://www.indracompany.com/en/noticia/portuguese-armed-forces-complete-cyber-perseu-national-cyberdefense-exercise-using-indras (letöltve és megtekintve: 2020. 03. 30.)

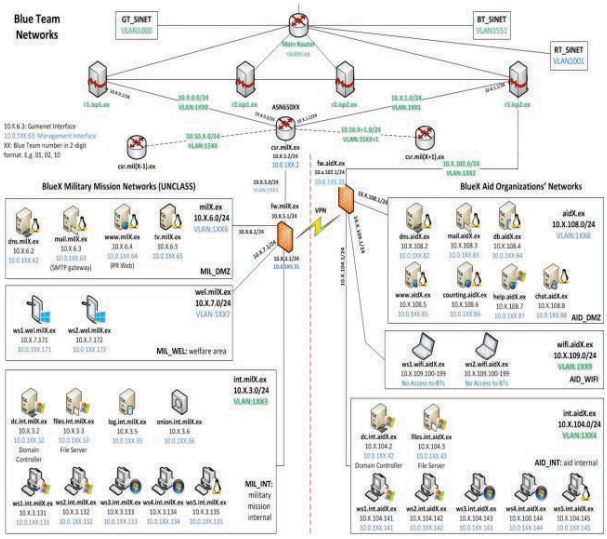
47 Jan Vykopal–Ondřej Mokoš, Czech cyber defence exercise https://www.terena.org/activities/tf-csirt/meeting47/J.Vykopal-O.Mokos-Czech-lessons.pdf (letöltve és megtekintve: 2020. 03. 30.)

48 Multinational Exercise „Cyber Tesla 2019. november 13. http://www.vs.rs/en/news/BA5E2A5D062D11EAAC980050568F5424/multinational-exercise-cyber-tesla-2019 (letöltve és megtekintve: 2020. 03. 30.)

49 NATO Cooperative Cyber Defence Centre of Excellence: Cyber Defence Exercise Locked Shields 2012. After Action Report https://ccdcoe.org/library/publications/cyber-defence-exercise-locked-shields-2012-after-action-report/ (letöltve és megtekintve: 2020. 03. 30.); NATO Cooperative Cyber Defence Centre of Excellence: Cyber Defence Exercise Locked Shields 2013. After Action Report https://ccdcoe.org/library/publications/cyber-defence-exercise-locked-shields-2013-after-action-report/ (letöltve és megtekintve: 2020. 03. 30.); NATO Cooperative Cyber Defence Centre of Excellence: Locked Shields 2014 After Action Report: Executive Summary https://ccdcoe.org/library/publications/locked-shields-2014-after-action-report-executive-summary/ (letöltve és megtekintve: 2020. 03. 30.)

egyes rendszerelemeket, illetve szándékosan kikapcsoltak bizonyos védelmi szerepeket. Az adott hálózati környezet inhomogén, jellemzően korszerűtlen vagy patchelés nélküli operációs rendszereket használnak, és több esetben régi, sérülékeny vagy nem megfelelő konfigurációval ellátott szolgáltatásokat alkalmaznak. A támadások kivédésével párhuzamosan az állomány tagjainak a csapaton belüli hatékony kommunikációt szükséges alkalmazniuk, ami magába foglalja a támadóról és a támadási módszerről szerzett információk megosztását, a feladatok priorizálását és a párhuzamosan felmerülő események kezelését. Ezenfelül különböző próbatételek fordulhatnak elő, amelyek többek között üzemeltetéshez, felhasználói segítségnyújtáshoz, új szerverfunkció beüzemeléséhez és konfiguráció változtatásához kapcsolódnak, valamint jogi és médiamegjelenéssel, illetve stratégiai döntéshez köthető feladatok adódnak. A megfelelő megoldásokat leszámítva a határidőket, a bemutatás módját, a szakmai hitelességet is figyelembe veszik. A gyakorlaton jelentések megírása is követelmény, melyeknek célja a lényeg felismerése és a szaknyelv használata.[50]

A gyakorlat oktatás és biztonságpolitika szempontjából rámutat arra, hogy a technikai akadályokkal megküzdő szakemberek csapatban dolgoznak, és az információt mind horizontálisan, mind vertikálisan megosztják. Ami hozzájárul mind a technikai, mind a döntéshozatali biztonságtudatosság és tudás fejlesztéséhez, fejlődéséhez.



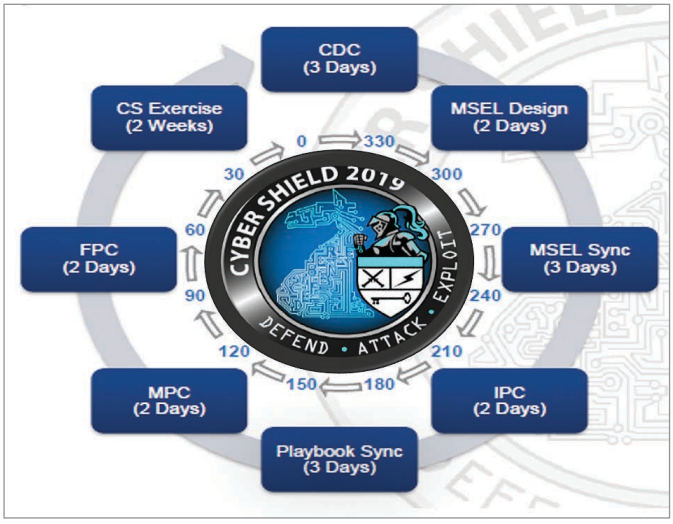
1. ábra: NATO Locked Shield 2013 gyakorlat virtuális infrastruktúrája
(Forrás: Cyber Defence Exercise Locked Shields 2013. After Action Report https://ccdcoe.org/library/publications/cyber-defence-exercise-locked-shields-2013-after-action-report/)

50 Szabó András, Technikai kiberbiztonsági gyakorlatok – nemzetközi kitekintés, Hadmérnök ISSN 1788-1929, XIII. Évfolyam 1. szám, 2018. március http://hadmernok.hu/181_23_szabo.pdf (letöltve és megtekintve: 2020. 03. 30.)

Cyber Shields

A Cyber Shield egy védekező kibertérműveleti képzési program, amely egyesíti az amerikai hadsereg, a nemzeti gárda, a légi nemzetőrség, a parti őrség, az ipari partnerek és a civilek képességeit, hogy gyakorolni és tesztelni tudják képességeiket a számítógépes eseményekkel kapcsolatban. A cél az, hogy az államok első védelmi vonalát gyorsan és hatékonyan kiképezzék a nemzetek kiszolgáltatott kritikus infrastruktúrája és az érzékeny közszolgáltatások elleni kibertámadások megakadályozására.[51]

A Cyber Shield néven ismert gyakorlat 2012-ben indult, ami egyszerű vörös-kék csapatgyakorlatként kezdődött, napjainkban viszont 800 fős eseménnyé nőtte ki magát, amely tükrözi a Gárda nagyobb szerepét az Amerikai Egyesült Államok kibervédelmében. 2019-ben 40 állam nemzetőrségi egységei vettek részt a gyakorlaton, valamint a magánszektor és a szövetségi ügynökségek emberei, például az FBI és a Nemzetbiztonsági Ügynökség. A résztvevők többek között vizsgálják, hogy képesek-e felismerni a hálózaton gyanús tevékenységeket és lezárni az illetéktelen hozzáférést a rendszerhez. *„Ez számunkra kollektív kiképző esemény, tehát javítja harci képességeinket. És ez nagyon fontos számunkra”* – mondta a gyakorlatról Jeffrey Burkett tábornok, a Nemzeti Gárda Iroda belső műveleteinek főnöke.[52] A gyakorlat első hete olyan képzési órákból állt, amelyek során a résztvevők újrahitelesített vagy továbbképző tanfolyamokat kaptak a meglévő képesítésük megőrzése céljából. A második hét egy tényleges képzési gyakorlatból állt, amelynek során a csapatok technikai készségeikkel védték meg hálózataikat a „digitális háború” eseménye nélkül.



2. ábra: Cyber Shile 2019 gyakorlat Életciklus eseményei *(Forrás: Cyber Shield 2019 unclassified COL Teri D. Williams)*

51 Defense visual information distribution sevice: Cyber shield 19 https://www.dvidshub.net/feature/cybershield19 (letöltve és megtekintve: 2020. 03. 30.)

52 Sean Lyngaas, Inside the National Guard's annual 'Cyber Shield' drill – 2019. április 16. https://www.fedscoop.com/inside-national-guards-annual-cyber-shield-drill/ (letöltve és megtekintve: 2020. 03. 30.)

Az oktatási vagy tanulási héten használt képzési forgatókönyvek célja a valós élet utánzása egy csapatrendszer segítségével. A Red Team az ellenerő (Opposite Force – a továbbiakban: OPFOR), akik virtuális infrastruktúrán tevékenykednek a védekező Kék Csapat ellen. A csapatrendszer lehetővé teszi a résztvevőknek, hogy valós időben reagáljanak a kibertámadásokra, és védekező manővereket hajtsanak végre. Valódi műveleteket hajtanak végre, hogy behatoljanak a védekező csapatok hálózatába a folyamatos jelenlét fenntartása, az adatok ellopása és a hálózat megszakítása érdekében. A cél nem a védelmi csapatok hálózatának a lerombolása, hanem a különféle számítógépes kockázatok tudatosítása. Miután ezek a forgatókönyvek befejeződtek, egy együttműködési mélyreható elemzést osztanak meg arról, hogy mi történt mind az OPFOR, mind a védekező csapatok szemszögéből. Noha a valós világ nem biztosítja a lehetőséget, hogy teljeskörű elemzést készítsenek arról, hogy mit végeznek el az egyes felek, a gyors áttekintés minden csapat számára felbecsülhetetlen információt szolgáltat, amelyből megtanulható a fenyegetések hatékonyabb felfedezése.[53]

A 8. számú ábrán látható életciklusmodell eseményei az alábbi tevékenységeket és döntéseket foglalják magukban:

- Koncepciótervezési Konferencia (Concept Design Conference – CDC): meghatározza a gyakorlat céljait, hozzárendeli a kezdeti feladatokat és csökkenti a korábbi hiányosságokat.
- MSEL-tervezés (Develop the Master Scenario Events List): elkészíti a fő forgatókönyv eseménylistáját (MSEL), és azonosítja a forgatókönyv kidolgozásához szükséges injekciókat.
- MSEL Sync (MSEL2): továbbfejleszti és finomítja az MSEL-gyakorlatot, a szcenárióbefecskendezéseket és a fenyegető szereplők tevékenységeit.
- Kezdeti tervezési konferencia (Initial Planning Conference – IPC): meghatározza a személyzettel, felszereléssel és képzéssel kapcsolatos követelményeket, és kidolgozza a működési koncepciót.
- Playbook Sync (MSEL3): elvégzi az edzés ütemtervét, az MSEL-t és a playbookot.
- Fő tervezési konferencia (Main Planning Conference – MPC): konszolidálja a kezdeti támogatási igényeket, véglegesíti a terepi környezetet, és finomítja a gyakorlat ütemezését.
- Végleges tervezési konferencia (Final Planning Conference – FPC): elvégzi a támogatási követelmények, a terepi környezet és a gyakorlati események kidolgozását.
- Cyber Shield Exercise (CS): megad egy kollektív gyakorlati rendezvényt, és megteremti az RC Cyber erők értékelésének feltételeit.

A gyakorlat foglalkozik többek között a behatolás észlelésével, az adatbiztonság törvényével és a fenyegetések elemzésével. A gyakorlat az oktatás és biztonságpolitika aspektusából rámutat arra, hogy a nemzetek technikai kibergyakorlati kihívásai milyen méreteket ölthetnek, és hogy az ezzel kapcsolatos munka folyamatos. A 2019-es gyakorlatra, mint szemlélő, meghívást kapott többek között Magyarország, Ukrajna és Szerbia. Ez jelentős előrelépés a tapasztalat- és információmegosztás területén.

53 Master Sgt. Brad Staggs, Indiana National Guard participates in Cyber Shield, 2016. április 29. https://www.army.mil/article/167051/indiana_national_guard_participates_in_cyber_shield_2016 (letöltve és megtekintve: 2020. 03. 30.)

Befejezés

A kiberteret műveleti térnek definiálták a 2016. évi varsói NATO-csúcson, amelyen a tagállamok vállalták a kibervédelmi képességeik fejlesztését, valamint megállapodtak az információmegosztás javításáról, a közös oktatás, kiképzés, továbbá gyakorlatok szervezéséről is. Megvizsgálva a NATO és az Amerikai Egyesült Államokbeli irányvonalakat arra a következtetésre jutottam, hogy a nemzetközi példák nem ültethetőek át teljes mértékben a magyarországi viszonyokra. A közös gyakorlatok mellett hazánknak önállóan kell meghatározni és kifejleszteni egy katonai kibergyakorlatot, mely alapot biztosít az informatikai hálózat tesztelésére, valamint a szakállomány megfelelő képzéséhez és a tudásanyag készségszinten való gyakorlati elsajátításához.

Az ilyen jellegű gyakorlatok megerősítik a különböző területeken dolgozó szakemberek kapcsolatait és a kiberbiztonság technikai vetületei mellett a biztonságpolitikai, nemzetbiztonsági, katonai hatásaira is felhívják a figyelmet. Az informatikai rendszerekkel kapcsolatban állókat segíthetik a biztonságtudatosság elsajátításában. Ezenfelül a gyakorlatok követhető keretet adnak, mely egyik módja lehet a pályamunkában részletezett stratégiák célkitűzéseinek elérésére. Így bizonyításként szolgálva a Nemzeti Stratégiák célkitűzéseinek katonai szempontból való eredményes végrehajtásához és teljesítéséhez.

Szakmai meggyőződésem, hogy a Magyar Honvédség informatikai és információvédelmi szakemberei a lehető legnagyobb szakértelemmel látják el üzemeltetési feladatukat. Azonban a Nemzeti Biztonsági, Nemzeti Katonai és Nemzeti Kiberbiztonsági Startégiában meghatározottakkal összhangban egy gyakorlat megszervezése, kifejlesztése jelentősen hozzájárul ahhoz, hogy előnyös pozíciót sikerüljön elérni és megtartani a nemzetek közti biztonságpolitika színterén, amihez üzemeltetési szerepkörök ellátása nem feltétlenül elégséges.

A technikai feladatvégrehajtás meghatározó és kimagalsó tudást, előkészületet, valamint felkészülést kíván, de a technikai feladatokat végrehajtó szakállomány oktatása gyakorlat hiányában nem lehet alapos és maximális. Ezek a kibergyakorlatok a technológia és technikai jártasság kiterjesztésével párhuzamosan a kommunikációs készséget, valamint a csapatmunkával, és a feladatok menedzselésével kapcsolatos képességeket is erősíti.

Azt is fontos látni, hogy az új hadviselési dimenziónak vannak kapcsolatai a fizikai (szárazföldi-, vízi-, légi- és űrtelepítésű) infrastruktúrákkal, így ezek kölcsönös egymásra hatásával is számolni kell. Ezek a dependenciák növelik a fenyegetések számát. Szükség van a gyakorlott állományra, akik a kibertérben felkészültek a kihívásokra, melyek összhangban állnak a biztonságpolitika digitalizációjának folyamatával.

Javaslom, hogy lépést tartva más államok biztonságpolitikában és kiberműveleti gyakorlatokban alkalmazott tevékenységeivel, Magyarországon is szervezzenek és hajtsanak végre technikai kiberbiztonsági gyakorlatokat, mind biztonságpolitikai és közigazgatási szinten, mind katonai vonatkozásban is. Így a hazai jogi, és technológiai környezetben készülne fel a szakállomány, és készségeik a jelenlegi nemzetközi kihívásokhoz igazodnának.

Irodalomjegyzék

1. Kovács László, A kibertér védelme, Budapest: Dialóg Campus Kiadó, 2018. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf (letöltve és megtekintve: 2020. 03. 30.)
2. Draveczki-Ury Ádám, Átadták a Magyar Honvédség Kiber Képzési Központját 2019. 06. 13. 12:00 https://honvedelem.hu/galeriak/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat/ (letöltve és megtekintve: 2020. 03. 30.)
3. 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
4. 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról
5. 1139/2013. (III. 21.) Korm. határozat
6. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
7. Jobbágy Szabolcs, Az információs társadalom, az informatika és a távközlés konvergenciája. Múlt, jelen, jövő. Hadmérnök IV. évfolyam 1. szám, 2009. március, 185–188. http://www.hadmernok.hu/2009_1_ jobbagy.pdf (letöltve és megtekintve: 2020. 03. 30.)
8. ITU-T X.1205 telecommunication standardization sector of ITU (04/2008) series x: data networks, open system communications and security telecommunication security overview of cybersecurity. 8. https://www.itu.int/rec/T-REC-X.1205-200804-I (letöltve és megtekintve: 2020. 03. 30.)
9. Az Észak-atlanti Szerződés, Washington DC, 1949. április 4., 1. 5. Cikk https://www.nato.int/cps/ic/natohq/official_texts_17120.htm?Selectedlocale=hu (letöltve és megtekintve: 2020. 03. 30.)
10. Kovács László–Szentgáli Gergely, National Cyber Security Organization: Hungary. 11. Tallinn, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_HUNGARY_2015-10-12.pdf (letöltve és megtekintve: 2020. 03. 30.)
11. Bucharest Summit Declaration – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008. https://www.nato.int/cps/en/natolive/official_texts_8443.htm (letöltve és megtekintve: 2020. 03. 30.)
12. Szentgáli Gergely, A NATO kibervédelmi politikájának fejlődése. Bolyai Szemle XXI. évf. 2. szám, 2012, 80–85. http://archiv.uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf (letöltve és megtekintve: 2020. 03. 30.)
13. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon 19–20. November 2010. https://www.nato.int/cps/ua/natohq/official_texts_68580.htm (letöltve és megtekintve: 2020. 03. 30.)
14. Joint Publication 3–12 (R) Cyberspace Operations. 5. Feb 2013, 69. http://www.dtic.mil/doctrine/new_ pubs/jp3_12R.pdf (letöltve és megtekintve: 2020. 03. 30.)

15. NATO Summit Guide Warsaw, 8–9. July 2016, 124–128. https://www.nato.int/nato_static_f l2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf (letöltve és megtekintve: 2020. 03. 30.)
16. The White House, 'The National Strategy to Secure Cyberspace', 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (letöltve és megtekintve: 2020. 03. 30.)
17. Executive Order 13025 - Amendment to Executive Order 13010, the President's Commission on Critical Infrastructure Protection November 13, 1996, https://www.gpo.gov/fdsys/pkg/WCPD-1996-11-18/pdf/WCPD-1996-11-18-Pg2390-3.pdf (letöltve és megtekintve: 2020. 03. 30.)
18. Presidential Decision Directive/NSC-63 The White House Washington May 22, 1998 https://fas.org/irp/offdocs/pdd/pdd-63.pdf (letöltve és megtekintve: 2020. 03. 30.)
19. Kevin P. Newmeyer, Who Should Lead U.S. Cybersecurity Efforts?, 2012, 118-119 http://cco.ndu.edu/Portals/96/Documents/prism/prism_3-2/prism115-126_newmeyer.pdf (letöltve és megtekintve: 2020. 03. 30.)
20. The United States Congress, 'H.R.2458 –E-Government Act of 2002. 107th Congress (2001-2002)', 2002 https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf (letöltve és megtekintve: 2020. 03. 30.)
21. Public Law 107–296—Nov. 25, 2002 107th Congress an Act To establish the Department of Homeland Security, and for other purposes. https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf (letöltve és megtekintve: 2020. 03. 30.)
22. U.S. Department of Homeland Security, 'Homeland Security Presidential Directive 7: Critical Infra-structure Identification, Prioritization, and Protection', 2003 http://www.dhs.gov/homeland-security-presidential-directive-7 (letöltve és megtekintve: 2020. 03. 30.)
23. National Infrastructure Protection Plan 2006 https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf (letöltve és megtekintve: 2020. 03. 30.)
24. National Military Strategy for Cyberspace Operations Chairman of the Joint Chiefs of Staff, Washington, December 2006 https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf (letöltve és megtekintve: 2020. 03. 30.)
25. National Security Presidential Directive 54/ Homeland Security Presidential Directive 23, The White House Washington, 2008 https://fas.org/irp/offdocs/nspd/nspd-54.pdf (letöltve és megtekintve: 2020. 03. 30.)
26. Comprehensive National Cybersecurity Initiative (CNCI) https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf (letöltve és megtekintve: 2020. 03. 30.)
27. Cyberspace Policy Review https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-028.pdf (letöltve és megtekintve: 2020. 03. 30.)
28. National Security Strategy http://nssarchive.us/NSSR/2010.pdf (letöltve és megtekintve: 2020. 03. 30.)
29. Quadrennial Homeland Security Review https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf (letöltve és megtekintve: 2020. 03. 30.)

30. US Department of Defense U.S. Cyber Command Fact Sheet https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf (letöltve és megtekintve: 2020. 03. 30.)
31. Blueprint for Secure Cyber Future https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf (letöltve és megtekintve: 2020. 03. 30.)
32. International Strategy for Cyberspace https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (letöltve és megtekintve: 2020. 03. 30.)
33. Improving Critical Infrastructure Cybersecurity (EO 13636) https://www.dhs.gov/sites/default/files/publications/EO-13636-Improving-Critical-Infrastructure-Cybersecurity-508.pdf (letöltve és megtekintve: 2020. 03. 30.)
34. Presidential Policy Directive The Critical Infrastructure Security and Resilience 55 https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf (letöltve és megtekintve: 2020. 03. 30.)
35. Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity Presidential Policy Directive (PPD) 21 Critical Infrastructure Security and Resilience https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf (letöltve és megtekintve: 2020. 03. 30.)
36. National Cybersecurity and Critical Infrastructure Protection (NCCIP) https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (letöltve és megtekintve: 2020. 03. 30.)
37. The Quadrennial Homeland Security Review https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf (letöltve és megtekintve: 2020. 03. 30.)
38. U.S. Department of Army, 'Cyber Electromagnetic Activities', No. 3–38, Washington, 2014 http://fas.org/irp/doddir/army/fm3-38.pdf (letöltve és megtekintve: 2020. 03. 30.)
39. Joint Cyberspace Operations Cyberspace Operations http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf (letöltve és megtekintve: 2020. 03. 30.)
40. Framework for Improving Critical Infrastructure https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (letöltve és megtekintve: 2020. 03. 30.)
41. A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats 2018 https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf (letöltve és megtekintve: 2020. 03. 30.)
42. National Cyber Security Organization: United States 2016 https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf (letöltve és megtekintve: 2020. 03. 30.)
43. Cyber Research Center – CDX Network https://www.usma.edu/centers-and-research/cyber-research-center/data-sets (letöltve és megtekintve: 2020. 03. 30.)
44. Cymmetria: The Crossed Swords wargame: Catching NATO red teams with cyber deception – 2017. május 25. https://cymmetria.com/blog/nato-crossed-swords-exercise/ (letöltve és megtekintve: 2020. 03. 30.)

45. NATO – NATO's flagship cyber exercise begins in Estonia (2017) https://www.nato.int/cps/ic/natohq/news_149233.htm (letöltve és megtekintve: 2020. 03. 30.)
46. Szűcs László, Sikeres volt a kibervédelmi gyakorlat (2011) https://honvedelem.hu/cikk/29471/sikeres-volt-a-kibervedelmi-gyakorlat (letöltve és megtekintve: 2020. 03. 30.)
47. INDRA - The Portuguese Armed Forces complete Cyber Perseu, the National Cyberdefense exercise, using Indra's Minsait Cyber Range platform https ://www.indracompany.com/en/noticia/portuguese-armed-forces-complete-cyber-perseu-national-cyberdefense-exercise-using-indras (letöltve és megtekintve: 2020. 03. 30.)
48. Jan Vykopal– Ondřej Mokoš, Czech cyber defence exercise https://www.terena.org/activities/tf-csirt/meeting47/J.Vykopal-O.Mokos-Czech-lessons.pdf (letöltve és megtekintve: 2020. 03. 30.)
49. Multinational Exercise Cyber Tesla 2019. november 13. http://www.vs.rs/en/news/BA5E2A5D062D11EAAC980050568F5424/multinational-exercise-cyber-tesla-2019 (letöltve és megtekintve: 2020. 03. 30.)
50. NATO Cooperative Cyber Defence Centre of Excellence: Cyber Defence Exercise Locked Shields 2012. After Action Report https://ccdcoe.org/library/publications/cyber-defence-exercise-locked-shields-2012-after-action-report/ (letöltve és megtekintve: 2020. 03. 30.)
51. NATO Cooperative Cyber Defence Centre of Excellence: Cyber Defence Exercise Locked Shields 2013. After Action Report https://ccdcoe.org/library/publications/cyber-defence-exercise-locked-shields-2013-after-action-report/ (letöltve és megtekintve: 2020. 03. 30.)
52. NATO Cooperative Cyber Defence Centre of Excellence: Locked Shields 2014 After Action Report: Executive Summary https://ccdcoe.org/library/publications/locked-shields-2014-after-action-report-executive-summary/ (letöltve és megtekintve: 2020. 03. 30.)
53. Szabó András, Technikai kiberbiztonsági gyakorlatok – nemzetközi kitekintés, Hadmérnök ISSN 1788-1929, XIII. Évfolyam 1. szám – 2018. március http://hadmernok.hu/181_23_szabo.pdf (letöltve és megtekintve: 2020. 03. 30.)
54. Defense visual information distribution sevice: Cyber shield 19 https://www.dvidshub.net/feature/cybershield19 (letöltve és megtekintve: 2020. 03. 30.)
55. Sean Lyngaas, Inside the National Guard's annual 'Cyber Shield' drill – 2019. április 16. https://www.fedscoop.com/inside-national-guards-annual-cyber-shield-drill/ (letöltve és megtekintve: 2020. 03. 30.)
56. Master Sgt. Brad Staggs, Indiana National Guard participates in Cyber Shield – 2016. április 29. https://www.army.mil/article/167051/indiana_national_guard_participates_in_cyber_shield_2016 (letöltve és megtekintve: 2020. 03. 30.)

HUNEXPERT

digitális jólét program

MATE
MAGYAR AGRÁR- ÉS ÉLETTUDOMÁNYI EGYETEM

SZENT ISTVÁN BIZTONSÁGKUTATÓ KÖZPONT

MAGYAR ATLANTI TANÁCS

ORSZÁGOS TUDOMÁNYOS DIÁKKÖRI TANÁCS

DOSZ doktoranduszok országos szövetsége