NEMZETBIZTONSÁGI SZEMLE
11. évfolyam (2023) 1. szám 34–48. • DOI: 10.32561/nsz.2023.1.3

Budavári Krisztina[1]

A védelmi ipar és a nemzetbiztonság kapcsolata az aktuális 21. századi környezetben

National Security and the Defence Industry in the 21st Century

A globális biztonsági, gazdasági és technológiai környezetben zajló folyamatok következtében, számos hatás eredőjeként az országok védelmi ipari bázisai jelentősen felértékelődtek a 2010-es évektől kezdődően. Ugyanezek a hatások a nemzetbiztonsági rendszereket is széleskörűen és mélyen érintik. A védelmi ipar stratégiai iparág jellegéből adódóan komplex kapcsolatban áll az állam működésével és a nemzetbiztonsággal is. Így az országok biztonsága szempontjából jelentős szerepe van a nemzetbiztonsági rendszerek hatékony és eredményes működésének a védelmi ipari bázisokhoz kapcsolódó kihívások, kockázatok és fenyegetések kezelésében, amelyek azonban a folyamatosan romló globális biztonsági környezetben és exponenciális technológiai fejlődés mellett egyre sokrétűbbek, változók és egyre nehezebben előrejelezhetők.

Kulcsszavak: *nemzetbiztonság, nemzetbiztonsági szolgálatok, védelmi ipar, technológiai fejlődés, kiberbiztonság, ellátási láncok biztonsága, hírszerzés, elhárítás*

Defence Industrial Bases (DIB) have gained in significance lately, as a result of a number of impacts derived from the global security, economic and technological environment. The same environmental factors affected the national security systems extensively and deeply. Due to the strategic nature of the defence industry, it also has a complex relationship with the proper functioning of the state, also with the national security. Thus, the efficient and effective operation of national security systems has a significant role to play in addressing the challenges, risks and threats associated with Defence Industrial

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: krisztina.budavari.7@gmail.com

Bases that are increasingly diverse, changing and unpredictable in a deteriorating global security environment and under the influence of exponential technological advances.

Keywords: *national security, national security agency, defence industry, technological advancement, cyber security, supply chain security, intelligence, counterintelligence*

Bevezetés

A védelmi ipar jelenlegi hazai fejlesztése minőségileg és nagyságrendileg más feladatot jelent a nemzetbiztonsági rendszerre nézve a korábban évtizedekig fennálló helyzethez képest. A feladatok meghatározása elengedhetetlenné teszi a potenciális kihívások, kockázatok és fenyegetések azonosítását, azonban az adott globális biztonsági, gazdasági, technológiai és társadalmi környezetben ez nagyon jelentős kihívás. A környezet alapvető jellemzője ugyanis a komplexitás, az előrejelezhetetlenség, valamint a cirkuláris okság (ahol a viszonyokat és eseményeket kölcsönhatások interdependens hálózata határozza meg, vagyis az események és a szereplők viselkedése egyszerre oka és következménye is a másik viselkedésének vagy egy másik eseménynek). Továbbá a probléma nem egyszerűsíthető lokális szintre, mert a védelmi ipar vagy védelmi ipari bázisok nemzeti biztonsággal és nemzetbiztonsággal való kapcsolata a jelenlegi komplex környezetben csak globális kontextusban értelmezhető.

A védelmi ipar és a nemzetbiztonság viszonyának elemzése keretében ezért az elvégzett kutatás célja az is volt, hogy megtalálja ezeknek a potenciális kihívásoknak, kockázatoknak és fenyegetéseknek vagy egy elméleti osztályozási rendszerét, vagy egy olyan megközelítését, amely alkamas azok rendszerezésére, így a nemzetbiztonsági rendszer leendő feladatai szempontjából átlátható és konkrét cselekvési irányokat mutathat a stratégiai tervezés, a kapcsolódó szakpolitikák és a nemzetbiztonsági rendszer számára, továbbá elméleti szinten feltárja a védelmi iparhoz, illetve védelmi ipari bázishoz kapcsolódó, nemzetbiztonság szempontjából legkritikusabb kockázatokat. A kutatás azonosította azt a két területet – kiberbiztonság és ellátási láncok biztonsága – amely a legjelentősebb releváns nemzetbiztonsági kihívásokat, kockázatokat és fenyegetéseket rendszerként integrálja, ebből adódóan az ezek felőli megközelítés segíti azok logikus átláthatóságát és rendszerezését.

A kutatásban kihívást jelentett a nemzetbiztonság-fogalom többféle hazai értelmezése – mikro vagy szervezeti/funkcionális és makro vagy politikai/kormányzati,[2] vagy más megközelítésben a nemzetbiztonsági szolgálatok összessége szemben a kiterjesztőbb nemzetbiztonsági rendszer[3] értelmezéssel –, valamint ehhez kapcsolódóan kihívás

[2] Farkas 2020.

[3] „A szakterülettel foglalkozó kutatók közül néhányan a nemzetbiztonsági tevékenységben érintett, illetve azzal szorosan összefüggő szervezetek összességét mint nemzetbiztonsági szervezetrendszert definiálják. E felfogás szerint ebbe beletartoznak – többek között a hírszerző, elhárító, adatszerző, adatvédelmi feladatokat ellátó – nemzetbiztonsági szolgálatok és e szolgálatok irányítói. Ide sorolandók továbbá a nemzetbiztonsági szolgálatokat ellenőrző szervezetek, amelyek a szolgálatok működését, különböző szempontok szerint – anyagi, törvényességi, szakmai és a legújabb területként adatvédelmi – vizsgálják. Végül, de nem utolsósorban a nemzetbiztonsági szervezetrendszer elemei a szolgálatok közötti koordinációért felelős, azt végrehajtó szervezetek.” Mezei 2022: 85.

a nemzetbiztonság makro vagy politikai/kormányzati megközelítése és a biztonságelméletekben és biztonság- és védelempolitikában alkalmazott „nemzeti biztonság" fogalmak közötti viszony is. A kutatás megközelítésében a nemzetbiztonság politikai/kormányzati megközelítését alkalmaztam, és bár a három szint nagyon átfed, azokat a tényezőket, amelyek kizárólag a szélesebb, nemzeti biztonsághoz kapcsolódnak, a vizsgálódás próbálta nem fókuszba helyezni (bár kérdés, hogy például a gazdasági biztonságot veszélyeztető tényezők honnantól [hatókör, hatás erőssége stb.] jelentenek nemzetbiztonsági problémát stb.)[4] A védelmi ipar témakörével kapcsolatban pedig kihívást jelentett (nemcsak ebben a kutatásban, hanem folyamatosan), hogy egyrészt a hazai védelemgazdaság-tan nemcsak a nemzetközi folyamatokat nem követte le, hanem alapvető fogalmak (védelmi ipar, védelmi ipari bázis stb.) definíciója is hiányzik. Összességében a védelmi ipar tekintetében az a tényező, hogy a hazai tudomány az aktuális globális folyamatokat nem követte le, azt jelenti, hogy nem is tudja megfelelően kezelni a problémát. Mindez nemcsak a stratégiák, szakpolitikák, a teljes nemzetbiztonsági rendszer, hanem a nemzetbiztonsági szolgálatok működési szintjén is problémákat fog okozni (például a jelenlegi állás szerint nem tudható, hogy konkrétan mi az a vállalati kör, amely a védelmi ipart vagy védelmi ipari bázist jelenti Magyarországon, amellyel kapcsolatban a nemzetbiztonsági szolgálatoknak feladata van/lesz, vagy még inkább, kellene lennie).[5]

Globális környezet – a kihívások, kockázatok, fenyegetések eredete

A globális biztonsági környezetben az utóbbi években bekövetkezett változások oda vezettek, hogy a globális hatalmi erőviszonyok változásnak indultak, jelenleg a nemzetközi rendszer globális architektúrájának átstrukturálódása zajlik,[6] amit Oroszország Ukrajna elleni jelenleg is zajló agressziója még inkább felgyorsított. A 2010-es évektől folyamatosan romló biztonsági környezet és az USA (Donald Trump ciklusában) alkalmazott külpolitikája miatt a védelmi költségvetések folyamatos emelkedése a védelmi ipari keresletet globálisan jelentősen növelte, és megnövekedett az országok védelmi ipari bázisainak és a technológiai bázisainak jelentősége. A nagyhatalmi versengés visszatért, jelenleg is fokozódik. A legjelentősebb szereplők, az Egyesült Államok, Kína és Oroszország a hatalmi pozíciójuk növelését a globális technológiai vezető

[4] Gyakorlati értelemben az alkalmazott megközelítés azt jelenti, hogy pl. a technológiai fejlődést nem olyan szempontból lényeges értékelni, hogy az milyen új eszközöket képes biztosítani a nemzetbiztonsági szolgálatok számára, és az pl. milyen szervezeti változásokat indukálhat, hanem abból a szempontból, hogy a védelmi iparban keletkező új technológiai eredményeket a rendszernek meg kell védenie (pl. ipari kémkedés kérdése, kritikus IP jogokkal kapcsolatos szabályozás stb.).

[5] Természetesen vannak különböző besorolások, a kötelező szabályozások végrehajtásából (különböző engedélyesek, listákon szereplők, statisztikai adatszolgáltatásra kötelezettek, különböző ellenőrzések vagy tanúsítások alá esők stb.) eredően képződő csoportok, álláspontok (pl. Védelmiipari Szövetség stb.), de amint tudományos vizsgálódás tárgyává tesszük ezeket, láthatóvá válnak a problémák. Vagyis a legegyszerűbb feladat esetében, az iparágról szisztematikusan gyűjtendő adatok esetében már az sem határozható meg megalapozottan, hogy azt konkrétan kitől és kiről kellene gyűjteni, a leendő új belépőket nem is említve.

[6] Budavári 2021: 172.

szerep megszerzésében látták, és olyan stratégiákat kezdtek el alkalmazni, amelyek elsősorban a védelmi technológiai fejlesztésekben és elsősorban a feltörekvő és diszruptív technológiák területén globális fejlesztési hajszához, valamint fegyverkezési versenyhez vezettek.

A globális hegemón és a kihívó nagyhatalmak pedig a teljes nemzetközi rendszerre hatással vannak. Több területen paradigmatikus változások indultak el már a 2010-es években, vagy azt megelőzően (5. generációs hadviselés, NATO 4.0, Ipar 4.0), valamint a számos komplex hatás a globális védelmi ipar transzformációját is elindította (Aerospace & Defense 4.0). A védelmi ipar átalakulása (is) egyrészt közvetlenül visszahat a biztonsági, gazdasági és technológiai folyamatokra. Másrészt a paradigmatikus változások, például az exponenciális technológiai fejlődés eredményei mélyreható, széles körű, strukturális változásokat is okoznak és még inkább fognak okozni a jövőben, ami társadalmi és környezeti hatásokat is eredményez. A 2010-es évektől jellemzően bizonytalan és előrejelezhetetlen környezet pedig a jelenlegi orosz–ukrán konfliktus miatt még kiszámíthatatlanabb lett, és a nemzetközi rendszer szereplői közötti bizalom jelentős átrendeződését okozta. A globális, összekapcsolt világgazdaságban, ahol az erőforrások, tőke, termelési tényezők és technológia áramlása korábban jelentős fejlődést eredményezett, egyben jelentős aszimmetrikus függőségeket is, jelenleg beláthatatlan következményekre kell számítania az államoknak.[7] Mindez pedig egy olyan helyzetben, amikor a nagy kihívások (Grand Challenges), a klímaválság, demográfiai kihívások stb. egyre súlyosabb és sürgetőbb problémákat jelentenek, és amelyek kezeléséhez nemzetközi konszenzusok, globális és megosztott áldozatvállalás és olyan mennyiségű pénzügyi forrás lenne szükséges, amelyet csak a teljes rendszer együttesen tud előállítani. Az eddig fennálló nemzetközi rend alapvető értékei kérdőjeleződnek meg, és a globális problémák megoldására létrehozott nemzetközi szervezetek válnak működésképtelenné.

21. századi nemzetbiztonság

A változások és az ezredfordulót követően „kitáguló" biztonságpolitikai problémák (fegyveres konfliktusok, humanitárius vészhelyzetek, tömeges illegális migráció, terrorizmus felerősödése, környezeti és egészségügyi veszélyek) napjainkra visszafordíthatatlanul befolyásolják az egyes nemzetek biztonságát, amelyek már nem egy jól látható másik féltől származnak, hanem az összetett nemzetközi politikai, gazdasági, társadalmi és technológiai kérdéskörök mentén formálódnak.[8] „A biztonságot befolyásoló tényezők jelentős arányban már nem az államok közigazgatási határain belül keletkeznek, továbbá a korábbi határok szigorú elválasztó szerepe is leértékelődött."[9] A „nemzetbiztonsági rendszerek egyre több, nélkülözhetetlen szálon kapcsolódnak az állam és a társadalom egyéb szektoraihoz",[10] és „a modern társadalmak egyre

7 Budavári 2021: 75–85.
8 Dobák 2022a: 13.
9 Dobák 2022a: 15.
10 Dobák 2022a: 15.

sebezhetőbbé váltak".[11] A merev funkcionális elkülönülés lebontása (a társadalmi, gazdasági és tudományos fejlődés miatt) egyre sürgetőbbé válik,[12] a komplex kihívások miatt pedig a minél szélesebb körű együttműködések, szektoron belül, szektoron kívül és a civil szereplőkkel is. A kialakult konvergencia a fenyegetések oldaláról[13] elengedhetetlenné teszi a konvergenciát a fenyegetések kezelése oldaláról is.[14]

> „Az infokommunikációs megoldások robbanásszerű fejlődése – annak az államra és a társadalomra gyakorolt […] pozitív hatásai mellett – ugyanakkor közelebb is hozta a biztonságot fenyegető kihívásokat."[15] Az információrobbanás (évtizedek óta exponenciálisan nő a világon az újonnan keletkezett információk mennyisége) hatása is széles körben hat a nemzetbiztonsági rendszerre. Mivel a „releváns információk megszerzését célzó információgyűjtés a nemzetbiztonsági szolgálatok fő feladata, így minden, ami ezzel összefügg, jelentősen befolyásolja a nemzetbiztonsági szolgálatok működését".[16]

Egyre fontosabbá válik a biztonságra, védelemre és a hadviselésre a jövőben hatást gyakorló különböző technológiák folyamatos monitorozása is, és annak megállapítása, hogy azok a jövőben kulcsfontosságúnak tekinthetők-e, hogyan befolyásolják egy adott nemzet védelmi képességeit, biztonsága növelésének lehetőségeit, valamint a nemzeti ipar szintjén rendelkezésre állnak-e annak fejlesztési képességei.[17] A feltörekvő technológiák közül a mesterséges intelligencia stratégiai szinten fogja befolyásolni a nemzetbiztonságot is, valamint a biztonság minden szektorára hatással lesz. Az Amerikai Egyesült Államok 2018. évi *Nemzeti Védelmi Stratégiá*ja a mesterséges intelligenciát a feltörekvő technológiák azon csoportja közé sorolja, amely „megváltoztatja a háború jellegét és kihívást jelenthet a régóta fennálló háborús elvekre".[18] Egyes elemzők szerint a mesterséges intelligencia a védelmi szektorokban olyan mértékű transzformációt fog eredményezni, mint a nukleáris fegyverek, repülőgépek, számítógépek és a biotechnológia.[19] Ez potenciálisan egy új hadügyi forradalomhoz vezethet,[20] és talán a védelem fogalmának újradefiniálásához.[21] A mesterséges intelligencia katonai alkalmazásának várhatóan messzemenő következményei lesznek a kormányzás, az emberi jogok, a nemzetközi hatalmi erőviszonyok és a hadviselés terén egyaránt,[22] és civil alkalmazása esetében hasonló transzformatív hatásokra kell számítani.

A kihívások és változások a nemzetbiztonsági gondolkodásra és az érintett szervek feladataira is közvetlenül hatottak,[23] és a nemzetbiztonság értelmezése is

11 Dobák 2022a: 15.
12 Bács 2022: 42–43.
13 Bács 2022: 48.
14 Bács 2022: 50–51.
15 Dobák 2022a: 15.
16 Mezei 2022: 95.
17 Dobák 2022b: 62.
18 Porkoláb–Négyesi 2019: 4.
19 Allen–Chan 2017: 1.
20 De Spiegeleire – Maas – Sweijs 2017.
21 Tonin 2019: 1.
22 Wilner 2018: 1.
23 Dobák 2017: 236.

egyre kiterjesztőbbé vált. „Ezen változások talán a legjelentősebbeknek tekinthetőek a hidegháború befejezése óta, amely a nemzetbiztonsági, illetve titkos információgyűjtési képességekkel rendelkező biztonsági struktúrák szerepének felértékelődését eredményezték."[24] „Azt, hogy mit hoz a század további része […] nehéz megjósolni. A változás dinamikája és az érintett területek sokasága alapján azonban rövid időn belül jelentős változásokra kell felkészülni."[25] „A kockázatok sokszorozódása, a határon átnyúló jellege, súlyossága okán tovább kell erősíteni az országokon belüli, illetve a nemzetközi együttműködéseket. […] A technológiai robbanás, a kibertér jelentőségének folyamatos növekedése következtében további, új típusú nemzetbiztonsági szintű kockázatok megjelenése várható."[26]

> „A titkosszolgálatok technikai vonatkozású szegmenseit […] a biztonság oldaláról jelentkező fenyegetések változása, valamint a technikai környezet fejlődése formálja majd a továbbiakban is. A fenyegetések terén a már most is látható hangsúlyeltolódások új hírszerzési célokat, és ezek mentén új és újabb információgyűjtési megoldásokat eredményeznek majd. […] Egyértelmű szerepet kap a technológiai fölény kérdése, amely a korszerű, határokon átnyúló, globális méretű információgyűjtési képesség mentén megjósolhatatlan előnyöket biztosíthat az ezekkel rendelkező országoknak. Mindezek mögött új alkalmazási elvek, módszerek jöttek és jönnek létre, ideértve mind az információgyűjtés, mind az információk elemzésének és értékelésének kiemelten fontos területeit is, és mindezek […] kihathatnak az érintett nemzetbiztonsági szervezetek struktúráira is."[27]

Ezekre a változásokra az egyes államoknak és azok nemzetbiztonsági rendszereinek ma még csak részben állnak rendelkezésére a megfelelő kezelési technikák.[28]

A védelmi ipar mint stratégiai iparág

A védelmi ipar szereplői tevékenységük jellegéből adódóan számos szempontból speciális üzleti, politikai, szabályozási környezetben működnek, speciális kapcsolatokkal, speciális piacokon, ahol más piacokhoz képest sokkal jellemzőbbek a piacot, a versenyt, az árakat, a tranzakció összelőnyét torzító anomáliák. Ráadásul az állammal együtt részt vesznek a védelem mint közjószág előállításában. A védelemhez szükséges termékek és szolgáltatások jelentős és kritikus részét a védelmi ipar állítja elő, vagyis működése és teljesítménye közvetlen kapcsolatban áll az ország védelmi képességeivel, a védelemgazdasági potenciállal és a katonai potenciállal, szélesebb körben a biztonság- és védelempolitikával stratégiai szinten. Másrészt (általában jelentős) gazdasági szereplő, ezen keresztül hatással van a makrogazdasági teljesítményre, valamint (általában széles körű) külkereskedelmi tevékenysége révén hatással van a fizetési mérlegre, ezeken keresztül a gazdaságpolitikára. Továbbá (leghangsúlyosabban) a fegyverkereskedelem és a védelmi technológiai transzferek

[24] Dobák 2017: 236.
[25] Mezei 2022: 102.
[26] Mezei 2022: 102.
[27] Boda–Dobák 2016: 23–24.
[28] Dobák 2022a: 13.

révén az alkalmazható külpolitikára is.[29] A védelmi ipari külkereskedelem, kiemelten a fegyverkereskedelem szabályozása szintén nemzetbiztonsági kérdés is. A védelmi iparnak az is sajátossága, hogy a biztonsági környezet romlása – ami egyébként a nemzetbiztonsági kockázatokat növeli – az emelkedő védelmi költségvetések révén számára pozitív kilátásokat jelent.

A globális védelmi ipar mai jellemzőit – ami azonban jelenleg ismét transzformálódik –, két jelentős időszak alakította, a hidegháború lezárulását követő időszak, amikor a védelmi költségvetések jelentősen csökkentek, és az államok biztonsági percepciói jelentősen megváltoztak, valamint az utóbbi évtized, a biztonsági környezet ismételt jelentős romlása, valamint az exponenciális technológiai fejlődés.[30] Ennek következtében az iparág mára egyrészt transznacionális értékláncok hálózataként értelmezhető, másrészt egyre nagyobb a koncentrációja, harmadrészt pedig egyre inkább együttműködik civil piaci szereplőkkel. Ez a rendszer egyre inkább híján van az átláthatóságnak, és a profitmaximalizálási célok mellett egyre nehezebb egyensúlyozni a biztonsági szempontokkal.

Látható, hogy a védelmi ipar működése komplex kölcsönhatásban van az állammal, a nemzeti biztonsággal és a nemzetbiztonsággal is. Ebből eredően számos és máshol nem jellemző, sajátos tényezők is nemzetbiztonsági kihívásként, kockázatként és fenyegetésként jelenhetnek meg az iparággal kapcsolatban, vagy onnan eredően. Példaként, a védelmi ipar esetében akár az iparág struktúrája is jelenthet nemzetbiztonsági kockázatot. Az USA-ban például jelenleg nemzetbiztonsági kockázatként értékelik az elmúlt időszak egyik iparági trendjéből (jelentős számú felvásárlás és összeolvadás, igen nagyértékű tranzakciók, „megamerger"-ek)[31] adódó iparági struktúrát. Az USA védelmi minisztériuma által nemrég kiadott jelentés szerint a védelmi ipar extrém konszolidációja a piaci versenyt olyan mértékben csökkentette, amely már nemzetbiztonsági kockázatot jelent.[32] További példaként említhető a klaszterizácó, amelynek számos gazdasági előnye van, például a járműiparban kiterjedten alkalmazzák, de más iparágaktól eltérően a védelmi iparban viszont jelentősen növeli a kockázatokat (a vállalati szintű, a piaci szintű és a nemzetbiztonsági kockázatokat egyaránt). A védelmi iparra jellemző speciális beszerzési metódusok szintén befolyásolják a piacot, valamint az iparágban kiemelt jelentőségű szellemi tulajdonhoz fűződő jogok (IP-) védelmének szabályozása is. (Mindkét tényező az utóbbi időben több országban jelentős stratégiai újragondolások tárgyává vált.) A két tényező külön-külön is alkalmas a piacot torzító jelenségeket létrehozni (éppen ezért hátrányokat kikerülő, akár illegális akciókat kiváltani), azonban ha figyelembe vesszük a köztük lévő kapcsolatot, a helyzet még bonyolultabb, ráadásul a legdrágább fegyverrendszereknél jelenik meg leginkább. Olyan komplex jelenségekről is beszélhetünk továbbá (piactorzító hatású jelenség, egyben nemzetbiztonsági kockázat), mint a katonai-ipari hatalmi komplexumok, amely egy erőteljes, kiterjedt és erőforrásban gazdag koalíció, amelynek önmagát fenntartó és megerősítő természete van, és a legfőbb közös célja a katonai szektor

29 Budavári 2021: 20–21.
30 Budavári 2021: 20–27.
31 Iparági trendekről és vállalati stratégiákról bővebben: Budavári 2021: 109–123.
32 The White House 2022.

folyamatos bővítése függetlenül a tényleges szükségletektől.[33] A védelmi iparban kifejlesztett és katonai felhasználásra alkalmazott új technológiák szintén relevánsak lehetnek nemzetbiztonsági szempontból. Az USA nemrég közzétette azoknak a technológiáknak a listáját, amelyeket a gazdasági biztonság és nemzetbiztonság szempontjából a legnagyobb hatásúaknak tart, ezek a mesterséges intelligencia, bioökonómia, autonóm rendszerek, kvantumtechnológia és félvezetők.[34]

Az összes potenciális kockázat bemutatása a reális vállalás kereteit jelentősen túllépné, azok meghatározása a nemzetbiztonsági rendszerek feladata, azonban látható a kihívás nagyságrendje, amivel a jelenlegi környezetben szembesülnek.

Hazai környezet

Magyarországon a védelmi ipar fejlesztése kormányzati stratégiai célkitűzés a *Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program*[35] – jelenleg Honvédelmi és Haderőfejlesztési Program (HHP) – 2017. évi elindulása óta. A program egyszerre tűzte célul a haderő haditechnikai korszerűsítését és a magyar védelmi ipar intenzív fejlesztését egy komplex gazdaság-, társadalom-, valamint biztonság- és védelempolitikai célrendszer részeként. A védelmi képességcélokon kívül a kormány a gazdaság diverzifikáltságának növelését, új munkahelyek teremtését, versenyképes és magas hozzáadott értéket termelő iparágak létrehozását, az ország innovációs képességeinek javítását is el kívánja érni. Védelmi területen pedig kiemelt célok az importfüggőség csökkentése, az ellátásbiztonság megteremtése, valamint a nemzeti ellenállóképesség növelése.[36] Mindezek a célok a legújabb stratégiai dokumentumokkal – 2020. évi Nemzeti Biztonsági Stratégia (NBS),[37] 2021. évi Nemzeti Katonai Stratégia (NKS),[38] 2021. évi Védelmi Ipari Stratégia (VIS)[39] – is igazolhatók. Mind az NBS, mind az NKS nagy súlyt helyez a védelmi ipar szerepére a nemzeti biztonság garantálásában. A nemzetbiztonsági megközelítés egy helyen jelenik meg az NBS-ben: „A hazai védelmi ipar, azon belül is a kutatás-fejlesztés és az innováció támogatása *nemzetbiztonsági érdek*, mivel ezek által csökkenthető az import függőség, növelhető az ellátásbiztonság és hazai gyártmányokkal korszerűsíthetőek a védelmi eszközök."[40]

Az iparág ilyen léptékű fejlesztése, ami a biztonság minden szektorára jelentős hatásokat gyakorolhat (és a célja is az, hogy jelentős biztonsági és makrogazdasági hatásokat érjen el), a nemzetbiztonsági rendszer számára a korábbi feladatokhoz képest minőségileg és nagyságrendben is sokkal jelentősebb feladatot fog jelenteni. Mindezt összevetve a regionális és globális biztonsági környezet jelenlegi folyamatos, jelentős romlásával és annak hatásaival és következményeivel (szankciók, embargók

33 Budavári 2021: 26.
34 NCSC 2021.
35 1298/2017. (VI. 2.) Korm. határozat.
36 Budavári 2021: 152–153.
37 1163/2020. (IV. 21.) Korm. határozat.
38 1393/2021. (VI.24.) Korm. határozat.
39 A VIS titkos minősítésű dokumentum, tartalmával kapcsolatban nyilvános, hiteles forrás: www.parlament.hu/documents/static/biz41/bizjkv41/HOB/2106081.pdf
40 1163/2020. (IV. 21.) Korm. határozat 105. pont.

szintjétől a nemzetközi rendszer szereplői közötti bizalomban történt átrendeződésig, a védelempolitikákban, védelmi költségvetésekben, a globális védelmi iparban, valamint a technológiai fejlesztések terén már ismertetett folyamatok felgyorsulásáig) még inkább.

Hazai tekintetben lényeges, és az eddigi folyamatokból már látható, hogy az újonnan épülő iparágban a hazai vállalatok a létrejövő transznacionális értékláncokba alacsony szinten fognak bekapcsolódni. Ezek az értékláncok rendkívül komplexek (például a Leopard II harckocsi ellátási lánca több mint 1500 vállalatból áll[41]). Viszont „az ellátási lánc annyira erős, mint a leggyengébb láncszeme".[42] Az is jellemző, hogy főleg kkv-k kapcsolódnak be a védelmi iparba (mivel nagyvállalatok nincsenek). Ezzel kapcsolatban az USA Védelmi Ipari Szövetségének kutatása kimutatta, hogy (az USA-ban) összefüggés van a vállalatok mérete és az általuk jelentett kockázat között: minél kisebb a vállalat, annál nagyobb a biztonsági rés.[43] Lényeges továbbá, hogy sem az iparági szereplők, sem az állam nem rendelkezik jelentős tapasztalattal, sem jelentős erőforrásokkal,[44] a szabályozás és a teljes rendszer (beleértve a teljes innovációs rendszert) az évtizedekig fennálló korábbi helyzetet ismeri. Ráadásul az iparág nem organikusan fejlődik, hanem irányítottan. Továbbá nemzetbiztonsági kockázatot jelenthet hazai szinten, és főként a nagyhatalmak közötti viszony elmúlt időszakbeli jelentős romlása mellett, az iparpolitika (nyugati védelmi ipari nagyvállalatok betelepítése minél nagyobb számban) és a külpolitikában a keletinyitás-politika (infrastrukturális beruházások, szállítási útvonalak, logisztikai csomópontok finanszírozási és tulajdonosi háttere) kombinációja is. A jelenlegi helyzetben az orosz–ukrán háború hatása is jelentős a hazai védelmi iparhoz kapcsolódó nemzetbiztonsági kockázatokra. Az elhúzódó konfliktus nagyon jelentős keresletnövekedést okozott, ami egyre nagyobb nyomást helyez (piaci és biztonsági tekintetben egyaránt) a védelmi ipari bázisokra globálisan, és komplex hatások révén számos kockázatot, veszélyt, fenyegetést keletkeztet. (Például egy hazánk szempontjából releváns kockázat, hogy az adott globális ellátásilánc-problémák mellett, rövid távon az alacsony stratégiai jelentőségű és alacsony alkuerejű országok – mint hazánk a régióban – jelentős ellátási problémákkal szembesülhetnek, ami gyengítheti a védelmi képességüket.)[45]

A hazai nemzetbiztonsági rendszer számára így a jelenleg épülő új iparág jelentős kihívásokat fog jelenteni, nemcsak az iparág speciális adottságaiból adódóan, hanem a globális és regionális folyamatokból, a lokális adottságokból és képességekből, valamint nem kevésbé a hazai alkalmazott politikák közötti stratégiai összhang esetleges hiányából adódóan.

41 The European Parliament 2014.
42 Lásd: www.cisa.gov/resources-tools/groups/ict-supply-chain-risk-management-task-force
43 Bourbon 2019.
44 A világ legnagyobb védelmi ipari vállalatainak néhány éves önálló költségvetése csak az új termékek fejlesztésére, egyes esetekben több mint a Zrínyi HHP teljes 10 éves költségvetése. Budavári 2021: 165.
45 Kandrík 2022.

A legjelentősebb kockázatok – kiberbiztonság és ellátási láncok biztonsága

A kutatás alapján a már említett két terület mint rendszer jelenti a legjelentősebb nemzetbiztonsági kockázatokat a védelmi ipar szempontjából: a kiberbiztonság és az ellátási láncok biztonsága. Tekintettel a hazai szakirodalom hiányosságaira is, a tárgyi témában az Amerikai Egyesült Államok (USA) – mint a világ legnagyobb védelmi ipari bázisával rendelkező, a globális technológiai vezető szerepet még birtokló, és messze a legmagasabb védelmi költségvetéssel rendelkező ország[46] – gyakorlatát vizsgáltam.[47]

A kiberbiztonság kiemelt, nemzetbiztonsági szintű kezelése már Magyarországon, a gyakorlatban is megvalósul. Viszont a védelmi ipar tekintetében figyelemre méltó, és a hazaitól teljesen eltérő szemléletet tükröz, hogy az USA-ban a védelmi ipari bázis külön szektort képez a kritikus infrastruktúrán belül (16 szektor összesen) a Kiberbiztonsági és Infrastruktúra Biztonsági Ügynökség (Cybersecurity & Infrastructure Security Agency, CISA) rendszere alapján. Minden szektor rendelkezik saját kockázatkezelési ügynökséggel, a védelmi ipari bázis szektor kockázatkezelési ügynöksége a Védelmi Minisztérium (Department of Defense, DoD). Az ügynökségek ágazatspecifikus tervet készítenek, az állami és a magánszektorbeli partnerek összehangolt együttműködésével, amely részletezi, hogyan valósul meg a Nemzeti Infrastruktúra Védelmi Terv kockázatkezelési keretrendszere az ágazat egyedi jellemzőinek és kockázatainak kontextusában.[48]

A védelmi szempontból kritikus ellátási láncok kockázatainak nemzetbiztonsági szintű kezelése tekintetében viszont szisztematikus hazai kormányzati gyakorlat nem igazolható. Az USA azonban az ellátási láncok problémáját a gyakorlatban is kiemelten, nemzetbiztonsági szinten kezeli. A Nemzeti Hírszerzési Igazgató Hivatalában (Office of the Director of National Intelligence, ODNI) a Nemzeti Elhárítási és Biztonsági Központ (National Counterintelligence and Security Center, NCSC) feladatkörébe tartozik az ellátási láncok fenyegetéseinek kezelésével kapcsolatos prioritások meghatározása és a Hírszerző Közösség (U.S. Intelligence Community, IC) erőfeszítéseinek összehangolása ezen a területen. A két terület össze is függ, vagyis a kiberbiztonság az ellátási láncokban és az IKT ellátási láncok biztonsága a legkritikusabb nemzetbiztonsági kihívásoknak tekinthetők. Az USA gyakorlatában az NCSC-n belül az Ellátási Lánc és Kiberigazgatóság (Supply Chain and Cyber Directorate, SCD) a két területért egyben felelős, feladata a nemzeti ellátási láncok biztonságának és a kiberbiztonság fokozása, tájékoztatás, irányítás és koordináció a stratégiai partnerekkel együttműködve a kockázatokkal kapcsolatos integrált döntések és reagálás érdekében.[49]

46 Bővebben: Budavári 2021: 72–123.
47 Lásd az irodalomjegyzéket.
48 Lásd: www.cisa.gov/defense-industrial-base-sector
49 Lásd: www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats

Az ellátási láncok[50] emberek, folyamatok, technológiák, információk, erőforrások alkotta globálisan kiterjedt és összekapcsolt hálózatok, amelyek termékeket és szolgáltatásokat hoznak létre és juttatnak el a vevőhöz. A globális ellátási láncok dinamikusak, sokrétűek és komplexek. Az átláthatóság és a követhetőség hiánya biztonsági kockázatot jelent, mert minden egyes komponensnek megvan a saját ellátási lánca, ami számos lehetőséget jelent az ellenséges szándékú szereplők számára, hogy szabotálják bármelyik összetevőt (az alapanyagoktól a gyártási folyamatokon keresztül, a szállításon és csomagoláson át, számos ponton).[51] Továbbá nemzetbiztonsági szempontból az egyes lánctípusok megkülönböztetésének is van jelentősége. A védelmi ellátási láncok vagy védelem szempontjából kritikus ellátási láncok az állam szemszögéből értelmezendők, a védelmi ipari ellátási láncok (amelyek részei az előbbieknek) pedig az iparág szemszögéből. Az állam biztonságközpontú érdeke az ellátási láncai tekintetében – ami befolyásolja azok ellenőrzését, védelmét és szabályozását – ugyanis nem minden esetben esik egybe az iparág és a vállalatok profitközpontú érdekeivel a saját láncaikra vonatkozóan. Természetesen az államnak is érdeke a gazdasági biztonság szempontjainak, ezért a vállalatok profittermelési képességeinek figyelembevétele, de a vállalatok profitelvárásaikban nem az ország gazdasági biztonságának ideális szintjéből indulnak ki. Az egyensúlytalanság, a nem megfelelő szabályozás, a túlzott korlátozások ezen a területen pedig automatikusan generálhatják a nemzetbiztonsággal ellentétes, akár illegális tevékenységeket (a szabályozások be nem tartásától kezdve, amelyek olyan biztonsági réseket okozhatnak, ahol a haderő vagy a kormányzat információi is kiszivároghatnak,[52] külföldi „outsourcing" vagy „offshoring" kritikus technológiai információk kiszivárgásának veszélyével, embargók megkerülése, illegális [fegyver]kereskedelem stb.).

A védelmi ellátási láncok nemzetbiztonsági kockázataival kapcsolatban az USA védelmi minisztériuma kiadott egy jelentést, amelyben átlátható csoportosításban összegzi azokat, elsősorban az *elhárítási kihívások* felőli megközelítésben:

„Nemzetbiztonsági kockázatok (Counterintelligence Risks):

1. Ellátási láncok nem megfelelő átláthatósága
   a) Képtelenség azonosítani a külföldi joghatóság vagy külföldi kormány irányítása alá tartozó alsóbb szintű beszállítókat
   b) A fenyegetések, sebezhetőségek és kockázatok azonosításának nehézségei az alsóbb szintű ellátási láncokban lehetővé teszik hamisított vagy kompromittált alkatrészek behelyezését az ellátási láncba

[50] Mivel a kiberbiztonsággal kapcsolatos kutatások hazai szinten is jelen vannak, és széleskörűen áll rendelkezésre a téma szakirodalma, illetve igazolhatóan a téma jelentősége felismert, ezért a fejezet a továbbiakban az ellátási láncokkal foglalkozik.

[51] Ferry–Poindexter 2016: 19.

[52] Az USA Nemzeti Védelmi Ipari Szövetségének (National Defense Industrial Association, NDIA) egy kutatása kimutatta, hogy az USA hazai védelmi beszállítói közül a kkv-k kevesebb mint 60%-a olvassa el azt a dokumentumot, amely a védelmi beszállítókra vonatkozó minimum biztonsági sztenderdeket tartalmazza. Lásd Bourbon 2019.

2. Elavult beszerzési politikák és eljárások
   a) A hazai befektetők elriasztása a magas tőkebefektetési igények miatt
   b) Az inkonzisztens minisztériumi beszerzési gyakorlatok instabilitást okoznak az alsóbb szintű beszállítóknál és akadályozzák a befektetéseket újabb technológiákba
3. Külföldi tulajdon, irányítás vagy befolyás
   a) A Védelmi Minisztérium kereslete nem elég jelentős ahhoz, hogy a szabványosítást és a technológiai modernizációt ösztönözze
   b) Erőteljes függés külföldi országoktól és kizárólagos beszállítóktól a kritikus komponensek tekintetében, az erodálódott hazai ellátási láncok miatt
4. A Védelmi Minisztériummal kapcsolatban álló hálózatok kiberbiztonsági pozíciója
   a) Egyre gyakoribbak a védelmi ipari bázist érintő kifinomult, megfelelő erőforrásokkal támogatott kibertámadások
   b) A védelmi ipari bázisban a szoftverfejlesztés és -terjesztés csatornáinak nem megfelelő a kiberbiztonsági helyzete, ami a védelmi ipari bázis kitettségét fokozza mind a hagyományos kibertámadásokkal, mind a szoftverek ellátási láncaiban végrehajtott kibertámadásokkal szemben."[53]

A fent azonosított kockázatok körvonalazzák azt a számtalan kockázatot, amellyel a védelmi ipari bázisnak szembe kell néznie. Azonban hangsúlyozni kell, hogy az információs és kommunikációs technológiák (IKT) ellátási láncainak biztonsága kiemelten hat a védelmi ellátási láncokban a kritikus termékekre és szolgáltatásokra. Ezért a védelmi ipari bázist támogató IKT ellátási láncok biztonságát előtérbe kell helyezni, így az IKT ellátási lánc védelme erősokszorozó a védelmi ellátási láncok tekintetében.[54]

Összefoglalás

A jelenlegi komplex környezetben mind a védelmi ipar, mind a nemzetbiztonsági rendszerek jelentős változásokon mennek keresztül. A globális biztonsági környezet romlásával mindkét terület felértékelődött az utóbbi években, ami továbbra is, gyorsulva folytatódik. A változások másik legfőbb okozója pedig a rohamos technológiai fejlődés. A nemzetbiztonsági rendszereknek így a védelmi ipari bázisok kapcsán nagyon jelentős kihívásokat, kockázatokat és fenyegetéseket kell kezelniük, úgy, hogy közben maguk is változnak. A kockázatok, kihívások és fenyegetések sokrétűek, komplex kölcsönhatásban állnak, egyre inkább előrejelezhetetlenek, váratlan forrásokból, országhatárokra tekintet nélkül jelentkeznek. Ebben a helyzetben a releváns kockázatokat és az azokból következő feladatokat is rendkívül nehéz meghatározni.

[53] NCSC 2022.
[54] NCSC 2022.

A kutatás alapján levonható az a következtetés, hogy nemzetbiztonsági szempontból, a védelmi ipar tekintetében a védelmi ellátási láncok kiberbiztonsági kockázatai a legjelentősebbek, a legmélyebb hatásokat tudják gyakorolni a nemzetbiztonságra, és a legsürgetőbb azok kezelése.

Irodalomjegyzék

Allen, Greg – Chan, Taniel (2017): *Artificial Intelligence and National Security.* Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs. Online: www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

Bács Zoltán György (2022): Viribus Unitis, avagy civil-professzionális konvergencia a 21. században. In Dobák Imre (szerk.): *Nemzetbiztonság a 21. század elején. Szemben a kihívásokkal.* Budapest: Ludovika, 42–51.

Boda József – Dobák Imre (2016): Titkosszolgálatok fejlődése – technikai szemmel. *Nemzetbiztonsági Szemle,* 4(4), 17–25. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1879/1168

Bourbon, Ben (2019): Agencies Look to Minimize Supply Chain Risks. *FedTech Magazine,* 2019. november 6. Online: https://fedtechmagazine.com/article/2019/11/agencies-look-minimize-supply-chain-risks

Budavári Krisztina (2021): *A magyar védelmi ipar helyzete és fejlődési lehetőségei.* Budapest: Magyar Hadtudományi Társaság. Online: https://doi.org/10.51491/vedelmi.ipar2021

De Spiegeleire, Stephan – Maas, Matthijs – Sweijs, Tim (2017): *Artificial Intelligence and the Future of Defense: Strategic Implications for Small- and Medium-Sized Force Providers.* The Hague: The Hague Centre for Strategic Studies. Online: https://bit.ly/3NVI0qn

Dobák Imre (2017): Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében. *Hadmérnök,* 12(2), 235–249. Online: http://hadmernok.hu/172_19_dobak.pdf

Dobák Imre (2022a): A nemzetbiztonság 21. századi értelmezése és jellemzői. In Dobák Imre (szerk.): *Nemzetbiztonság a 21. század elején. Szemben a kihívásokkal.* Budapest: Ludovika, 13–28.

Dobák Imre (2022b): Társadalom – technológiai környezet – nemzetbiztonság. In Dobák Imre (szerk.): *Nemzetbiztonság a 21. század elején. Szemben a kihívásokkal.* Budapest: Ludovika, 52–67.

The European Parliament (2014): *Defence Industrial Supply Chains and the Role of SMEs in the Sector.* Online: https://bit.ly/3LAPaNR

Farkas Ádám (2020): Gondolatok a nemzetbiztonság fogalmáról. *Szakmai Szemle,* 18(3), 5–20. Online: www.knbsz.gov.hu/hu/letoltes/szsz/2020_3_szam.pdf

Ferry, Heath – Poindexter, Van (2016): Supply Chain Risk Management. An Introduction to the Credible Threat. *Defense AT&L,* 2016. július–augusztus. 19–22. Online: www.dau.edu/library/defense-atl/DATLFiles/Jul-Aug2016/Ferry_Poindexter.pdf

Kandrík, Matej (2022): The Defense Impact of the Ukraine War on the Visegrád Four. *German Marshall Fund,* 2022. július 28. Online: www.gmfus.org/news/defense-impact-ukraine-war-visegrad-four

Mezei József (2022): A szervezetrendszerek módosítása, strukturális válaszok. In Dobák Imre (szerk.): *Nemzetbiztonság a 21. század elején. Szemben a kihívásokkal.* Budapest: Ludovika, 85–102.

NCSC (2021): *NCSC Fact Sheet – Protecting Critical and Emerging U.S. Technologies from Foreign Threats.* 2021. október 21. Online: www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_Emerging%20Technologies_Fact-sheet_10_22_2021.pdf

NCSC (2022): *Fortifying the Defense Industrial Base (DIB) Supply Chains.* 2022. február. Online: www.dni.gov/files/NCSC/documents/supplychain/dod-supply-chain-spotlight-2022-4C850B07-.pdf

Porkoláb Imre – Négyesi Imre (2019): A mesterséges intelligencia alkalmazási lehetőségeinek kutatása a haderőben. *Honvédségi Szemle,* 147(5), 3–19. Online: https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/208

Tonin, Matej (2019): *Artificial Intelligence: Implications for NATO's Armed Forces.* NATO Parliamentary Assembly, Science and Technology Committee (STC), Sub-Committee on Technology Trends and Security (STCTTS), 2019. október 13. Online: https://bit.ly/3Vu9lS8

The White House (2022): *Fact Sheet: Department of Defense Releases New Report on Safeguarding our National Security by Promoting Competition in the Defense Industrial Base.* 2022. február 15. Online: https://bit.ly/3LAEChK

Wilner, Alex S. (2018): *Artificial Intelligence and Deterrence: Science, Theory and Practice.* (STO-MP-SAS-141) NATO Science and Technology Organization. Online: www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-141/MP-SAS-141-14.pdf

Jogi források

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

2011. évi CLXXI. törvény a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény katonai nemzetbiztonsági szolgálatok összevonásával kapcsolatos módosításáról, valamint az azzal összefüggő további törvénymódosításokról

2014. évi CIX. törvény a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény, valamint egyes törvényeknek a nemzetbiztonsági ellenőrzéssel összefüggő módosításáról

1298/2017. (VI. 2.) Korm. határozat a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról
1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
1393/2021. (VI.24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról
128/2011. (XII. 2.) HM utasítás a katonai nemzetbiztonsági szolgálatok összevonásával kapcsolatos egyes feladatokról
60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról