Szabó Hedvig[1] – Dobák Imre[2]

Az információs társadalom nemzetbiztonsága[3]

A tanulmány a társadalom – infokommunikációs környezet – nemzetbiztonság összefüggéseibe kíván betekintést engedni, felölelve többek között az innováció kiemelt szerepét, valamint a technológiai környezet egyre jobban érezhető hatásait. Kitér az államok oldaláról megjelenő válaszlépésekre, valamint az egyes országok biztonságpolitikai gondolkodásában is hangsúlyossá váló, a különböző platformokon keresztül beszűrődő veszélyekkel szembeni biztonsági szempontokra. Ismertetésre kerül az innováció hazai nemzetbiztonsági szférában való megjelenése és az egyre fontosabb innovációs struktúrák szerepe. Kulcskérdésként vizsgálatra érdemes az innováció mai jelentősége, a globális infokommunikációs szereplők működése és a mögöttük álló technológiai fejlődés, amely hatással lehet egy adott ország (nemzet)biztonságára.

Kulcsszavak: *nemzetbiztonság, innováció, infokommunikáció, technológia*

National Security of the Information Society

The aim of the study is to provide an insight into the increasingly complex context of the social – info-communication environment – national security, including the key role of innovation and the increasing effects of the technological environment. It addresses the responses from the states and the security aspects of the threats posed by the various platforms, which are also highlighted in the security thinking of countries. The emergence of innovation in the Hungarian security sphere and the role of increasingly important innovation structures will be described. As a key issue, it is worth examining the importance of innovation nowadays, the importance of global info-communication actors and the technological development behind them, which may have an impact on the security of a given country.

Keywords: *national security, innovation, infocommunication, technology*

Bevezetés

Minden állam kiemelten kezeli a biztonságához köthető területeket, amelyek felölelik a nemzetbiztonsági gondolkodás körét is. A nemzeti szintű biztonságért felelős intézményrendszerek számos elemből tevődhetnek össze,[4] alapvető szereplői közé tartoznak

[1] Szabó Hedvig a Nemzetbiztonsági Szakszolgálat főigazgatója. E-mail: nbsz@nbsz.gov.hu

[2] Dobák Imre a Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézetének egyetemi docense. E-mail: dobak.imre@uni-nke.hu

[3] A munka a TKP2020-NKA-09 számú projekt keretében, a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a „Tématerületi Kiválósági Program 2020” pályázati program finanszírozásában valósult meg.

[4] Lásd Dorith Kool – Tim Sweijs: A Security Sector Assessment Framework. In Dorith Kool et al.: *The Good, the Bad, and the Ugly. A Framework to Assess Security Sectors' Potential Contribution to Stability*. Hague, Centre for Strategic Studies, 2020. 22–37.

a rendvédelmi és fegyveres szervek, többek között a nemzetbiztonságért felelős szolgálatok is. Tevékenységüket a 20. századhoz képest egy jelentősen megváltozott biztonsági és technológiai környezetben látják el, és feladatrendszereik is kitágultak az elmúlt évtizedekben. A felgyorsuló fejlődés kihat a nemzetbiztonsági feladatok ellátását érintő információs és kommunikációs technológiákra (IKT), a digitális térbe áthelyeződő „eszközök" kiszolgáltatottságára és ennek kapcsán a mindennapok során alkalmazott megoldások „kiberbiztonságára", de idesorolhatók a kiberbűnözés növekvő jelensége, a kibertér terroristacélú felhasználása vagy akár az egyes államok működését célzó, nem kívánt „befolyásoló" jelenségek is.

Általános érvényű megállapítás, hogy a nemzetbiztonsági feladatok elválaszthatatlanok az általános technológiai környezettől, különös tekintettel annak infokommunikációs szegmensétől. Ennek fejlődését jól jelzik az ITU[5] statisztikai adatai,[6] amelyek alapján 2020 végén globálisan több mint 4 milliárd volt az internethasználók száma, szemben az öt évvel ezelőtti 3 milliárddal. Napjainkra a városi területeken a háztartások mintegy 72%-a már rendelkezik internet-hozzáféréssel, igaz, ezzel szemben a Föld számos régiójában még mindig rendkívül alacsonynak tekinthető az internet elérésének lehetősége. Az ITU által közzétett becslés alapján az elmúlt években sajátosan alakult a mobiltelefon-előfizetések száma is. Amíg 2019-ben 100 lakosra még 108 mobiltelefon-előfizetés jutott, addig 2020 közepére ez a szám 105-re csökkent, azonban a fejlett országokban még továbbra is növekedést láthatunk. A mobilkommunikációs megoldások jelentőségét egy másik statisztikai adatforrás[7] is alátámasztja, amely szerint a népesség több mint 96%-a rendelkezett valamilyen okostelefonnal.

A technológiák gyors fejlődésébe bepillantva is azt láthatjuk, hogy amíg például 2010-ben az 5,3 milliárd mobiltelefon-előfizetőből 940 millióra volt tehető a 3G platform felhasználóinak száma,[8] 2020 közepére az előfizetések száma már 8,15 milliárd[9] volt, és az év végére a Föld lakosságának 85%-át fedte le a 4G hálózat (amely arány Európában 97% feletti volt).[10] A közösségimédia-platformokat tekintve, a 2021 januárjában 4,2 milliárdos aktív közösségimédia-felhasználói szám az előző év elejéhez képest több mint 13%-os növekedést jelentett.[11] A változás szembetűnő, a hátterében már ott van az a fiatalabb generáció, amely életének elválaszthatatlan része az internet, az arra épülő szabad információelérés és -továbbítás lehetősége. Minden három közösségimédia-felhasználóból két fő a 35 év alatti korosztályból kerül ki.[12] Az ITU adatai alapján 2019 végén globális átlagban a fiatalok közel 70%-a (a fejlett országokban szinte minden fiatal) használta az internetet.

---

5 *International Telecommunication Union* (Nemzetközi Távközlési Egyesület).

6 *Facts and Figures 2020. Measuring digital development.* 4–7. [online], 2020. Forrás: www.itu.int [2021. 05. 12.]

7 Simon Kemp: *Digital 2021. Global Overview Report – DataReportal – Global Digital Insights.* [online], 2021. 01. 27. Forrás: datareportal.com [2021. 05. 12.]

8 *The World in 2010.* [online], 2010. 10. 20. Forrás: www.itu.int [2021. 05. 12.]

9 *ITU Statistics. Key ICT indicators for developed and developing countries, the world and special regions (totals and penetration rates) table.* [online], 2021. Forrás: www.itu.int [2021. 05. 12.]

10 Facts and Figures (2020) i. m. 2.

11 Kemp (2021) i. m. 4.

12 Simon Kemp: *Social Insights.* [online], 2020. 12. Forrás: datareportal.com [2021. 05. 12.]

Tényként megállapítható, hogy a korszerű IKT-megoldások gyors terjedése azt eredményezte napjainkra, hogy a társadalom valamennyi szereplője az infokommunikációs eszközökre alapozza számos mindennapos tevékenységét, legyen az a munka, a tanulás vagy a szórakozás területe. A széles körű használat, a felhasználók igénye, a versenytársak fejlődése újabb és újabb megoldások keresésére ösztönözte a piaci szereplőket, elfogadhatatlanná téve a statikus szemléletet az IKT-szektorban. Továbbá a technológia felhasználói folyamatosan új, jobb, gyorsabb megoldásokat, szolgáltatásokat várnak el a technológia előállítóitól, így az innovációs megfelelés szükségszerűen a cégek stratégiájává vált. Ezt támasztja alá, ha megnézzük a Boston Consulting Groupnak a világ 50 leginnovatívabb gazdasági társaságáról készített felmérését, ahol az első tíz cég között hét technológiai vállalat található (Apple, Alphabet, Microsoft, Samsung, Huawei, Facebook, IBM), valamint három fogyasztási cikkeket forgalmazó vállalat, amelyek tevékenysége azonban megkérdőjelezhetetlenül technológiai (Amazon, Alibaba, Sony).[13] A 21. században az innovációs fejlettség egyenes összefüggésben áll a cég vagyoni értékével, a használt márka értékével. Így nem meglepő módon – a brit Brand Finance piackutató és üzleti tanácsadó vállalat 2021-es „Global 500" ranglistája szerint – az Apple a legértékesebb márka a világon, de az Amazon, a Microsoft és a Facebook is az első tíz helyen szerepel.[14]

Az a világtendencia, hogy az üzleti életben azok a cégek kerülnek lépéselőnybe, amelyek technológiát és innováció alkalmaznak, a biztonsági szektort is változásra kényszerítette. Azon, a bevezetőben már jelzett tényen túl, hogy a nemzetbiztonsági feladatok elválaszthatatlanok az általános technológiai környezettől, érdemes azt is leszögeznünk, hogy a gyorsuló IKT-fejlődés abból a szempontból is hatott a biztonsági területre, hogy olyan, új típusú fenyegetések jelentek meg, amelyek pár évtizede még nem léteztek, és az információs társadalom technológiája nélkül nem jöttek volna létre. A technológiai fejlődés ezzel együtt azonban nem eredményezte azt, hogy a régi típusú fenyegetések megszűntek volna. A biztonsági szféra így az infokommunikációs társadalomban két kihívással is szembesül. Egyrészről az új típusú biztonsági fenyegetésekkel, másrészről, hogy mind az új, mind a régi fenyegetések már egy folyamatosan fejlődő technológián alapulnak. Ennek megfelelően érdemes vizsgálnunk azt a kérdést is, hogy a technológiai környezet megváltoztatta-e a nemzetbiztonsági szervekkel kapcsolatos alapvető elvárásokat.

A nemzetbiztonsági szféra kapcsolata az infokommunikációs társadalommal

A 21. század nemzetbiztonsága ugyanannak az elvárásnak kell megfeleljen, amelynek már évszázadok óta: a döntéshozókat kell ellátni információkkal, ami alapján a törvényes működési rend fenntartható, az állam szuverenitása biztosítható és az állampolgár biztonsága garantálható. Azonban a 21. században teljesen más környezetben kell elérni ezeket a célokat, mint a történelem folyamán eddig bármikor. Szinte közhelyszerűen hat,

[13] Carman Ang: *Ranked. The 50 Most Innovative Companies*. [online], 2020. 07. 17. Forrás: visualcapitalist.com [2021. 05. 12.]

[14] *Global 500 2021. Brand Finance. The annual report on the most valuable and strongest global brands.* [online], 2021. 01. Forrás: brandirectory.com [2021. 05. 12.]

hogy a gyorsan változó világban új kihívások jelentek meg, és a szolgálatoknak már úgy kell szembenézni ezekkel, mi több válaszokat adni rájuk, hogy nem állnak rendelkezésre a megoldáshoz szükséges jól bevált sémák, amelyekhez fordulni lehetne. Így a változó világ, a változások sebességének növekedése önmagában kikényszerítette a szolgálatoktól, hogy alkalmazkodva a velük szemben megjelenő elvárásokhoz új módszereket, metódusokat kezdjenek el alkalmazni.

A változásokhoz való alkalmazkodás nem szüntette meg azt az igényt, hogy a nemzetbiztonsági szféra rendeltetésénél fogva, a feladatainak ellátásához szükséges információ megszerzésének érdekében – jogi felhatalmazás alapján – az állampolgárok szabadságjogait (a szükségesség-arányosság elvét érvényesítve) korlátozhatja. Az infokommunikációs társadalomban a változások ugyanakkor megkövetelték a biztonsági szervektől, hogy alkalmazkodjanak a kihívásokhoz és találják meg azokat a módszereket, amelyekkel ugyanolyan hatékonysággal hajthatják végre a feladataikat, mint az ipari társadalom korában. A különböző országok szolgálatai történelmi tapasztalataik, kultúrájuk alapján különböző megoldásokhoz nyúltak.

A szolgálatok általában két megközelítést alkalmaznak arra, hogy az infokommunikációs társadalomban is végre tudják hajtani a feladatukat az információ, különösen a technikai információ megszerzésének érdekében.

1. Jogszabályalkotás (amely jogszabályalkotás alatt nem az állam, a nemzetbiztonsági szervek jogkörét, feladatait, továbbá eljárásainak garanciáit szabályozó tevékenységét, hanem a titkos információgyűjtés lehetőségeit megteremtő tevékenységét értjük).
2. Technológia (az információgyűjtésre alkalmas technológia alkalmazása).

Bármelyik megközelítés alkalmazása esetén a társadalom, az állam, a gazdaság szereplőinek viszonyrendszerében elmozdulás következik be, aminek célja az, hogy a nemzetbiztonsági érdekek érvényesíthetőek legyenek, de egyben az elmozdulás új helyzetet is teremt a képességek/kitettségek tengelyén, amit folyamatosan értékelni kell, és ha szükséges, ismételten kiigazításokat kell tenni.

Jogszabályalkotás

Az állam a nemzetbiztonsági szervek feladatainak végrehajtása érdekében jogszabályokat alkot, amelyek alapján lehetőség nyílik arra (ezt az állam teremti meg mesterségesen a jogszabályok által), hogy a szolgálatok végre tudják hajtani titkos információgyűjtő tevékenységüket. Ezek a jogszabályok általában a gazdasági szereplőket kötelezik arra, hogy olyan fejlesztéseket hajtsanak végre, amelyek lehetővé teszik a nemzetbiztonsági szervek számára a titkos információk megszerzését, összegyűjtését.[15] A jogalkotási módszer alkalmazásának megvannak az előnyei, így a nemzetbiztonsági feladatok végrehajtásakor a privát szféra is érintetté válik. Ez egyrészről tehermentesíti a nemzetbiztonsági szektort,

[15] Az európai példák mellett hazánkban az elektronikus hírközlésről szóló jogszabály említhető, amely 2003-ban (2003. évi C. törvény az elektronikus hírközlésről) kötelezte a hírközlési szolgáltatókat, hogy a törvényes lehallgatáshoz szükséges fejlesztéseket hajtsák végre.

amely részéről kevesebb humán és anyagi erőforrás közvetlen bevonását igényli a feladatok színvonalas teljesítése. Másrészről hátrányként jelentkezhet, különösen hosszabb távon vizsgálva, hogy a technológiai innováció „kiszervezése" – amely a példát nézve nem a szolgálatoknál, hanem a privát szférában jelentkezik – milyen képesség növekedését jelenti a gazdasági szférában, és esetlegesen milyen típusú kitettség növekedését a nemzetbiztonsági szféra vonatkozásában.[16]

Technológiaalkalmazás

A szolgálatok a megfelelő, rendelkezésre álló technológiákkal hajtják végre az információgyűjtést, nem pedig a jogszabállyal kötelezett gazdálkodó szervezetek végzik el azt helyettük. Ami nem jelenti azt, hogy ne működne a vegyes modell (a valóságban ez működik a leginkább), amikor a jogszabály bizonyos kötelezettségek előírása által támogatást nyújt a szolgálatok által használt technológiák alkalmazásához. A technológiai megközelítés során – a jogszabályi megközelítéssel ellentétben – az állam nem jogszabállyal kötelezi a gazdálkodó szervezeteket a nemzetbiztonsági fejlesztések végrehajtására, hanem a szolgálatok (a gazdasági élet szereplői gyanánt) megrendelőként, vásárlóként jelennek meg, és piaci alapon vesznek igénybe fejlesztést mint üzleti szolgáltatást. Ebben a megközelítésben az egyik legfontosabb kérdés, hogy a szolgálatok ki által fejlesztett technológiát használnak, ahol a két lehetséges opció a saját fejlesztésű, illetve a vásárolt technológiák alkalmazása.

A saját fejlesztés valamennyi szolgálat számára fontos feladat maradt, de az IKT-szektor fejlődése eljuttatta oda a szolgálatokat, hogy kizárólag saját fejlesztéssel (legalábbis, ha nem innovációs nagyhatalom szolgálatáról beszélünk) nem tudják hatékonyan megoldani feladataikat, és az államok szolgálatai kisebb-nagyobb mértékben, az IKT-szektor fejlődésével párhuzamosan egyre inkább igénybe veszik minősített beszállítók fejlesztéseit/termékeit. Természetesen továbbra is vannak olyan területei az információgyűjtésnek és az információvédelemnek, amelyeken a szolgálatok saját fejlesztésű technológiát használnak, szigorú biztonsági szempontok figyelembevételével. Az, hogy melyik állam, mennyire él a privát szektorbeli lehetőségekkel, függ gazdasági, kulturális hagyományaitól.

A változó környezet általános jellemzői

A nemzetbiztonsági gondolkodás változó környezethez való alkalmazkodását számos, az ágazaton túlmutató sajátosság és tendencia jellemzi, amelyek érvényesülésére a nemzetközi színtéren láthatunk példákat:

A nemzetbiztonság szereplői számára egyre fontosabbá válnak a társadalmi, ipari, tudományos kapcsolatrendszerek, ezek kialakítása és fenntartása. A biztonság komplex megközelítésében előtérbe kerül a nem állami, informális biztonsági szereplőkkel

[16] Bács Zoltán György: Innováció és nemzetbiztonság a 21. században. In Ruzsonyi Péter (szerk.): *Közbiztonság. Fenntartható biztonság és társadalmi környezet tanulmányok III.* Budapest, Ludovika Egyetemi Kiadó, 2020. 959–971.

való közös gondolkodás szükségessége, az innováció és az azt biztosító struktúrák alkalmazása.[17] Az innováció nagy, nemzetközi üzleti szereplői mellett teret nyernek a kisebb K+F szereplők, amelyek közül kiemelhetők például a mesterséges intelligencia területén a technológiai startup-vállalkozások, amelyek földrajzi értelemben jól behatárolható térségekre (például Észak-Amerika, Kína, Európa és Izrael területére)[18] koncentrálódnak. A felértékelődő kapcsolatok okai között látható, hogy a technológiai fejlődés jelen van mind a katonai, mind a civil területeken, amelyek között nincs egyértelmű választóvonal, és kölcsönösen hatással vannak egymás fejlődésére.[19] A fejlesztési irányok mögött ugyanakkor közvetlenül megjelenik a gazdasági érdekszféra is, ahol az államok partnerként tekinthetnek a külső üzleti és „akadémiai" tudományos szereplőkre. Ennek folyamatai nem új keletűek, már a 20. században számos példát láthatunk az egyetemi tudósok eredményeinek kereskedelmi hasznosítására.[20] Amíg az Egyesült Államok, illetve az EU esetében e folyamatok erőteljesebben támaszkodnak a nem állami szereplőkre, addig Kína, illetve Oroszország esetében a fokozottabb kormányzati megjelenést figyelhetjük meg.

– Továbbra is jelen van a (nemzet)biztonsági rendszerekkel szembeni bizalom hiánya. Ennek mértéke a demokráciáktól az autokratikus államokig széles skálán mozoghat, így a társadalmi „érzékenységhez" igazodva eltérő megközelítéseket láthatunk a korszerű technológiáknak a biztonság szolgálatába való állítása terén is.[21] Talán legegyszerűbb példaként a globális pandémia kérdése emelhető ki. Mivel a világjárvány egyaránt sújtja az országokat, így az annak kezelése során szolgálatba állított új „biztonsági célú technológiák, megoldások" megválasztása jól jelezheti éppen ezek társadalmi elfogadottságának mértékét, valamint a (nemzet)biztonsági kihívások egyéb területein is lehetséges jövőbeli szerepét. Míg egyes országokban a járvány terjedésének megfékezése érdekében megkerülhetetlen megoldásként tekintettek az IKT-környezet biztosította új megoldásokra, addig más országokban az egyének döntésének szabadsága, valamint az adatvédelem fokozott szerepe került előtérbe.
– Jól látható azonban az a folyamat is, amely a kibertér „határainak ismeretlensége" és így szabályozatlansága révén a profitorientált globális szereplők térnyerését eredményezte. Mindez kétélű fegyver, hiszen a korszerű technológiák által biztosítható előnyök közvetve számos „függőséget" is eredményeznek. A globális technológiai cégek megoldásainak használatához köthető, korábban elképzelhetetlen mértékű adatmennyiség akaratlanul is az adott egyén, csoport, társadalom vagy állam működésének lenyomatát jelentheti, amelyek képviselői addig nem látott

[17] Hazánk esetében ezt támasztja alá az NKFIH TKP 2021 Nemzetvédelem, nemzetbiztonság alprogramja is. Lásd *Tématerületi Kiválósági Program 2021*. [online], 2021. 05. Forrás: nkfih.gov.hu [2021. 05. 12.]

[18] *Artificial Intelligence – A strategy for European startups.* [online], 2018. Forrás: rolandberger.com [2021. 05. 12.]

[19] Anthony H. Cordesman – Grace Hwang: *U.S. Competition with China and Russia. The Crisis-Driven Need to Change U.S. Strategy*. Center for Strategic & International Studies, 2020. 138.

[20] Jon Agar: The central debates on science and innovation. In *Science Policy under Thatcher.* London, UCL Press, 2019. 67.

[21] Dobák Imre: Társadalom – technológiai környezet – nemzetbiztonság. In Ruzsonyi Péter (szerk.): *Közbiztonság. Fenntartható biztonság és társadalmi környezet tanulmányok III*. Budapest, Ludovika Egyetemi Kiadó, 2020. 959–971.

vitákat generálhatnak a tudomány, az etika, a jog vagy akár a biztonság különböző színterein.[22] Amíg a digitalizáció – többek között rendkívüli gazdaságformáló hatása miatt – a technológiai fejlettségért vívott küzdelem fontos területe, addig a polgárok szintjén alkalmazott „túlzott megfigyelések" gyakran az ellenvélemények visszaszorításának lehetőségétől való félelmet erősítik.

– A biztonságpolitikai szaktanulmányok egyre gyakrabban hangsúlyozzák azon, nem állami szereplők jelentőségét, amelyek biztonságpolitikai, határokon átnyúló befolyásoló hatásával az egyes államoknak számolniuk kell. E szereplők mögöttes szándékainak, képességeinek, biztonságra gyakorolt hatásainak valós súlya nehezen meghatározható. Tevékenységük közvetlen hatással van a világról szóló ismereteinkre, napi információinkra, környezetükben összpontosul a technológiai fejlődés új irányainak jelentős része. A társadalom széles rétegeit megszólító képesség, valamint az ehhez kapcsolódó kétélű felelősség különös szerepet jelent, főként a közösségi média platformjai számára, ahol a szabad hozzáférés, az információtovábbítás szabadsága eddig nem látott etikai kérdéseket hozott felszínre.
– A média témakörére kitekintve, az erőszakos tartalmak korlátozásának kérdéseit láthatjuk, amelyekre ezek a szereplők is egyre nagyobb hangsúlyt fektetnek. Számos szolgáltató, így például a Google már szkenneli a gyermekek szexuális kizsákmányolásához kapcsolódó anyagokat, azonban ennek gyakorlati formái szintén vitákat generálhatnak. Példaként az Apple által bejelentett, a gyermekekkel történő szexuális visszaélésekre irányuló fotók feltöltésének felismerésére szolgáló megoldás említhető, amely a keresést már a felhasználó telefonján megkezdené.[23] A magánszféra védelmét hangsúlyozók oldaláról az ügyféloldali szkennelés egyfajta kezdetként értelmezhető, és ellentmondhat a korábban még hangoztatott, a magánszféra védelmében alkalmazott titkosítás fontosságának. Tényként kezelhetjük, hogy az adatok védelmét biztosító megoldások egyrészről szolgálhatják a magánszféra fokozottabb védelmét, ugyanakkor egy-egy biztonsági esemény (például terrorcselekmény) kapcsán a nemzetbiztonsági szervezeteket komoly feladat elé állíthatják, de technikai nehézséget okozhatnak a káros tartalmak automatizált felismerése során is.
– Amíg a témakörben született tanulmányok egy évtizeddel ezelőtt még csak a kibertér egyre erősödő szerepére hívták fel a figyelmet, addig napjainkra már egyértelművé vált, hogy jelentősége a biztonság szempontjából alapvető tényezővé vált.[24] A NATO által is hadszíntérként értelmezett kibertérben napról napra jelennek meg új K+F megoldások, főként az Egyesült Államok, Kína és Oroszország haditechnikai, illetve nemzetbiztonsági ágazatához sorolható területeken. A hadviselés szempontjából a kibertér és a mesterséges intelligencia terrénumának jelentősebb szereplői ma az Egyesült Államokhoz, Oroszországhoz, Kínához és kisebb mértékben

[22] Dobák (2020) i. m. 18.

[23] Tonya Riley: *Apple's new solution to combat child abuse imagery could radically shift encryption debate.* [online], 2021. 08. 06. Forrás: cyberscoop.com [2021. 09. 12.]

[24] Krasznay Csaba: Kiberbiztonsági kompetencia hálózatok Európában – K+I+F-lehetőségek a következő évtizedben. *Scientia et Securitas,* 1. (2020), 1. 43–48.

az Európai Unióhoz kapcsolhatók.[25] Egyes tanulmányok[26] a technológiai fölény kapcsán a nukleáris fegyverek nagyhatalmi birtoklásával látnak hasonlóságot, ahol egy „információs ernyő" létrehozása és bizonyos technológiák szövetségesekkel történő megosztása segítheti elő ennek a fölénynek a megtartását.

– A technológiai fölényért vívott küzdelemben a kulcstechnológiák (az IKT területéhez kapcsolódva például az 5G és a mesterséges intelligencia) kérdései napjainkra már stratégiai szinten vannak jelen, és fejlődési irányaik hosszabb távon hatást gyakorolnak a biztonságpolitikai viszonyokra (így például az európai viszonylatban a kulcstechnológiák körében megfigyelhető kínai térnyerés már az Egyesült Államok stratégiai érdekeit is érzékenyen érintheti).[27] A fejlődés kapcsán egyrészről a fő kérdés az, hogy ezen technológiák milyen gyorsan válnak meghatározóvá a különböző iparágak tevékenységében, valamint milyen mértékben érintik majd az egyes nemzetek kritikus infrastruktúráját. Másrészről, értékteremtő képességeikkel alapvető módon befolyásolhatják a következő évtizedek gazdaságának és kiberbiztonsági fejlődésének irányait, ahol az előrejelzések alapján 2035-re Kína, az USA, Japán, Németország, Dél-Korea, Franciaország és Nagy-Britannia szerepe válhat meghatározóvá.[28] (Több tanulmány is a várható kínai erőfölényt emeli ki, Peking modern információs és kommunikációs technológiái révén nemcsak a saját, hanem más országok lakosságának megfigyelésére és ellenőrzésére is képessé válhat.)[29]
– A fejlődésben meghatározóvá válnak a korszerű technológiák nemzeti és nemzetközi stratégiai irányai. Az egyik ilyen megállíthatatlanul fejlődő terület a mesterséges intelligencia, amely már most is látható eredményeinek köszönhetően egyre fontosabb tényezőként van jelen a biztonsági és – a témakörben csak néhány évre visszatekintő – stratégiai gondolkodásban. Az első nemzeti mesterségesintelligencia-stratégiát a kanadai kormány adta ki 2016-ban,[30] majd a szabályozást megelőző ütemben fejlődő technológiai terület kezelésének stratégiai szintű dokumentumait több ország is elkészítette. A technológiai téren globális nagyhatalomnak tekinthető Kína 2017-ben adta ki saját nemzeti szintű mesterségesintelligencia-stratégiáját,[31] az EU 2019 áprilisában adta közre etikai iránymutatását a megbízható mesterséges intelligencia[32] témakörében, egyfajta etikai keretet biztosítva a rohamosan fejlődő terület európai jövőjéhez. Hazánk *Mesterséges Intelligencia Stratégiá*ja

[25] Benjamin Fricke: *Artificial Intelligence, 5G and the Future Balance of Power.* [online], 2020. 01. 01. Forrás: jstor.org [2021. 09. 12.]
[26] Mariel Borowitz: An Interoperable Information Umbrella. Sharing Space Information Technology. *Strategic Studies Quarterly,* 15. (2021), 1. 129.
[27] Luis Simón – Linde Desmaele – Jordan Becker: Europe as a Secondary Theater? Competition with China and the Future of America's European Strategy. *Strategic Studies Quarterly,* 15. (2021), 1. 107.
[28] Frank Umbach: *EU Policies on Huawei and 5G Wireless Networks Economic Technological Opportunities vs. Cybercecurity Risks.* [online], 2020. Forrás: jstor.org [2021. 05. 12.]
[29] Fricke (2020) i. m. 18.
[30] Peter Engelke: *AI, Society, and Governance. An Introduction.* [online], 2020. 03. 01. Forrás: jstor.org [2021. 05. 12.]
[31] Graham Webster et al.: *Full Translation. China's ‚New Generation Artificial Intelligence Development Plan'.* [online], 2017. 08. 01. Forrás: newamerica.org [2021. 06. 07.]
[32] *Ethics Guidelines for Trustworthy Artificial Intelligence.*

2020-ban jelent meg,[33] a témakör azonban az EU szintjén is még csak a jogalkotási fázis kezdeti szakaszánál jár.[34] A társadalom számára pozitív hatásai mellett vizionált negatív hatásai széles tudományos közeget késztetnek társadalmi szintű vitára akár a tudományos, a technikai, a politikai vagy humanista oldalról megközelítve.[35] Jelen van ebben a korszerű technológiák szélesebb köre iránti általános bizalmatlanság is, a globális biztonságpolitikai erőviszonyok módosulásától való félelem, a társadalom működése során keletkező nagy mennyiségű adat „etikátlan" felhasználásával való szembesülés vagy akár az egyre nagyobb mértékben digitalizálódó társadalom manipulálhatóságának tapasztalata. Nemzetbiztonsági szempontból még megválaszolatlan kérdés, hogy a mesterséges intelligencia hogyan fogja „támogatni" a kibertérben megjelenő illegális tevékenységeket, felhasználhatják-e majd azokat számítógépes támadásokra, vagy éppen az illegális tevékenységek elleni küzdelem és a kiberbiztonság erősítése terén kaphatnak majd kiemelt szerepet. A nemzetbiztonság vs. megfigyelés témakörét érintve a nemzetközi szakirodalmak az arcfelismerési technológiákat, valamint egyes, biztonsági szempontból érzékeny területeken a személyek azonosítását, viselkedésük figyelemmel kísérését emelik ki példaként, ahol az állami szereplők már széles körben alkalmaznak különböző megoldásokat.

– Az európai biztonsági kérdések sokszínűségéhez kapcsolódik az Egyesült Államok – Kína – EU, illetve Oroszország viszonylatában hangsúlyossá váló technológiai kulcselem, az ötödik generációs mobilhálózati technológia (5G) kérdésköre. Ez a technológia szakértők szerint alapjaiban változtathatja meg a biztonság és a gazdasági fejlődés számos elemét, hiszen az információtovábbítás gyorsaságának és adatátviteli kapacitásának növekedésével lehetővé teszi a tárgyak internetje (IoT), valamint egyéb intelligens megoldások tömeges térhódítását, használatát. A fejlődés ütemére utal, hogy „az előrejelzések szerint az internetre csatlakoztatott eszközök száma 2025-től kezdődően eléri az 50 milliárdot".[36] Ugyanakkor e változások korábban nem látott mértékű és komplexitású kiberbiztonsági kockázatokat, sebezhetőségeket is eredményeznek, amelyeknek már nemzetbiztonsági összefüggései vannak. Prognosztizálható ugyanakkor az is, hogy hosszabb távon a jelzett technológiai versenyben előnybe kerülő országok vélhetően nagyobb súllyal lesznek képesek formálni a korszerű technológiák fejlődését, ami hatással lehet az érdekeiket alacsonyabb szinten képviselni tudó országok biztonságára is. Kína példája ebből a szempontból sajátosnak tekinthető, hiszen amíg alapvető elzárkózást tapasztalhatunk esetében a nyugati globális infokommunikációs technológiai cégek platformjai elől, addig a számára meghatározó 5G szabad, globális szintű térnyerésében érdekelt.

---

[33] 1573/2020. (IX. 9.) Korm. határozat Magyarország Mesterséges Intelligencia Stratégiájáról, valamint a végrehajtásához szükséges egyes intézkedésekről. *Magyar Közlöny,* (2020), 202. 6356.

[34] Auer Ádám: Gondolatok a mesterséges intelligencia egyes polgári jogi kérdéseiről. *Scientia et Securitas,* 2. (2021), 1. 108.

[35] Engelke (2020) i. m. 24.

[36] *5G – Fifth generation of mobile technologies.* [online], 2019. 12. Forrás: itu.int [2021. 06. 08.]

A fentiekkel összhangban, a nemzetközi színtérre kitekintve eltérő (nemzet)biztonsági gondolkodással, nemzeti szintű intézményrendszerekkel, valamint a biztonságot szolgáló technológiákba vetett társadalmi bizalommal találkozhatunk. Közös elemnek az innováció felértékelődő szerepe, továbbá a technológiai környezet fejlődéséhez köthető külső hatások, tendenciák tekinthetők, amelyek hosszabb távon mindenképpen hatással lesznek térségünk és az egyes országok biztonságára, valamint azok nemzetbiztonsági intézményi szereplőinek tevékenységére.

Európa és Magyarország az innovációs versenyben

Az Európai Unió minden évben értékeli saját innovációs helyzetét.[37] A 2021-es vonatkozó dokumentum a következő megállapításokat teszi:

> „Globális értelemben az EU jobban teljesít, mint Brazília, Dél-Afrika, India, Kína és Oroszország, azonban lemaradásban van Ausztráliához, Dél-Koreához, az Egyesült Államokhoz, Japánhoz és Kanadához képest. 2014 és 2021 között az EU javított relatív pozícióján hat globális versenytársával szemben: az Ausztráliához és Kanadához viszonyított teljesítménybeli lemaradása csökkent, ugyanakkor a Brazíliához, Dél-Afrikához, Indiához és Oroszországhoz viszonyított teljesítménybeli előnye nőtt. Az EU relatív pozíciója azonban romlott négy globális versenytársával szemben: a Dél-Koreához, az Egyesült Államokhoz és Japánhoz viszonyított teljesítménybeli lemaradása nőtt, a Kínához viszonyított teljesítménybeli előnye pedig csökkent."[38]

Az eredmények jelentős részben a kutatásra fordított összegektől függnek, és a pénzügyi adatokat vizsgálva az Európai Unióban „évente kutatás-fejlesztésre fordított összeg az Egyesült Államokétól a GDP 0,8%-ával, Japánétól pedig a GDP 1,5%-ával marad el".[39]

E tendenciák megváltoztatása céljából az EU létrehozta az Innovatív Unió koncepcióját. Az Innovatív Unió végső célja, hogy Európa bekerüljön a világ innovációs nagyhatalmai közé (az Egyesült Államok és Kína mellé). Ennek érdekében megvalósítandó feladat, hogy az innovatív ötletek társadalmasítása előtt ne legyenek adminisztratív akadályok, valamint szorgalmazza, hogy az innovációs szereplők közötti kollaboráció mind nemzeti, mind nemzetközi szinten megerősítést nyerjen. Az Innovatív Unió koncepciójának megvalósítása érdekében 2021-ben indították el a Horizont Európa[40] programot, amelynek egyértelmű célja növelni az EU versenyképességét, segíteni a stratégiai prioritások megvalósítását. A stratégiai prioritások a következők:

---

[37] Vö. *European innovation scoreboard 2021.* [online], 2021. 06. 28. Forrás: ec.europa.eu [2021. 09. 02.]

[38] *EIS 2021. Executive summary.* [online], 2021. 07. 22. Forrás: ec.europa.eu [2021. 08. 12.]

[39] Frédéric Gouardères – Albane Keravec: *Innovációs politika.* [online], 2021. 06. Forrás: europarl.europa.eu [2021. 08. 06.]

[40] *Javaslat az Európai Bizottság és Tanács Rendeletének megalkotására a Horizont Európa kutatási és innovációs keretprogramról, valamint részvételi és terjesztési szabályainak megállapításáról.* [online], 2018. 06. 07. Forrás: europarl.europa.eu [2021. 08. 06.]

– nyílt tudomány (25,8 milliárd eurós költségvetés);
– globális kihívások és ipari versenyképesség (52,7 milliárd eurós költségvetés);
– nyílt innováció (13,5 milliárd eurós költségvetés).[41]

Az Európai Unió a tagállamok vonatkozásában kidolgozott egy értékelési rendszert is az innovációs teljesítmény mérésére, amely több indikátorból áll, és a következő területekre állapított meg mérőszámokat: az állami és privát szféra által támogatott oktatási rendszer, a megfelelő kutatási környezet, a hatékony partnerség a gazdasági élet és az akadémiai szektor között, az innovációbarát üzleti környezet és nem utolsósorban a meglévő/fejlődő erős digitális infrastruktúrák és digitális képességek.

Az Unió minden évben az Innovációs Eredménytáblában foglalja össze a kulcsmutatók alapján összeállított uniós innovációs teljesítményi rangsort. Az eredménytábla alapján[42] az innovációs rangsor élén Svédország áll, mögötte a skandináv és a nyugat-európai országok mint a vezető vagy erős innovátorok csoportja. Magyarország a szerény innovátorok csoportjába tartozik (Romániával, Bulgáriával, Litvániával, Lengyelországgal és Szlovákiával együtt), összesített innovációs mutatójának értéke az uniós átlag 67,9%-át éri el. Ha az innováció dinamikáját[43] vizsgáljuk, a 2014-es évet véve bázisnak (ez volt az előző uniós költségvetési ciklus első éve), az Unió 12,5%-kal növelte innovációs teljesítményét, kiugró eredménnyel Észtország (36%-kal) és Ciprus (33%-kal) fejlődött a leginkább, Magyarország (6%-os erősödéssel) az Uniós országok közül Romániát, Bulgáriát, Litvániát, Szlovákiát előzte meg a fejlődés ütemét tekintve.

2020 és 2021 között az innovációs eredménytábla adatai alapján Magyarország a digitalizáció (szélessávú internet elterjedtsége), valamint az ipari szereplők kutatás-fejlesztési tevékenységének kormányzati támogatása terén erősödött. A kormányzati támogatás erősödését támasztja alá az is, hogy a magyar Kormány az innovációs ökoszisztéma fejlesztése érdekében, a meglévő szervezetrendszer keretében, a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal (NKFIH) vezetésével 2020-ban Laboratóriumok kialakítását kezdte meg több, innovatív megközelítést igénylő támogatási területen. A Nemzeti Laboratóriumok finanszírozására az NKFIH 2020. évi költségvetésében 14,095 milliárd forint állt rendelkezésre, 2021-ben 15,123 milliárd forint.[44]

A témakört ismertető forrás megfogalmazza, hogy a Nemzeti Laboratóriumok rendszerének célja, hogy egy teljesen új megközelítést hozzon a tudományos gondolkodásba. Olyan tudásközpontok kialakításáról van szó, amelyek „együttműködésen alapuló, dinamikus színteret biztosítanak”[45] a kutatások számára. A megvalósítandó vízió szerint

---

[41] *Az Európai Parlament és a Tanács Rendelete a Horizont Európa kutatási és innovációs keretprogram létrehozásáról, valamint részvételi és terjesztési szabályainak megállapításáról.* [online], 2018. 06. 07. Forrás: eur-lex.europa.eu [2021. 08. 06.]

[42] EIS (2021) i. m.

[43] *European and Regional Innovation Scoreboards 2021 – Questions and Answers.* [online], 2021. 06. 21. Forrás: ec.europa.eu [2021. 08. 12.]

[44] *A Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal 2021. évi költségvetésének szöveges indokolása.* [online], 2020. Forrás: parlament. hu [2021. 06. 07.]

[45] Bencze Áron: *Aktivizálták az innovációs ökoszisztéma szereplőit.* [online], 2021. 08. 02. Forrás: innoteka.hu [2021. 08. 20.]

egy tématerület „hazai szakmai műhelyei koncentrálódnak ezekben a tudományos csomópontokban, azzal az elérendő céllal, hogy a tevékenységükből származó gazdasági, társadalmi és környezeti eredményeket hazai és nemzetközi környezetben egyaránt hasznosítani”[46] lehessen.

A Nemzeti Laboratórium fő célkitűzései:

- „egy adott tématerület hazai szakmai műhelyeinek koncentrálása;
- globális kihívásokra nemzetközi szinten választ adni képes képességek kialakítása, továbbfejlesztése;
- kutatási eredmények gazdasági, környezeti, kormányzati hasznosítása (tudástranszfer).”[47]

A 2020-as évben a következő tématerületeket határozták meg, amelyekben a Laboratóriumok kutatási-fejlesztési célzattal megkezdhették a működésüket:[48]

- ipar és digitalizáció;
- kultúra és család;
- egészség;
- biztonságos társadalom és környezet.

A tématerületek meghatározásánál az NKFIH figyelembe vette a társadalom legfontosabb szegmenseit, amelyekben az innováció alapvető elvárás a fejlődés érdekében. A negyedikként említett kutatási-fejlesztési tématerület a biztonságos társadalmat és környezetet állította a központba, ezzel is hangsúlyozva, hogy a kormányzat felismerte és elvárja, hogy az állam biztonsági szervei képesek legyenek a globális kihívásokra nemzetközi szinten választ adni, aminek kulcsa az infokommunikációs társadalmakban a folyamatos innováció.

Hazai nemzetbiztonsági innovációs struktúrák

Valamennyi szolgálat célja, hogy az általa alkalmazott titkos információgyűjtéssel kapcsolatos megoldások technikailag fejlettek legyenek és minél kevésbé ismertek az arra nem jogosultak előtt. Ezeket a célokat meg lehet valósítani vásárlással is, hiszen a hadiipari és kettős felhasználású termékeknek/technológiáknak önálló iparága alakult ki.

A védelmi ipar a különböző országokban különböző fejlettségi szinten áll, azonban kijelenthetjük, hogy az elmúlt években Magyarországon „kiemelt nemzeti és gazdaságstratégiai célként került megjelenítésre, hogy Magyarország a közép-európai régió meghatározó védelmi ipari központjává váljon”.[49] Ennek vannak hagyományai Magyarországon, hiszen a rendszerváltás óta több modern hadiipari cég működik nálunk, továbbá 2021-ben a hazai védelmi ipar következő szintre lépését jelentette, hogy az Innovációs

[46] Bencze (2021) i. m.

[47] *Nemzeti Laboratóriumok Program.* [online], 2021. 01. 05. Forrás: nkfih.gov.hu [2021. 05. 12.]

[48] Nemzeti Laboratóriumok Program (2021) i. m.

[49] *Palkovics László szakmai irányítása alá kerülnek a védelmi iparhoz kapcsolódó állami cégek.* [online], 2021. 06. 04. Forrás: portfolio.hu [2021. 08. 03.]

és Technológiai Minisztérium irányítása alatt a Kormány létrehozta a Nemzeti Védelmi Ipari Innovációs Zrt.-t.

A hadiipartól[50] célszerű bizonyos szempontból megkülönböztetnünk a nemzetbiztonsági jellegű ipart, amelyben az előállított technológiák felhasználási célja jelentős különbséget mutat, de egyéb jellemzőiben is vannak eltérések. A nemzetbiztonsági ipar nagyobb hasonlóságot mutat a polgári iparral, mintegy átmenetet képezve a polgári és hadiipar között. Habár a nemzetbiztonsági iparnak Magyarországon is vannak gyökerei, a kezdeti lépéseken túl még nem jellemző a nemzetbiztonsági szektorra a hadiiparhoz hasonló dinamikus fejlődés, amelynek fejlettségi szakaszában már valódi nemzetbiztonsági iparról lehetne beszélni.

Az infokommunikációs társadalom kihívásainak való megfelelés, a diszruptív technológiák megjelenése a 2020-as évek elején megmutatta, hogy a nemzetbiztonsági közösségnek újabb kihívással kell szembenéznie. Az IKT-szektor fejlődési üteme exponenciálisan növekszik, és a nemzetbiztonsági szervezetek által alkalmazott eddigi megközelítések (jogalkotás, technológiaalkalmazás) már nem nyújtják azt az eredményességet, amelyet egy évtizeddel ezelőtt. A nemzetbiztonsági közösség az eddig alkalmazott megközelítések mellett új irányok feltérképezését kezdte meg. A szolgálatok célja egyszerű – ez nem változott az ipari társadalmak kora óta – az információgyűjtési képesség fenntartása/fokozása az újonnan megjelent technológiák esetében is.

Mindennek alapján felmerül a kérdés, hogy milyen technológiákkal kell szembenéznie a nemzetbiztonsági szférának 2021-ben. Az iparági szakértők szerint[51] a kvantumszámítástechnika, a 3D nyomtatás, a felhőalapú alkalmazások (a többszintű felhő kérdései), az Ipar4.0 projektek, az automatizáció, a robotika és a mesterséges intelligencia azok a kihívások, amelyek meghatározzák a gazdasági élet szereplőinek fejlesztéseit, amelyeket azután a társadalom hasznosít. Továbbá az 5G, valamint a dolgok internetjének (IoT) a mindennapi életben való megjelenése mind a mennyiségi, mind a minőségi kihívások szempontjából arra ösztönzi a szolgálatokat, hogy ők is olyan módszereket vezessenek be, amelyek eddig nem nyertek szisztematikus felépítést a nemzetbiztonsági kollaborációk rendszerében. Ma már tényként kijelenthető, hogy az új IKT-k (például 5G, IoT) megjelenése lépésre kényszerítette a szolgálatokat, és már az innovációs ökoszisztémában megjelenő állandó szereplőként lehet rájuk tekinteni.

Innovációs struktúrák

Chris Anderson fogalmazta meg az innovációról:

> „Az innováció az emberek között történik. Minél jobban bevonódnak emberek a különböző témákba, minél nyitottabbak a különböző szintek egymásra, annál gyakoribb

[50] A témakörhöz lásd Petkovich Tamás: A hadiipar fejlesztési lehetőségei Magyarországon. *Katonai Logisztika,* 24. (2016), 1. 54–87.

[51] Lásd többek között Krasznay (2020) i. m.; Robin Mansell: Adjusting to the digital. Societal outcomes and consequences. *Research Policy,* 50. (2021), 9. 1–10.

> a szikra, és annál jobb innováció születik. Nem kell mást tenni, mint kitárni a kapukat, és teret adni az embereknek."[52]

Az innovációs szemlélet nemcsak mérföldkő, de egyben szükségszerű lépés, amely azért jelent új megközelítést a nemzetbiztonsági munkában, mert a szervezeteknél kezdetektől fogva érvényesülő alapelv, a zártság, a titkosság újragondolását jelenti most, ami egyben alkalmazkodás az infokommunikációs társadalom kihívásaihoz.

Az a változás, hogy Magyarországon a nemzetbiztonsági szféra az innovációs ökoszisztéma tagjává vált, szakmai szükségszerűség volt, mert az innovációs folyamat (tudás létrehozása – technológiafejlesztés – sikeres bevezetés)[53] legegyszerűbb megvalósítása így vált lehetővé 2020-ban, amikor az NKFIH létrehozta a Nemzeti Laboratóriumok programot, amelynek keretében 17 Nemzeti Labor jött létre. A „Biztonságos társadalom és környezet" tématerületen hat laboratórium kezdte meg működését a biztonsági kérdések széles spektrumán, így a termőföldbiztonságtól a nukleáris hulladék kezelésének kérdésein át előtérbe kerültek azok a jövőnket meghatározó kérdések, amelyeket az innovációs térben szükséges és ideális kezelni. (Nemzeti Lézeres Transzmutációs Központ, Nemzeti Agrártechnológiai Laboratórium, Nanoplazmonikus Lézeres Fúzió Kutatólaboratórium, Éghajlatváltozás Multidiszciplináris Nemzeti Laboratórium).

A biztonsági témakörök között egyértelmű volt, hogy a nemzetbiztonsági kérdéseknek is helyük van a laboratóriumok között, ezek sem maradhatnak ki a programból, hiszen az innováció szükségszerűvé vált a szolgálatok számára. Így két laboratórium is – a Biztonsági Technológiák Nemzeti Laboratóriuma és az Infokommunikációs és Információtechnológiai Nemzeti Laboratórium – napjaink nemzetbiztonsági kihívásainak kutatását tűzte zászlajára.

A Biztonsági Technológiák Nemzeti Laboratóriuma[54] Magyarország Nemzeti Biztonsági Stratégiáját[55] követve a technológiaalapú biztonság három pillérének – intézménybiztonság, településbiztonság és kiberbiztonság – integrált kutatását és a kapcsolódó innovációt célzó programokat helyezte fókuszába, aminek keretében nemzetstratégiai fontosságú alapkutatásokat végez a migráció, az energiabiztonság, a kiberbiztonság, a katasztrófavédelem és a klímavédelem területén. A Biztonsági Technológiák Nemzeti Laboratóriumának megvalósítója a Nemzeti Közszolgálati Egyetem.

Az Infokommunikációs és Információtechnológiai Nemzeti Laboratórium (Infolab)[56] célja elsősorban az, hogy az egyes technológiák – különösen az új generációs mobiltechnológiák (5G, 6G), a mesterséges intelligencia, a kvantum-számítástechnika – fejlesztésével létrejövő eredményekkel együtt megjelenő biztonsági kihívások ismertek és egyértelműek legyenek a szolgálatok előtt, másodsorban, hogy a biztonsági kérdésekre már

---

[52] Chris Anderson: *Az innovációról.* [online], 2017. 05. 13. Forrás: citatum.hu [2021. 07. 04.]

[53] *Oslo Manual 2018. Guidelines for Collecting, Reporting and Using Data on Innovation.* [online], 2018. Forrás: oecd-ilibrary.org [2021. 07. 16.]

[54] *Nemzeti Laboratóriumok bemutatása.* [online], 2021. 01. 07. Forrás: nkfih.gov.hu [2021. 07. 15.]

[55] A *1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.* [online], 2020. 04. 21. Forrás: net.jogtar.hu [2021.08. 16.]

[56] Nemzeti Laboratóriumok bemutatása (2021) i. m.

a megjelenésük időszakában megszülessenek a válaszok is. Ezzel is lehetőséget adva arra, hogy a szolgálatok a retrospektív szemlélet helyett a prospektív megközelítést alkalmazzák tevékenységük nagyobb részében. Az Infolab meghatározta főbb kutatási irányait, amelyek a következők:

- „az alapnyilvántartások és a nemzeti adatvagyon nyilvántartásokhoz kapcsolódó szakrendszerek szemantikai interoperabilitásának kapcsolódása MI technológiákhoz;
- a közigazgatási szakrendszerek elektronikus (automatikus) együttműködését megteremtő köztes réteg kapcsolódása az adaptív megoldásokhoz;
- az ügyintézési eljárások formális leírása és gépi reprezentáció;
- a nemzeti adatvagyon védelméhez szükséges K+F;
- a mesterséges intelligencia (MI) alkalmazásának kutatása a kibervédelem területén;
- kiberképességek fejlesztésének támogatása (észlelés, felderítés, reagálás);
- protokollok és titkosítási algoritmusok sebezhetőségének vizsgálata, kvantumkommunikáció.
- 5G vonatkozású kibervédelmi kutatások”.[57]

Az Infolab megvalósítója a Nemzetbiztonsági Szakszolgálat (NBSZ) és az IdomSoft Informatikai Zártkörűen Működő Részvénytársaság (Idomsoft) konzorciumi formában. Az Infolab létrehozása mérföldkőnek tekinthető a nemzetbiztonsági szolgálatok magyarországi történetében, mert ez az első lépés, amikor egy technológiát alkalmazó nemzetbiztonsági szolgálat teljes transzparenciával jelenik meg az innovációs ökoszisztémában. Cél azokban az alap- és alkalmazott kutatásokban való részvétel, amelyek a nemzetbiztonsági szolgálat fejlesztési céljait segítik az alapfeladatok végrehajtása érdekében. A széles körű együttműködésben az egyetemi, kutatói közösségek, az iparági szereplők, valamint az NBSZ is aktív szerepet vállal a kitűzött célok megvalósítása érdekében. Az InfoLab, hasonlóan a többi laboratóriumhoz, 2020-ban jött létre, és 2021-ben már szintet tudott lépni a kollaboráció kérdésében, amikor a konzorciumon belül létrehozta a Biztonságos Digitális Társadalom Innovációs Klasztert (BDTIK),[58] amelyek együtt intézményes színteret képeznek a kutatási eredmények társadalmi, gazdasági és környezeti hasznosításának együttműködéséhez.

A Laboratórium működése öt évre tervezett, és az elmúlt év tapasztalata megmutatta, hogy a kutatási célkitűzéseken túli sikereket is el lehet érni az önálló prioritásként kezelt tudományos együttműködések erősítése tekintetében, így a Laboratóriumok aktívan tudják érvényesíteni Chris Anderson innovációs szemléletét, amely szerint „nem kell mást tenni, mint kitárni a kapukat, és teret adni az embereknek”.[59]

---

[57] Nemzeti Laboratóriumok bemutatása (2021) i. m.

[58] *A Biztonságos Digitális Társadalom Innovációs Klaszter alakuló ülése.* [online], 2021. 07. 27. Forrás: idomsoft.hu [2021. 07. 12.]

[59] Anderson (2017) i. m.

Összegzés

Összességében jól látható, hogy a globális infokommunikációs környezet innovációs folyamatai a nemzetbiztonsági ágazat technikai fejlődésének különböző útjait is jelentősen befolyásolják. A nemzetbiztonsági szervezeteknek – a hagyományos technológiákhoz sorolható információgyűjtési képességeik megtartása mellett – illeszkedniük kell a kor kihívásaihoz, követniük kell a nemzetközi technológiai cégek által diktált gyorsuló ütemet, és folyamatosan figyelemmel kísérni a nemzet biztonságát szolgáló új típusú biztonsági technológiákat. Mindez értelemszerűen nem kötődik csupán egyetlen technológiához, hanem a környezet komplex folyamatainak és irányainak nyomon követését és az ágazati innovációk kiemelt jelentőségének felismerését igényli.

Egyetértve a szakértők széles körével: a mesterséges intelligencia megoldásai és az 5G hálózati technológia, geopolitikai és gazdasági fölényt biztosítva, alapvetően módosíthatják a globális erőviszonyokat a következő évtizedekben az infokommunikáció terén.[60] Mindez érinteni fogja a technológiai versenyben élre kerülő nagyhatalmak gazdasági ágazatait, a katonai eszközrendszereik modernizációját és nemzetbiztonsági vonatkozásban azon megoldások fejlődését is, amelyek hatással vannak a társadalom biztonságára. Ennek mentén válik jelentőssé a technológiák nemzeti szintű rendelkezésre állása, a tanulmányban tárgyalt kutatás-fejlesztés kiemelt szerepe, az innováció és az idegen kézben lévő technológiák nemzetbiztonsági szemléletű megközelítése.

A hazai nemzetbiztonsági ágazat a Nemzeti Biztonsági Stratégiával[61] összhangban figyelmet szentel a kor információtechnológiai kihívásainak, amelyek nem pusztán az információk megszerzésének irányait jelentik, hanem felölelik a digitális eszközökre épülő társadalom működését veszélyeztető tényezők elleni védekezést, valamint a kutatás-fejlesztés kiemelt szerepét is. Mint a Stratégiában is megfogalmazódik, „[h]azánk biztonsága megkívánja, hogy a kulcsfontosságú területeken – mint például a kibervédelem, a mesterséges intelligencia, az autonóm rendszerek, a biotechnológia – kiemelt figyelmet fordítsunk a kutatás-fejlesztésre és annak védelmi összetevőjére".[62]

A globalizált információs társadalom valamennyi szereplőjének (legyen az akár állami, akár piaci) meg kell küzdeni azzal az általános jelenséggel, hogy sem a közigazgatás, sem a gazdálkodó szervezetek normál működésének fenntartásához már régen nem elegendő az üzletmenet folytonosságához és az üzembiztonság fenntartásához szükséges beruházások megtétele. A sikeres létükhöz és fejlődésükhöz aktív szerepet kell vállalniuk az innovációs ökoszisztémában, kihasználva az ebből adódó lehetőségeket és vállalva az ezzel járó kötelezettségeket. Egyértelmű célkitűzése a magyar államnak, hogy a társadalom egyes szereplői elérjék innovációs tevékenységükben a kritikus tömeg mennyiségi mutatóit is, a teljes társadalom innovációs tevékenysége átlendüljön a holtponton és Magyarország bekerüljön a vezető innovációs államok sorába. A nemzetbiztonsági szolgálatoknak feladatrendszerükből és a velük kapcsolatos elvárásokból adódóan élen járónak kell lenni ebben az innovációs tevékenységben.

---

[60] Fricke (2020) i. m. 18.

[61] A 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. i. m.

[62] A 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. i. m. 106. pont.

Felhasznált irodalom

5G – Fifth generation of mobile technologies. [online], 2019. 12. Forrás: ITU [2021. 06. 08.]
A Biztonságos Digitális Társadalom Innovációs Klaszter alakuló ülése. [online], 2021. 07. 27. Forrás: idomsoft.hu [2021. 07. 12.]
Agar, Jon: The central debates on science and innovation. In *Science Policy under Thatcher.* London, UCL Press. 2019. Online: https://doi.org/10.2307/j.ctv8xnfk4
Anderson, Chris: *Az innovációról.* [online], 2017. Forrás: citatum.hu [2021. 07. 04.]
Ang, Carman: *Ranked. The 50 Most Innovative Companies.* [online], 2020. 07. 17. Forrás: visualcapitalist.com [2021. 05. 12.]
Artificial Intelligence – A strategy for European startups. [online], 2018. Forrás: rolandberger.com [2021. 05. 12.]
Auer Ádám: Gondolatok a mesterséges intelligencia egyes polgári jogi kérdéseiről. *Scientia et Securitas,* 2. (2021), 1. Online: https://doi.org/10.1556/112.2021.00010
Bács Zoltán György: Innováció és nemzetbiztonság a 21. században. In Ruzsonyi Péter (szerk.): *Közbiztonság. Fenntartható biztonság és társadalmi környezet tanulmányok III.* Budapest, Ludovika Egyetemi Kiadó, 2020.
Bencze Áron: *Aktivizálták az innovációs ökoszisztéma szereplőit.* [online], 2021. 08. 02. Forrás: innoteka.hu [2021. 08. 20.]
Borowitz, Mariel: An Interoperable Information Umbrella. Sharing Space Information Technology. *Strategic Studies Quarterly,* 15. (2021), 1. 116–132.
Cordesman, Anthony H. – Grace Hwang: *U.S. Competition with China and Russia. The Crisis-Driven Need to Change U.S. Strategy*. Center for Strategic & International Studies, 2020.
Dobák Imre: Társadalom – technológiai környezet – nemzetbiztonság. In Ruzsonyi Péter (szerk.): *Közbiztonság. Fenntartható biztonság és társadalmi környezet tanulmányok III.* Budapest, Ludovika Egyetemi Kiadó, 2020. 959–971.
EIS 2021. Executive summary. [online], 2021. 07. 22. Forrás: ec.europa.eu [2021. 08. 12.]
Engelke, Peter: *AI, Society, and Governance. An Introduction.* [online], 2020. 03. 01. Forrás: jstor.org [2021. 05. 12.]
European and Regional Innovation Scoreboards 2021 – Questions and Answers. [online], 2021. 06. 21. Forrás: ec.europa.eu [2021. 08. 12.]
European innovation scoreboard 2021. [online], 2021. 06. 28. Forrás: ec.europa.eu [2021. 09. 02.]
Facts and Figures 2020. Measuring digital development. [online], 2020. Forrás: www.itu.int [2021. 05. 12.]
Fricke, Benjamin: *Artificial Intelligence, 5G and the Future Balance of Power.* [online], 2020. 01. 01. Forrás: jstor.org [2021. 09. 12.]
Global 500 2021. Brand Finance. The annual report on the most valuable and strongest global brands. [online], 2021. 01. Forrás: brandirectory.com [2021. 05. 12.]
Gouardères, Frédéric – Albane Keravec: *Innovációs politika.* [online], 2021. 06. Forrás: europarl.europa.eu [2021. 08. 06.]
ITU Statistics. Key ICT indicators for developed and developing countries, the world and special regions (totals and penetration rates) table. [online], 2021. Forrás: www.itu.int [2021. 05. 12.]
Kemp, Simon: *Digital 2021. Global Overview Report – DataReportal – Global Digital Insights.* [online], 2021. 01. 27. Forrás: datareportal.com [2021. 05. 12.]
Kemp, Simon: *Social Insights.* [online], 2020. 12. Forrás: datareportal.com [2021. 05. 12.]
Kool, Dorith – Tim Sweijs: A Security Sector Assessment Framework. In Dorith Kool et al.: *The Good, the Bad, and the Ugly. A Framework to Assess Security Sectors' Potential Contribution to Stability.* Hague, Centre for Strategic Studies, 2020. 22–37.
Krasznay Csaba: Kiberbiztonsági kompetencia hálózatok Európában – K+I+F lehetőségek a következő évtizedben. *Scientia et Securitas,* 1. (2020), 1. 43–48. Online: https://doi.org/10.1556/112.2020.00007
Mansell, Robin: Adjusting to the digital. Societal outcomes and consequences. *Research Policy,* 50. (2021), 9. 1–10. Online: https://doi.org/10.1016/j.respol.2021.104296
Nemzeti Laboratóriumok bemutatása. [online], 2021. 01. 07. Forrás: nkfih.gov.hu [2021. 07. 15.]
Nemzeti Laboratóriumok Program. [online], 2021. 01. 05. Forrás: nkfih.gov.hu [2021. 05. 12.]

Oslo Manual 2018. Guidelines for Collecting, Reporting and Using Data on Innovation. [online], 2018. Forrás: oecd-ilibrary.org [2021. 07. 16.] Online: https://doi.org/10.1787/9789264304604-en

Palkovics László szakmai irányítása alá kerülnek a védelmi iparhoz kapcsolódó állami cégek. [online], 2021. 06. 04. Forrás: portfolio.hu [2021. 08. 03.]

Petkovich Tamás: A hadiipar fejlesztési lehetőségei Magyarországon. *Katonai Logisztika,* 24. (2016), 1. 54–87.

Riley, Tonya: *Apple's new solution to combat child abuse imagery could radically shift encryption debate.* [online], 2021. 08. 06. Forrás: cyberscoop.com [2021. 09. 12.]

Simón, Luis – Linde Desmaele – Jordan Becker: Europe as a Secondary Theater? Competition with China and the Future of America's European Strategy. *Strategic Studies Quarterly,* 15. (2021), 1. 90–115.

Tématerületi Kiválósági Program 2021. [online], 2021. 05. Forrás: nkfih.gov.hu [2021. 05. 12.]

The World in 2010. [online], 2010. 10. 20. Forrás: www.itu.int [2021. 05. 12.]

Umbach, Frank: *EU Policies on Huawei and 5G Wireless Networks Economic Technological Opportunities vs. Cybercecurity Risks.* [online], 2020. Forrás: jstor.org [2021. 05. 12.]

Webster, Graham – Rogier Creemers – Paul Triolo – Elsa Kania: *Full Translation. China's ‚New Generation Artificial Intelligence Development Plan'.* [online], 2017. 08. 01. Forrás: newamerica.org [2021. 06. 07.]

Jogi források

A Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal 2021. évi költségvetésének szöveges indokolása. [online], 2020. Forrás: parlament. hu [2021. 06. 07.]

Javaslat az Európai Bizottság és Tanács Rendeletének megalkotására a Horizont Európa kutatási és innovációs keretprogramról, valamint részvételi és terjesztési szabályainak megállapításáról. [online], 2018. 06. 07. Forrás: europarl.europa.eu [2021. 08. 06.]

Az Európai Parlament és a Tanács Rendelete a Horizont Európa kutatási és innovációs keretprogram létrehozásáról, valamint részvételi és terjesztési szabályainak megállapításáról. [online], 2018. 06. 07. Forrás: eur-lex.europa.eu [2021. 08. 06.]

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. [online], 2020. 04. 21. Forrás: net.jogtar.hu [2021.08. 16.]

1573/2020. (IX. 9.) Korm. határozat Magyarország Mesterséges Intelligencia Stratégiájáról, valamint a végrehajtásához szükséges egyes intézkedésekről. *Magyar Közlöny,* (2020), 202. 6356.