

Koller Marco¹

Szuverenitásvédelem és digitális szuverenitás

A komplex biztonsági kihívások láncolata

Sovereignty Protection and Digital Sovereignty

The Chain of Complex Security Challenges

Absztrakt

Egy adott állam minden nemű függetlenségének, befolyástól mentes működésének szavatolása alapvető állampolgári és társadalmi érdek. A szuverenitásvédelem komplex tevékenység, amely átfogja az egész államigazgatást, de kiemelt szerepe van benne a rendvédelemnek, illetve a nemzetbiztonsági szolgálatoknak. Azonban a változó világot a változó és komplex biztonsági kihívások jellemzik, amelyek lehetnek akár környezeti, humán vagy technológiai eredetűek, ezért fontos a proaktív szemléletmód, valamint a hazai és nemzetközi együttműködések hangsúlyozása. A digitalizálódó világban a kibertér egyre inkább meghatározó jelentőségű lesz, így a digitális szuverenitás elérése, annak védelmezése is hangsúlyos.

Kulcsszavak: szuverenitás, digitalizáció, biztonság, kockázatok, lehetőségek, digitális szuverenitás

Abstract

Ensuring a state's independence from external interference is a core interest of society at large. The entire state apparatus is involved in the complicated task of defending sovereignty, but the police and national security agencies are particularly important in

¹ Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: marcoakoller@gmail.com

this regard. But whether it's environmental, human, or technological, the changing globe brings with it ever-changing and complicated security concerns. For this reason, it's critical to be proactive and to prioritize both domestic and international collaboration. Achieving and defending digital sovereignty is crucial since cyberspace will grow in importance in a world that is becoming more digitally integrated.

Keywords: sovereignty, digitalisation, security, risks, opportunities, digital sovereignty

Bevezetés

A jelenkor jellemzője a dinamikusan változó biztonsági környezet, amely számos új feladatot indukál az állami szervek számára, többek között a biztonság – különböző aspektusú – fenntartásával foglalkozó intézmények számára is, mint a rendőrség vagy a nemzetbiztonsági szolgálatok. A változó világhoz kapcsolódó kihívások és kockázatok fokozódásáról számos szakirodalom, illetve hazai és nemzetközi joganyag (például a *Nemzeti Biztonsági Stratégia* és az *Alaptörvény* stb.) is megemlékezik, azonban kevesebb figyelmet kap az, hogy a biztonsági kihívások komplexek, azaz nem lehet őket önmagukban – hatékonyan és szakszerűen – értelmezni. Egy-egy jelenség összefonódik a másikkal, az egyik a másikból következik, illetve egymást generálja, fokozza. Így a biztonsági kihívások komplex láncolatáról beszélhetünk, amely mind a világ, mind Európa és hazánk biztonsági környezetét befolyásolja.

„Magyarország szuverenitását egyre gyakrabban éri jogellenes támadás. Évek óta tetten érhető – és sok esetben a nyilvánosság számára is ismert – befolyásszerzési kísérletek történnek, melyek során külföldi szervezetek és személyek a saját érdekeiket igyekeznek érvényesíteni hazánkban, szemben a magyar érdekekkel és szabályokkal.”² A fentiek tükrében egyre fontosabbá vált az ország függetlenségének, biztonságának szavatolása, azaz a szuverenitásvédelem. Többek között ezért jött létre a Szuverenitásvédelmi Hivatal a 2023. évi LXXXVII. törvény által.

A kutatás célja és az alkalmazott módszerek

Európa és hazánk szuverenitása több dimenzióban is érintett, annak védelmét több aspektusból szükséges vizsgálni. Jelen tanulmány célja, hogy bemutassa azokat a biztonsági kihívásokat, amelyek hazánk biztonságát, szuverenitását veszélyeztetik a változó világ, illetve az európai biztonsági környezet tükrében, különös figyelmet fordítva arra, hogy az egyes, biztonságot érintő elemek milyen láncolatban, összefüggésben figyelhetők meg, továbbá a digitális szuverenitás tükrében, mint a jelenkor egyik aktuális problematikája. A feltárt kihívások és kockázatok nem teljes körűek, azok az aktuális trendek, illetve egyedi nézőpontok alapján változhatnak, azonban a kiemelt kategóriaelemek álláspontom szerint rendkívül jól összefoglalják a főbb problémaköröket.

² 2023. évi LXXXVII. törvény a nemzeti szuverenitás védelméről, preambulum.

A fentiekén túlmenően a feltárt kihívások és kockázatok bemutatása, illetve elemzése után a tanulmány ajánlásokat tesz, amelyek esetleges végrehajtása Magyarország nemzetbiztonságát, illetőleg szuverenitásának védelmét segítené elő.

A tanulmány elkészítése során a főbb vonatkozó hazai joganyagokat hívtam segítségül: a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényt (a továbbiakban: Nbtv.) és a Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Korm. határozatot (a továbbiakban: NBS). Ezek alapján határoztam meg a főbb kockázati kategóriákat, amelyeket aztán PESTEL-analízis alapján rendszereztem, elemeztem, és megfogalmaztam a vonatkozó ajánlásokat. A PESTEL-analízis egy stratégiai tervezési eszköz, amelyet alapvetően az üzleti szférában alkalmaznak; a PEST-analízis kibővített verziója.

„A PEST elemzés során a vállalkozásra ható hosszabb távú környezeti tendenciákat vesszük számba és strukturáljuk, ezáltal megragadhatóvá, kiemelhetővé válnak azok a fontosabb tényezők, amelyek befolyásolhatják a stratégiai döntéseket. Cél megtalálni a jelen és jövő fontos környezeti tényezőit, amelyek a vállalkozás szempontjából meghatározóak. A PEST elemzés négy dimenzió mentén vizsgálja a környezetet.”³

Jelen tanulmány során implementáltam eszközeit, így lehetővé vált, hogy megértsük a külső tényezőket, amelyek hatással vannak egy adott nemzet biztonságára, stabilitására és fejlődési lehetőségeire. Az elemzés politikai, gazdasági, társadalmi és technológiai (PEST), valamint környezeti és jogi (EL) tényezők vizsgálatát foglalja magában. Az elemzés segít megérteni a külső környezet hatásait a nemzeti biztonságra, a gazdasági stabilitásra és a társadalmi folyamatokra, továbbá lehetővé teszi a jövőbeni biztonsági és politikai trendek azonosítását, amelyek befolyásolhatják az ország stabilitását.

Fogalmi háttér

A téma komplexitása okán a megfelelő értelmezéséhez szükséges a felmerülő fogalmi keret meghatározása, a fontosabb kifejezések definiálása az alábbiak szerint.

Biztonság

A biztonság mint fogalom és jelenség rendkívül összetett, számos aspektussal rendelkezik (például nemzetbiztonság, nemzeti biztonság, gazdaságbiztonság, energiabiztonság, egészségügyi biztonság stb.). A legegyszerűbben úgy lehet meghatározni a biztonságot, mint egy veszély nélküli stabil állapotot, amelynek fenntartása mind állami, mind egyéni szinten kiemelt jelentőségű, hiszen maga a biztonság Abraham Maslow amerikai pszichológus szükségletpiramisán a második legfőbb szükségleti kategóriaként jelenik meg, amely magában foglalja a fizikai védeltséget és a kiszámíthatóságot.⁴

³ RABI 2009.

⁴ MEZŐ 2007: 121–125.

Nemzeti biztonság és nemzetbiztonság

A nemzeti biztonság egy sokrétű *össztársadalmi teljesítmény*,⁵ mindent magában foglal, ami kockázatként, kihívásként, illetve valamilyen fenyegetésként jelenik meg az adott állam irányában (például természeti katasztrófák, demográfiai, egészségügyi kihívások, kockázatok stb.). Nemzetbiztonság alatt szűk értelemben a titkosszolgálati tevékenységet értjük, az úgynevezett *intelligence* tevékenységi kört. A fent említett különböző kihívások és kockázatok, fenyegetések jellegéből, sokaságából és igen nagy fokú különbözőségéből fakadóan a nemzet biztonságát nem tudja lefedni a titkosszolgálati tevékenységet végző szervek munkája, hanem más rendészeti és egyéb szervek összehangolt közös feladatvégzése is szükségeltetik a problémák kezeléséhez.

Szuverenitás

A szuverenitás az állam önállóságát jelenti, azaz az állam a saját jogrendjét maga alkotja és tartja fenn kizárólagos területi főhatalommal a területén lévő személyek és dolgok felett. A szuverén állam más államokkal való kapcsolatában szabadon, függetlenül dönt, területi épsége és politikai függetlensége sérthetetlen, és joga van ahhoz, hogy szabadon válassza meg és alakítsa politikai, társadalmi és kulturális rendszerét.⁶

Digitális szuverenitás

Az Európai Unió legnagyobb kihívása a digitális szuverenitás elérése, így hazánké is.⁷ Digitális szuverenitás alatt a Gartner definíciója szerint a kormány azon képességét értjük, „hogy a politikát a külföldi kormányok digitális szabályozása által közvetlenül az állampolgáira és a székhelye szerinti vállalkozásokra rótt akadályok nélkül valósítsa meg, beleértve a szabályozási ellenőrzés alatt álló digitális óriáscégek által gyakorolt szabályozást is.”⁸ Philip von Brockdorff véleménye szerint, amelyet az Európai Gazdasági és Szociális Bizottság (a továbbiakban: EGSZB) egyik állásfoglalásában ismertetett, a digitális szuverenitást talán úgy lehet körülírni, mint a kormányok és a vállalkozások autonómiáját saját adataik, hardvereik és szoftvereik kezelése és létrehozása tekintetében.⁹ A fenti fogalmak a szuverenitást az állam szempontjából közelítik meg, azonban ezt kisebb egységre lebontva is lehet vizsgálni. Személyek digitális szuverenitása alatt azt értjük, hogy az egyén saját ellenőrzése alatt tudja tartani, ki férhet hozzá és milyen céllal használhatja a személyéhez kötődő digitális információt.¹⁰ Jól látható, hogy az egyik fő tartalmi elem az adatok és az azokat kezelő rendszerek feletti tényleges, kiszolgáltatottság nélküli felügyelet. Az EGSZB-vélemény szerint

⁵ MEZŐ 2007: 121–125.

⁶ TÁLAS [é. n.].

⁷ TÓTH 2021: 31.

⁸ A digitális szuverenitás jelentősége 2023.

⁹ VON BROCKDORFF 2022: 2.1 pont.

¹⁰ PATÓ 2021.

az EU nagymértékben támaszkodik EU-n kívül működő nagy technológiai vállalatokra, és az EU-nak csökkentenie kell a nem uniós technológiai óriásoktól való függőségét annak ellenére, hogy jelentős előrelépést tett digitális szuverenitásának javítása terén. A vélemény kiemeli, hogy támogatni kell a technológiai fejlődést célzó kutatásokat, hogy az EU lépést tudjon tartani Kínával és az USA-val.¹¹ Európa legfőbb kihívása a technológiai függés csökkentése a két említett nagyhatalomtól.¹²

A magyar nemzetbiztonsági érdekek érvényesítését veszélyeztető aktuális kihívások és esetleges lehetőségek

A fejezetben a hazai szuverenitásvédelmet érintő aktuális kihívásokat mutatom be és kategorizálom. A főbb faktorokat az NBS-ben meghatározott kockázatok alapján állapítottam meg, illetve a PESTEL-elemzés szerint csoportosítottam őket.

Politikai tényezők

A PESTEL-analízisben vállalatokra vonatkozóan a politikai (*political*) tényezők között szerepelnek a törvényi előírások, az adópolitikai és a kormányzati stabilitás. Ezek érinthetnek egy vállalkozást, ugyanis egy váratlan adóemelés csökkentheti egy adott cég profitját.¹³

Az NBS 10. pontja deklarálja többek között a politikai stabilitást és függetlenséget, illetve a demokratikus jogrendet. Ezen alapvető érdekek védelme mentén meg lehet határozni azokat a kockázati faktorokat, amelyek Magyarország szuverenitását és biztonságát befolyásolják.

Az NBS-ben deklarált kockázatok közül kiemelendő jelen elemzés szempontjából a 68. pont: „Az állami és nem állami szereplők által szponzorált politikai, gazdasági és társadalmi folyamatok befolyásolására irányuló stratégiák száma, változatossága és határfoka növekszik.”

Jelen fogalom egyértelműen a hadtudományban jól ismert kifejezésre, az információs műveletekre utal. Az információs műveletek az információért folyó küzdelem, olyan összehangolt tevékenységek, „amelyek a műveletek célkitűzéseinek elérése érdekében, kognitív képességekkel közvetlenül, illetve technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire”.¹⁴ Az információs műveletek egyik típusa a kognitív információs műveletek, amelyek a humánusra fókuszálnak, az emberek és a társadalmi csoportok attitűdjét próbálják befolyásolni.¹⁵

¹¹ VON BROCKDORFF 2022.

¹² TÓTH 2021: 31.

¹³ KOMÁROMI 2025.

¹⁴ HAIG 2018: 15.

¹⁵ HAIG 2018: 218.

Amennyiben a politikai destabilizáció a cél, akkor jelen részhez lehet még sorolni az egyes kritikus infrastruktúrák elleni támadásokat¹⁶ vagy a terrorizmus jelenségét¹⁷ is, mivel utóbbi „politikai, vallási vagy ideológiai célkitűzések elérése érdekében kormányok és társadalmak kényszerítésére vagy megfélemlítésére tett kísérletet, egyének vagy javak elleni erő vagy erőszak törvénytelen alkalmazása, illetve azzal való fenyegetés által”.¹⁸

Gazdasági tényezők

A gazdasági tényezők a PESTEL-elemzés folyamatában alapvetően olyan változókat jelentenek, mint az infláció vagy a kamatlábak.¹⁹ Jelen esetben az NBS-ben nevesített gazdasági vonatkozású kockázatokat összegezzük (például infláció és a munkaerővel kapcsolatos kihívások).

A történelmi előzmények is jól prezentálják, hogy a különböző gazdasági nehézségek a társadalmi konfliktusok kiéleződéséhez, illetve a radikális eszmék terjedéséhez vezetnek. A fentiek mellett kiemelendő a munkaerőhiány és a munkanélküliség, az előzőkből következő vagy azok mellett lévő társadalmi jelenségek, amelyek a gazdasági növekedést hátráltathatják.²⁰ Ezen tényezők kormányzati, állami szinten kezelendő kihívások, amelyekkel az NBS is kiemelten foglalkozik.²¹ Nemzetbiztonsági szempontból fontos kiemelni a célzott gazdaságellenes állami és nem állami lépések felderítését és elhárítást, azonban a hírszerzés részéről megjegyzendő a hazai gazdaság erősítéséhez vezető információgyűjtő tevékenység is.

Társadalmi tényezők

A PESTEL-elemzés alapján – kifejezetten a vállalkozásokra vonatkozóan – a társadalmi tényezők magukban foglalják a demográfiai tényezőket, illetve az adott társadalom vallását, kultúráját is.²² Egy állam biztonsági szempontjából a társadalmi tényezők, az azokra ható kockázati faktorok kiemeltnek számítanak, az NBS is számos kockázatot tartalmaz erre vonatkozóan, amit a következő alfejezetekben fejtek ki részletesen. Megjegyzem, hogy habár az elemzés során az egyes faktorok elkülönülnek, ezek komplexitása, egymásra hatása miatt nehezen szeparálhatók el a valóságban.

¹⁶ NBS 124. d) pont.

¹⁷ NBS 124. m) pont.

¹⁸ DOBÁK 2011: 83.

¹⁹ KOMÁROMI 2025.

²⁰ SZÜCS 2017.

²¹ NBS 124. h) pont.

²² KOMÁROMI 2025.

Migráció és demográfia

A migráció egy alapvetően komplex kockázati faktor, tekintettel arra, hogy nem maga a jelenség, hanem a rá épülő bűncselekmények, tevékenységek vagy a következmények és a bekövetkező események azok, amelyek az igazi kockázatokat jelentik. A migrációra épülő tevékenységek lehetnek például a szervezett bűnözés, az okmányhamisítás, az embercsempészet. A migrációval összefüggő következmények is sokrétűek lehetnek, mint például az etnikulturális konfliktusok kiéleződése és a demográfiai eltolódás.²³ Tekintettel arra, hogy hazánk egyelőre tranzitország (a migránsok csak áthaladnak az országon, nem céljuk itt letelepedni), egyes bevándorlással érintett biztonsági faktorok csak áttételesen érintik, azonban nem lehet tudni – az elmúlt évek nemzetközi párbeszédeire alapozva –, mikor vezetnek be egy elosztási mechanizmust az Európai Unióban.²⁴ A szuverenitás fogalmából is következik, hogy az állam kizárólagos főhatalommal bír az általa irányított terület és az ott lakó népesség felett, továbbá maga választja meg kulturális és politikai rendszerét, amely külső befolyástól mentes. Ennek érdekében szükséges az ilyen irányú – nyílt vagy leplezett – törekvések felderítése és elhárítása, amely mind politikai, mind nemzetbiztonsági szinten kiemelt.

Amikor a migráció szóba kerül, sokan elfelejtik, hogy ez egy kétarcú jelenség: amennyiben van bevándorlás, akkor szükségszerűen van kivándorlás is. Magyarország szempontjából is kihívást jelentő probléma a tartósan külföldre távozó, főleg fiatal munkaerő, mivel ez negatívan érinti az adóbevételeket, illetve a nyugdíjrendszert is, hiszen a demográfiai csökkenés mellett a meglévő kivándorlás miatt egyre kevesebb adófizető termeli ki a növekvő nyugdíjállományt, ami hosszú távon akár a nyugdíjrendszer összeomlásához is vezethet. Jelen kategóriába kell még sorolni az úgynevezett „agyelszívás” jelenségét is, amely a magasan képzett munkaerő elvándorlását jelenti (ideértendők az orvosok, a mérnökök stb.).²⁵ Az NBS is kiemelt kockázati kategóriába sorolja a tartós népességfogyást és a lakosság átlagéletkorának folyamatos emelkedése miatt kritikus demográfiai helyzet kialakulását.²⁶ A kivándorlás és a népességcsökkenés a gazdaságra is negatív hatással van, hiszen a szakképzett vagy a magasan kvalifikált munkaerő (kiváltképpen a fejlődő iparágak, mint az IT területén) hozzájárul hazánk gazdasági növekedéséhez és stabilitásához. A politikai döntéshozatal megalapozottságához a titkosszolgálatok hozzá tudnak tenni, hiszen olyan szűk körben ismert információkat is képesek megszerezni, amelyek előmozdíthatják a hazai gazdaságot, és ez akár munkahelyet is teremthet.

²³ Póczik Szilveszter szerint ezek a kategóriák: demográfiai; egészségügyi; embercsempész-hálózatok; emberkereskedelem; etnikai bűnözés; etnikulturális különbségek; gazdasági kihívások; globális kényszermigráció; konfliktusok migrációja; korrupció; közbiztonsági kihívások; legalizációs cselekmények; okmánybiztonság, hamis okiratok; ötödik hadoszlop jelenség; politikai feszültségek, kihívások; szervezett bűnözés; szociális kihívások; terrorizmus; tiltott határátlépés; védelmi képesség gyengülése; vízumhoz kötődő visszaélések; xenofóbia, rasszista indítékú bűncselekmények. PÓCZIK 2008: 18–74.

²⁴ FARKASA 2021.

²⁵ CSANÁDY et al. 2008.

²⁶ NBS 124. g) pont.

Radikalizáció

Megfigyelhető jelenség a különböző radikális eszmék terjedése, mint a radikális iszlám, szélsőjobboldali nézetek, vagy éppen a szélsőbaloldali antifasiszta, radikális környezet- vagy állatvédelmi attitűd térhódítása. Ezek egymást gerjesztő folyamatok,²⁷ amit további faktorok erősítenek, mint a migráció jelensége vagy a gazdasági visszaesés. A társadalom radikalizációja nem csupán közbiztonsági kihívások elé állítja az adott államot, hanem szélsőséges esetben az ilyen csoportok akár az alkotmányos rend erőszakos megváltoztatása érdekében is felléphetnek, vagy a kritikus és/vagy állami infrastruktúra működését is megzavarhatják, amelynek felderítése és elhárítása nemzetbiztonsági feladat.²⁸ Továbbá az ilyen csoportok kapcsán felmerülhet a terrorista cselekmények elkövetése is, amely az NBS 124. e) pontja alapján kiemelt kockázatnak minősül.

A radikális csoportok kapcsán fontos megjegyezni, hogy a globalizációval és a digitalizációval azok is nemzetköziesedtek, így kiemelt jelentőségű a nemzetbiztonsági szolgálatok és a rendvédelmi szervek közötti hazai és nemzetközi kooperáció, illetve a radikális csoportok térnyerésének, szerveződésének online térben történő monitorozása, esetlegesen elhárítása különböző eszközökkel. Fontos továbbá kiemelni jelen alfejezetnél, hogy ezen csoportok külföldi állami és nem állami szervezetek általi erősítése még nagyobb kihívást jelent, és a hibrid (nem hagyományos) hadviselés eszköze lehet. Ezen csoportok felhasználása ilyen célból nem csupán társadalmi tényező, hanem a politikai tényezők közé is besorolható lehet.

Technológiai tényezők

A PESTEL-elemzés idesorolja, hogy milyen technológiák állnak rendelkezésre, és hogyan használhatók fel ezek egy vállalkozásban. A technológia fejlődése gyors ütemben zajlik, és fontos vele lépést tartani.²⁹ A technológiai tényezők egy állam szempontjából nem csupán kockázatot, hanem rendkívüli lehetőségeket is jelentenek, amelyeknek az esetleges alkalmazására külön fejezetben térek ki.

Jelen rész kapcsán hangsúlyozandó az NBS 124. k) pontja, amely kiemelt kockázatként nevesíti „a forradalmi technológiai fejlesztések illetéktelen kezekbe kerülésével a nemzet biztonságát veszélyeztető támadásokat vagy terrorcselekmények megjelenését”. Az alábbiakban olyan forradalmi technológiákat ismertetek röviden, amelyek ellenérdekelte kézbe jutva komoly károkat tudnak okozni, és hátrányosan érinthetik hazánk szuverenitását.

²⁷ MURÁNYI 2021.

²⁸ Nbtv. 5 § b) pont.

²⁹ KOMÁROMI 2025.

Fokozódó digitalizáció

Manapság szinte minden információ átkerül a digitális térbe, az ez irányú fejlesztések egyre inkább észrevehetőek a mindennapokban is. A fentiekhez kapcsolódóan kiemelendő az e-kormányzás, illetve e-közigazgatás is, amely az állami feladatok és szolgáltatások digitális térbe történő áthelyezését jelenti, de a számos lehetőség mellett kockázatot is hordoz magában. A fentiekhez kapcsolódóan az NBS is kiemelt kockázatként nevesíti a „jelentős károkat okozó kibertámadásokat a kormányzati informatikai rendszerek, az E-közigazgatás, a közműszolgáltatók, a stratégiai vállalatok, a létfontosságú infrastruktúra egyéb elemei és más, a társadalom működésében fontos szervezetek számítógépes hálózatai ellen”.³⁰ Ez a jövőben is várhatóan fennálló, sőt növekvő problémakör, amely a biztonsággal foglalkozó intézmények technikai és humán felkészültségét is előíranyozza.

Big data és mesterséges intelligencia

Big data alatt – ahogy a neve is sugallja – nagy mennyiségű adathalmazt, illetve *big data* elemzés alatt a nagy mennyiségű adat tárolását, feldolgozását, tisztítását és elemzését értjük.³¹ Számos iparág alkalmazza, mivel olyan végtermék tud létrejönni egy jól elemzett adathalmazból, amely a nagyvállalatok, sőt az államok számára is igencsak értékes. A módszertanhoz kapcsolódó egyik legismertebb eset a Cambridge Analytica botrány, amikor a 2016-os amerikai elnökválasztás kapcsán felmerült, hogy a cég illetéktelenül hozzáfért 87 millió Facebook-felhasználó adataihoz, amelyeknek az elemzése és egy célzott stratégia által került hatalomra Donald Trump.

A mesterséges intelligencia (a továbbiakban: MI) alatt egy olyan speciális szoftvert értünk, amely az emberi értelemhez hasonlóan képes tanulni, fejlődni, feladatokat megoldani.³² Az MI szorosan kapcsolódik a *big data* elemzéshez, mivel egyrészt egy jól működő MI-hez szükséges a nagy mennyiségű adat betáplálása, másrészt egy ilyen szoftver felgyorsítja az adatok feldolgozását, rendszerezését és elemzését.³³ Az MI-re az egyik legismertebb aktuális példa a ChatGPT, egy olyan *chatbot*, amely képes bonyolult feladatok megoldására, kérdések megválaszolására, és alkalmas lehet a hagyományos keresőmotorok forradalmasítására (például Google, Bing, Yandex stb.).³⁴

A fentiekben nevesített technológiák azt is lehetővé tehetik, hogy külső felek befolyásolják akár a választásokat, vagy egyszerűen a közvéleményt olyan irányba tereljék, amely a radikális eszmék térnyerését segítené elő. Habár a módszertanok alkalmasak arra, hogy a bűnmegelőzési, bűnfelderítési, illetve nemzetbiztonsági tevékenységet segítsék, nem szabad elfelejtenünk az ellenérdekelt alkalmazás lehetőségéről sem.

³⁰ NBS 124. d) pont.

³¹ Microsoft [é. n. b].

³² Microsoft [é. n. a].

³³ Microsoft [é. n. b].

³⁴ RÁDI 2023.

Kvantumszámítógépek

A kvantumszámítógépek kifejlesztése kapcsán hatalmas verseny folyik a világ fejlett államai között, figyelemmel arra, hogy ez a forradalmi technológia lehetővé teszi, hogy az eddig alkalmazott védelmi technológiák hatástalanok legyenek.³⁵ A kvantumszámítógépek kifejlesztése és megszerzése minden állam érdeke, illetve az is, hogy olyan új védelmi technológiákat hozzanak létre, amelyek alkalmasak a kvantumszámítógépek által használt algoritmusok, kártékony kódok kivédésére. Így a fejlesztéssel kapcsolatos információk rendkívül szenzitívek, azok védelme, illetve megszerzése mindenképpen nemzetbiztonsági érdek, az ország szuverenitásának védelme szempontjából kiemelt jelentőségű.

Természeti tényezők

A PESTEL-elemzésben a környezeti tényezők magukban foglalják azt, hogy milyen környezeti problémák vannak. Példaképpen említhető az éghajlatváltozás vagy a természeti erőforrások hiánya.³⁶ A tanulmány szempontjából is kiemelt témakörnek tekinthetők a természeti tényezők, mivel sokszor olyan jellegű kockázatokat rejtenek magukban, amelyeket nehezen lehet előre látni, elhárításuk pedig összetársadalmi, sőt többnemzeti feladat is lehet.

Humán eredetű katasztrófák

Eklatáns magyarországi példaként³⁷ lehet felhozni jelen kategóriában a vörösi-szap-katasztrófát,³⁸ de bármely, az emberre visszavezethető, nem környezeti eredetű probléma is idesorolandó, amely szándékosan vagy mulasztás által következik be. Jelen esetben az egyik legrosszabb forgatókönyvként lehet megnevezni az atomkatasztrófákat, amilyen a csernobili eset is volt. De a közelmúltbeli történéseket is lehet említeni, amikor felmerült annak a lehetősége, hogy ha az orosz–ukrán háború miatt az ukrán oldalon található zaporizzsjai erőművet támadás éri, az nukleáris katasztrófát okoz.³⁹ A fentiekre utaló információk gyűjtése kiemelt jelentőségű, hiszen előzetes információk nélkül nem készíthető fel a lakosság egy ilyen esemény bekövetkezésére (például jódtabletták szétosztásával).⁴⁰

³⁵ NKI 2018.

³⁶ KOMÁROMI 2025.

³⁷ NBS 124. n) pont.

³⁸ SZTOJCSEV 2020.

³⁹ Magyarországon egyelőre nem kell aggódni a zaporizzsjai atomerőmű miatt, de a helyzet nem megnyugtató 2022.

⁴⁰ Kornel 2024.

Klímaváltozás, elsivatagosodás, ivóvíz- és élelmiszerhiány

Jelen kategória önmagában is rendkívül súlyos tud lenni, hiszen a klímaváltozás alapvetően akár a bolygó élhetetlenné válásához is vezethet, a kialakult elsivatagosodás az élelmiszer és az ivóvíz hiányához, azok árának megemelkedéséhez, és ebben a kevésbé tehetősebb európai réteg is érintett lehet, nem beszélve a harmadik világbeliekről, akik végső elkeseredésükben útnak indulnak a fejlettebb államok felé, ami így visszamutat a migrációs kockázatokra. Már a 2020-as NBS is kiemelt kockázatként nevesítette a fentieket, de az idő előrehaladtával ez még inkább fokozódó kihívássá fog válni.⁴¹ A nemzetbiztonság szerepe jelen kategóriában főként az új technológiák kapcsán merülhet fel, hiszen a fenti kihívásokat kezelő technológiák megszerzése, illetve a fejlesztés illetéktelen kézben történő megakadályozása már nemzetbiztonsági feladat lehet.

Energiahordozók és ritkaföldfémek hiánya

Az energiainportban bekövetkezett fennakadásból fakadó ellátási válsághelyzet egyrészt létrejöhet⁴² mesterségesen (az adott állam nem exportál valamilyen okból), vagy hosszú távon, természetes úton, hiszen a manapság használt energiahordozók a legtöbb esetben nem megújuló energiaforrások, így számuk véges. Ezért, illetve az egyes államoknál található energiaforrások nem egyenlő megoszlása miatt fontos az energiadiverzifikáció, ezek leggazdaságosabb módjainak megtalálása hírszerzési feladat is lehet. Továbbá a hazai energiaszektor kritikus infrastruktúrájának védelme mindenképpen titkosszolgálati feladat, ugyanis ellenérdekelt támadás bekövetkezhet akár a kibertérben, akár a valóságban mind állami és nem állami szereplők, mind esetlegesen radikális csoportok által.

Vírusok és betegségek

A Covid-19 okozta pandémiás helyzet óta tudjuk, hogy egy járvány milyen szintű kihívást tud okozni nemcsak egy állam, hanem az egész világ számára is. Az egészségügyi ellátórendszer túlterhelésén kívül a gazdasági kihívások is jelentősek voltak, számos iparágat rendkívül súlyosan érintettek a lezárások (például turizmus és vendéglátás stb.). A fentiekre tekintettel nem csoda, hogy a jogalkotó a kiemelt kockázatok közé sorolta „a lakosság tömeges és súlyos megbetegedésének kockázatát hordozó járványos betegség magyarországi megjelenését és gyors terjedését”.⁴³ A titkosszolgálatok ezen a téren a kormányzat munkáját támogató információk megszerzését tudják végrehajtani (például oltások és egyéb egészségügyi felszerelések beszerzéséhez kapcsolódóan), de az elhárítás szempontjából releváns az álhírterjesztések megakadályozása is.

⁴¹ NBS 124. g) pont.

⁴² NBS 124. i) pont.

⁴³ NBS 124. o) pont.

Környezeti eredetű katasztrófák

Az ipari katasztrófákhoz hasonló kategória, azonban ez nem humán, hanem környezeti eredetű. Magyarország természeti adottságaira tekintettel a hurrikán, a tengeri árvíz – amely általánosságban külföldön kiemelt kategória szokott lenni – nem kiemelt jelentőségű. Azonban már a különböző belvizek és a folyókhoz kapcsolódó árvizek, heves viharok kockázatot jelenthetnek,⁴⁴ ugyanakkor ezek kezelése alapvetően nem nemzetbiztonsági feladat, viszont az előrejelzést végző hivatalos szervek munkája befolyástól mentes működésének szavatolása már az lehet.

Jogi tényezők

Vállalati szempontból a jogi tényezők érintik a törvényeket és az előírásokat, amelyek befolyásolhatják egy adott cég működését. Ez magában foglalja például az adótörvényeket vagy a munkajogot.⁴⁵ Az NBS a jogi tényezők kapcsán is fogalmaz meg kijelentéseket biztonsági aspektusból, ezek kifejezetten a fentiekben már nevesített tényezők kapcsán felmerülő jogi szabályozatlanságokra utalnak, ilyen az NBS 159. pontja is, amely deklarálja a kibertérben jelentkező új típusú kockázatok kapcsán, hogy a technológiai és társadalmi háttér erősítésén túlmenően a kibertér jogi szabályozásának fejlesztése is célkitűzés.

Szintén a technológia (MI) kapcsán emeli ki az NBS 161. pontja, hogy koncentrálni kell a megfelelő jogi és felelősségi környezet kialakítására. Továbbá új típusú kockázatként jelent meg a nem hagyományos fizetőeszközök (kriptoalutak) nem kellő szabályozottsága is.⁴⁶

Kiemelendő, hogy a nemzetközi jogi térben kockázatok megnevezésére is sor került, amelyek befolyásolhatják hazánk biztonsági környezetét, ilyen többek között a nemzetközi jog csökkenő kikényszeríthetősége,⁴⁷ vagy hogy a nagyhatalmi törekvések a nemzetközi jogot figyelmen kívül hagyják.⁴⁸

Az ellenérdekelt (állami és nem állami) fél fentiekre ható tevékenysége

Habár jelen alfejezet inkább a politikai tényezők közé illene, a hagyományos PESTEL-elemzésen túlmutató helyet szántam neki, tekintettel, hogy az ilyen jellegű kockázati faktor a fentiekben már felsorolt tényezőkre alapul. Nemzetbiztonsági szempontból a legnagyobb relevanciával az bír, ha az egyes – előzőleg felsorolt és kifejtett – kockázatok nem véletlenszerűen, illetve önmaguktól következnek be, hanem külső befolyás által generálják őket, esetlegesen egy fennálló kihívást erősít meg egy másik fél. Ez lehet akár állami szereplő (Magyarországgal ellentétes érdekeltségű állam, állami

⁴⁴ NBS 124. p) pont.

⁴⁵ KOMÁROMI 2025.

⁴⁶ NBS 76. pont.

⁴⁷ NBS 44. pont.

⁴⁸ NBS 52. pont.

hátterű hackercsoport stb.) vagy nem állami szereplő is (nem kormányzati szervezet, terrorista csoport, nem állami hátterű bűnözői, hackercsoport stb.). Akármilyen típusú kockázat erősítése, kialakítása egy másik fél által már nemzetbiztonsági kockázat, ami az ország szuverenitásának, külső befolyástól mentes működésének biztosítását indukálja. Az ilyen irányú esetleges tevékenység felderítése és elhárítása rendkívüli jelentőségű, az NBS úgy fogalmaz, hogy kiemelt kockázat az „összehangolt és széles körű diplomáciai, információs és titkosszolgálati műveletek, pénzügyi-gazdasági nyomásgyakorlással, pénzügyi spekulációs támadásokkal vagy katonai fenyegetéssel párosulva (hibrid) Magyarország destabilizálása, kormányzati cselekvőképességének, politikai stabilitásának és társadalmi egységének gyengítése, továbbá nemzetközi érdekérvényesítő képességének korlátozása céljából”.⁴⁹

Lehetséges szuverenitásvédelmi lépések a kockázatok mérséklésének érdekében

A fentiekben felsorolt kockázatok alapvetően össztársadalmi, illetve kormányzati lépéseket indukálnak, hiszen olyan szinten összefüggő és szerteágazó problémakörökről beszélünk, amelyek hatékony kezelése nem kivitelezhető csupán a nemzetbiztonsági szolgálatok vagy a rendvédelmi szervek által. Ahogy az NBS 126. pontja is fogalmaz: „A biztonság szavatolása érdekében elsődleges cél a nemzeti intézkedések hatékonyságának és rugalmasságának, valamint a nemzeti együttműködés szilárdságának erősítése. Az azonosított kihívások megelőzése, kezelése és elhárítása elsődlegesen nemzeti felelősség, amely a Kormány feladata, együttműködésben a társadalommal.” Ugyanakkor szükséges lehet, hogy az egyes kockázatok elhárítása, megelőzése érdekében a hazai nemzeti biztonság szavatolásában részt vevő szervek (rendvédelmi szervek, honvédség, minisztérium stb.) különböző intézkedéseket, fejlesztéseket hajtsanak végre.

Magyarország szuverenitásának – beleértve a digitális szuverenitást is – védelme kapcsán kiemelendő, hogy jelen tevékenység nem kell hogy elsősorban reaktív legyen, hanem minél inkább a proaktív szemléletmód irányába kell elmozdulni. Ennek érdekében a hazai rendvédelmi szerveknek szükségszerűen emelniük kell munkájuk színvonalát, képességeiket fejleszteni kell, különös tekintettel az új típusú technológiákra. A 21. század információs kihívása nem az, mint korábban, hogy a rendelkezésre álló adatok szűkösek, hanem éppen ellenkezőleg, hatalmas mennyiségű adat keletkezik nap mint nap, azonban azok megszerzésén túlmenően rendkívüli kihívást jelent azok feldolgozása, szintetizálása, illetve hasznosítása.

A mesterséges intelligencia nem csupán kihívás lehet, hanem egyben lehetőség is, egyfajta kétélű pengeként jelentkezik. Az NBS 161. pontja is azt mondja, hogy „a mesterséges intelligencia szerepe a jelen és a jövő fejlesztései szempontjából rendkívüli jelentőségű, ezért ki kell terjeszteni alkalmazását. Koncentrálni kell azokat az infrastrukturális és humán erőforrásokat, amelyek megfelelő jogi és felelősségi környezet kialakításával lehetővé teszik a mesterséges intelligencia-alapú rendszerek

⁴⁹ NBS 124. c) pont.

fejlesztését és biztonságos üzemeltetését." Amennyiben Magyarország számára hozzáférhetővé válik egy olyan MI, amelynek használata biztonságos, és a nagy mennyiségű adathalmazokat segít rendszerezni és elemezni, akkor a fellelhető információkat hatékonyabban lehetne feldolgozni, későbbi hasznosításuk pedig hazánk szuverenitásának védelméhez is hozzájárulhat. A kérdéskör nehézségét okozza, hogy az ilyen MI-k fejlesztése idő-, energia- és forrásigényes, és általában csak a magasan kvalifikált munkaerővel és erős gazdasággal rendelkező országok tehetik meg. Azonban ha Magyarország egy ilyen szoftver megvételét tervezi, akkor számolnia kell azzal, hogy a felhasznált adatok esetlegesen kitettek lesznek a fejlesztő ország részére, akár egy tudatosan beépített kiskapu által, amely a feldolgozott adatokat továbbítja. Ilyen módon a digitális szuverenitás nemhogy nem valósul meg, hanem tovább sérül.

A fentiekre való tekintettel vagy olyan partnertől szükséges licenszt vásárolni, amelynek üzletfél-megbízhatósága nem megkérdőjelezhető, vagy szükségyszerűen saját terméket kell fejleszteni. Álláspontom alapján, habár a második eset rendkívül idő-, költség- és energiaigényes, mindenképpen érdemes ezt a forgatókönyvet követni, hiszen egy ilyen jellegű szoftver rendvédelmi, illetve nemzetbiztonsági célú felhasználása roppant körültekintést igényel, ugyanis beláthatatlan következménye lehet, ha egy ilyen MI a magyar rendészeti intézményrendszer minden információs adatbázisához hozzáférne, és azt vagy annak elemzett formáját továbbítaná valamilyen illetéktelen félnek. De nem lehet eltekinteni hosszú távon, sőt már-már közép- és rövid távon sem egy ilyen szoftver beszerzésétől, mivel a rendkívüli mennyiségű adatállomány elemzése humán szinten nem kellőképpen hatékony. A hatékonyság csökkenése pedig azt eredményezheti, hogy egy releváns esemény bekövetkezése előtt nem lesz arra utaló ismeret, sőt, rosszabb esetben az utólagos felderítési tevékenységet is megnehezítheti. Fontos megjegyezni azonban, hogy további jogi, szakmai, illetve erkölcsi kérdést jelent a különböző adatbázisok összekapcsolása és esetlegesen azok kombinált elemzése, akár a mesterséges intelligencia segítségével.

Összegzés

Összességében megállapítható, hogy hazánkat és Európát számos kihívás és kockázat érinti a biztonság széles mezsgyéjén, amelynek kezelése, elhárítása rendkívül összetett, több szerv és akár nemzetek fokozott koordinációját teszi szükségessé. A biztonsági kihívások összefüggő láncolata miatt egy-egy elemet nem lehet szimplán önmagában értelmezni, hiszen azok egymást gerjeszthetik, indukálhatják. Álláspontom alapján az egyik legnagyobb lehetőség – a benne rejlő kihívások ellenére – a technológiai innovációk célirányos fejlesztése, illetve beszerzése, amellyel akár számos más kockázati faktor kezelhető, csökkenthető. A mesterséges intelligencia, a *big data* és a kvantum-számítógépek kapcsán a legnagyobb probléma lehet, amennyiben az adott állam nem áll a megfelelő fejlettségi szinten, így egy esetlegesen ellenérdekelt állam vagy piaci, illetve más szereplő a képességei által előnyösebb helyzetben lehet. Fontos kiemelni, hogy a digitális szuverenitás elérése nemcsak állami érdek, hanem egyéni is. A fentiek alapján a legfontosabb minimum a technológiai fejlődés szoros követése.

Felhasznált irodalom

- A digitális szuverenitás jelentősége. *ICT Global*, 2023. szeptember 11. Online: <https://ictglobal.hu/rovid-hirek/a-digitalis-szuverenitas-jelentosege/>
- CSANÁDY Márton Tamás et al. (2008): A magyar képzett migráció a rendszerváltás óta. *Magyar Tudomány*, 169(5), 603–616.
- DOBÁK Imre (2011): *Az uniós külső határok által kettéosztott Kárpátok Eurorégió biztonságföldrajzi elemzése*. PhD-értekezés. Pécs: PTE Földtudományok Doktori Iskola.
- FARKASA (2021): Újra napirendre kerülhet az unióban a menekültkvóta. *Index*, 2021. január 6. Online: https://index.hu/kulfold/2021/01/06/menekultkvota_napirend_europai_unio/
- HAIG Zsolt (2018): *Információs műveletek a kibertérben*. Budapest: Dialóg Campus Kiadó.
- KOMÁROMI Zsombor (2025): PESTEL elemzés, PEST analízis példákkal. *Kanga Design*, 2025. január 10. Online: <https://kangadesign.hu/pestel-elemzes.html>
- Kornel (2024): Katasztrófa esetén jódtabletta? *Kekjod*, 2024. december 13. Online: <https://kekjod.hu/katasztrofa-eseten-jodtabletta/>
- Magyarországon egyelőre nem kell aggódni a zaporizzsai atomerőmű miatt, de a helyzet nem megnyugtató. *VG*, 2022. augusztus 8. Online: www.vg.hu/energia-vgplus/2022/08/magyarorszagonegyelore-nem-kell-aggodni-a-zaporizzsai-atomeromu-miatt-de-a-helyzet-nem-megnyugtato/
- Microsoft [é. n. a]: *Mit jelent a mesterséges intelligencia?* Online: <https://azure.microsoft.com/hu-hu/resources/cloud-computing-dictionary/what-is-artificial-intelligence#%C3%B6nvezet%C5%91-aut%C3%B3k>
- Microsoft [é. n. b]: *Mit jelent a big data elemzés?* Online: <https://azure.microsoft.com/hu-hu/resources/cloud-computing-dictionary/what-is-big-data-analytics>
- MEZŐ Ferenc (2007): Az emberi szükségletekre irányuló lélektani műveletek (PSYOPS). *Hadtudomány*, 17(1), 121–125.
- MURÁNYI József Ignác (2021): A terror árnyékában. *Magyar Rendészet*, 21(3), 171–180. Online: <https://doi.org/10.32577/mr.2021.3.12>
- NKI (2018): *A kvantumszámításban rejlő veszélyek*. Online: <https://nki.gov.hu/it-biztonsag/hirek/a-quantumszamitasban-rejlo-veszelyek/>
- PATÓ Viktória Lilla (2021): Európai Digitális Identitás, a biztonságosabb és ellenőrizhető személyi adattér. *NKE Európa Stratégia Kutatóintézet*, 2021. október 4. Online: <https://eustrat.uni-nke.hu/hirek/2021/10/04/europai-digitalis-identitas-a-biztonsagosabb-es-ellenorizhető-szemelyi-adatter>
- PÓCZIK Szilveszter (2008): A nemzetközi migráció tendenciái a 20. és a 21. században elméleti és történelmi nézőpontból. In PÓCZIK Szilveszter – DUNAVÖLGYI Szilveszter (szerk.): *Nemzetközi migráció – nemzetközi kockázatok*. Budapest: HVG-ORAC Lap- és Könyvkiadó Kft., 18–74.
- RABI Sándor (2009): *A vállalati környezet vizsgálata és a PEST elemzés kis-, középvállalati alkalmazása*. Online: www.veniens.hu/vallalatepito/2009/09/19/a-vallalati-kornyezet-vizsgálata-es-a-pestelemzes/
- RÁDI Balázs (2023): Egy másnak feszül a ChatGPT és a Google Bard. *Index*, 2023. február 7. Online: www.index.hu/gazdasag/2023/02/07/chatgpt-google-microsoft-mesterséges-intelligencia-keresomotor-bard/

- SZÚCS Gáborné (2017): Munkaerőhiány és munkanélküliség együttes jelenléte a munkaerőpiacon. Miben segíthet az oktatás a helyzet megoldásában? In KESERŰ Barna Arnold (szerk.): *Doktori Műhelytanulmányok 2017*. Győr: Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskola, 359–370. Online: <https://dfk-online.sze.hu/images/egyedi/doktori/doktori%20m%C5%B1helytanulm%C3%A1nyok%202017/sz%C5%B1cs%20g.pdf>
- TÁLAS Péter [é. n.]: Szuverenitás. In *Közszolgálati Online Lexikon*. Online: <https://lexikon.uni-nke.hu/szocikk/szuverenitas/>
- TÓTH András (2021): Az Európai Unió (szabályozási) útja a szuverenitás felé az adatalapú gazdaságban. *Európai Tükör*, 24(2), 27–56. Online: <https://doi.org/10.32559/et.2021.2.2>
- SZTOJCSEV Iván (2020): Tíz évvel a vörösiszap-katasztrófa után: a Mal Zrt. már nincs sehol, de jogerős ítéletre várni kell. *HVG*, 2020. október 3. Online: www.hvg.hu/gazdasag/20201003_vorosiszap_ajka_kolontar_devecser_evfordulo/
- VON BROCKDORFF, Philip (2022): *Digitális szuverenitás: az EU digitalizációjának és növekedésének alapvető pillére (saját kezdeményezésű vélemény)*. Európai Gazdasági és Szociális Bizottság. Online: <https://op.europa.eu/hu/publication-detail/-/publication/119809e3-6502-11ed-9f85-01aa75ed71a1/language-hu>

Jogi források

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról
2023. évi LXXXVII. törvény a nemzeti szuverenitás védelméről
1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról