Stratégiai Védelmi Kutatóintézet
ELEMZÉSEK 2022/15

2022. november 28.

Selján Péter:[1] Forradalmi technológiák Csehországban – Fókuszban a kiberbiztonság

Vezetői összefoglaló

- A nemzetközi biztonsági környezet jelentős változásokon megy keresztül, amit a modern technológiák rohamos fejlődése is alakít. A fejlődő és felforgató technológiák (mint például a mesterséges intelligencia vagy a kvantumtechnológia) elterjedése a kiberbiztonság területén is paradigmaváltáshoz fog vezetni. Miközben az államok és a társadalmak modern technológiáktól való függősége csak fokozódni fog, a támadási felületek növekedése révén a kiberbűnözők, a nemzetállami és a nem állami szereplőkhöz köthető támadók lehetőségei is kiszélesednek.
- A Csehországot érintő biztonsági kihívások között kiemelt helyen szerepelnek a kibertámadások. Prága szerint az egyik legnagyobb fenyegetést az egyoldalú politikai, gazdasági, katonai és hírszerzési nyomásgyakorlással, vagy akár nyílt agresszióval önálló befolyási övezet kialakítására törekvő nemzetállami szereplők jelentik. A nyomásgyakorlás, illetve a hírszerző és katonai műveletek pedig a kibertérre is kiterjednek. Éppen ezért Csehország vezető szerepet kíván betölteni a közép-európai régióban a kiberbiztonság terén, és offenzív kiberképességek kifejlesztésén is dolgozik.
- Egyre fontosabbá válik a nemzetközi kiberbiztonsági együttműködés. Ma már megkérdőjelezhetetlen, hogy a kiberbiztonság az egyik legfontosabb aspektusa a nemzetközi biztonságnak, a kiberbiztonsági kihívásokkal pedig csak proaktív hozzáállással és széleskörű nemzetközi együttműködéssel lehet hatékonyan felvenni a versenyt.

Csehország biztonsági környezete az elmúlt években jelentős mértékben megváltozott, és a számos biztonsági kihívás, befolyásoló tényező, valamint a már viszonylag régóta zajló trendek kölcsönhatása révén egyre kiszámíthatatlanabbnak mutatkozik. Prága számára az elmúlt években az elsőszámú kihívás a gazdasági és a társadalmi fejlődés biztosítása volt. Miközben a közvetlen katonai támadás esélye minimálisnak volt tekinthető, fokozódott a nem katonai jellegű fenyegetések jelentősége, mint például a stratégiai ellátási láncok megszakadásának kockázata, a nemzetközi migráció negatív vonatkozásai, az egyre növekvő globális egyenlőtlenségek, valamint a gazdasági és a pénzügyi bűncselekmények számának növekedése. Habár a biztonsági fenyegetések elsősorban államokhoz köthetők, növekszik a nem állami szereplők jelentette, akár aszimmetrikusnak is nevezhető kockázatok mértéke.

Mivel Csehország számára is a NATO-tagság, illetve a szilárd alapokon nyugvó kollektív védelem jelenti az elsőszámú garanciát biztonságának megőrzésére, Prága szempontjából is kiemelt fontosságú a NATO tagállamaival és az Európai Unióval ápolt multilaterális mechanizmusok működésének megőrzése. A legnagyobb fenyegetést már 2014 óta az Oroszországhoz hasonló, egyoldalú politikai, gazdasági, katonai és hírszerzési nyomásgyakorlással, vagy akár nyílt katonai agresszióval önálló befolyási övezet kialakítására törekvő nemzetállami szereplők jelentik Prága számára – és Oroszországot tekintik ilyen szereplőnek. Ez a fajta nyomásgyakorlás, illetve a hírszerző és katonai műveletek pedig a kibertérre is kiterjednek.[2]

Éppen ezért, a Csehországot érintő biztonsági kihívások között kiemelt helyen szerepelnek a kibertámadások. Elemzésünkben először lényegre törően áttekintjük a cseh stratégiai dokumentumok releváns tartalmi elemeit, bemutatva Csehország védelmi stratégiájának pilléres szerkezetét. Ezt követően bemutatjuk a kiberbiztonsággal kapcsolatos stratégiai irányokat, a kormányzati irányítási struktúra szerkezetét, a cseh kiberbiztonsági rendszer működési

[1] Selján Péter (peter@seljan.hu) az NKE Eötvös József Kutatóközpont Stratégiai Védelmi Kutatóintézetének külső munkatársa.

[2] Security Strategy of the Czech Republic, [online] 2015. 02. Forrás: army.cz [2022. 06. 30.], 10, 13-14.

kereteit, valamint összefoglaljuk az elmúlt év fontosabb csehországi kiberbiztonsági eseményeit. Mindemellett röviden kitérünk az űrtechnológiával kapcsolatos fejlesztésekre is, mivel a fejlődő és felforgató technológiák (*emerging and disruptive technologies*) tekintetében Prága ezen a területeken is azonosít stratégiai célkitűzéseket.

Releváns stratégiai dokumentumok

A cseh stratégiai dokumentumok jellemzően megemlítik, hogy az egyre komolyabbá váló nem katonai jellegű biztonsági fenyegetések (köztük a kibertámadások) és az Európai Unió területének, illetve a NATO tagállamoknak a közvetlen szomszédságában látható romló biztonsági helyzet miatt egyre sürgetőbb kérdéssé vált Európa gyors és független reagálóképességének megteremtése/megerősítése, ami ismét felszínre hozta mind a katonai képességekben tapasztalható hiányosságok problémáját, mind a fenyegetések elhárítására való felkészültségben megmutatkozó hiányosságokat. Mindeközben pedig a globalizáció negatív hatásai, köztük például a rohamosan fejlődő információs és kommunikációs technológiákkal való visszaélések a nem állami szereplőket is lehetőségekhez juttatják. Tekintettel arra, hogy a közszféra és a magánszektor is egyre inkább rá vannak utalva az információs technológiák és a kommunikációs rendszerek alkalmazására, a kritikus információs infrastruktúrák[3] és rendszerek működési zavarainak egyre súlyosabb következményei lesznek.[4]

A vonatkozó stratégiai dokumentumokat tekintve Csehország legutóbb 2015 februárjában adott ki Biztonsági Stratégiát. Ez a korábbi, 2011-es dokumentumra épít, megőrizve annak struktúráját, valamint a követendő alapelvek és a biztonsági érdekek definícióit. Egy új stratégia kiadásakor azonban jellemzően sor került a biztonsági környezetben az előző dokumentum elfogadása óta bekövetkezett változások vizsgálatára a legutóbbi fejlemények alakulásának tükrében. A 2015-ös biztonsági stratégia kiemelt fontosságúnak értékelte a NATO- és EU-tagállamokkal folytatott együttműködés fokozását, ami az ukrajnai háború 2022-es eszkalációja, illetve a tovább romló biztonsági környezet és a fokozódó fenyegetések révén még inkább felértékelődött.[5]

A biztonsági stratégia mellett 2012 után legutóbb 2017-ben adtak ki Védelmi Stratégiát, amely tartalmazza Csehország védelempolitikájának alapelveit, illetve a Cseh Köztársaság védelmének három pillérből (az állam, a fegyveres erők és az állampolgár) álló összetételének leírását.[6] A védelmi stratégiában Oroszország kiemelt fenyegetésként szerepel, tekintettel arra, hogy Moszkva a katonai erő alkalmazásától sem riadt vissza hatalmi ambícióinak elérése érdekében, és már számos alkalommal megsértette a nemzetközi jogot, illetve szerződéses nemzetközi kötelezettségeit – például a szomszédos országok területi integritásának sérthetetlenségére vonatkozó alapelveket, illetve a konkrétan Ukrajnára vonatkozó Budapesti Memorandumot. Az Oroszországi Föderáció mindemellett hibrid műveleteket is végrehajtott már NATO és EU tagországok ellen, beleértve a célzott dezinformációs kampányokat és a kibertámadásokat is.[7] Az információs hadviseléssel és a szervezett kiberbűnözéssel összefüggésben megjelenő fenyegetések valóban komoly kihívást és veszélyt jelentenek Európa biztonságára nézve, az ezirányú negatív fejlemények pedig Csehországot is érintik. Ennek eredményeképpen Prágának különösen fontos érdeke, hogy fokozza az ország védelmi képességeit és növelje felkészültségét, valamint, hogy kivegye részét szövetségeseinek és partnerországainak a támogatásából.[8]

2019-ben adta ki a cseh Ipari és Kereskedelmi Minisztérium a Nemzeti Mesterséges Intelligencia Stratégiát (NAIS)[9], melynek fő célkitűzése a mesterséges intelligenciával kapcsolatos kutatások és fejlesztések

[3] „Azok az infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikusinfrastruktúra-elemek, továbbá a kritikus infrastruktúra elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése a kritikus infrastruktúrákat vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené.” Krasznay Csaba – Muha Lajos: Az elektronikus információs rendszerek biztonságának menedzselése. Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, Budapest, 2022, 119.
[4] Security Strategy of the Czech Republic, i.m., 11.
[5] Uo.
[6] Defence Strategy of the Czech Republic, [online] 2017. 04. Forrás: army.cz [2022. 06. 30.]
[7] Defence Strategy of the Czech Republic, i.m., 7. o.
[8] Uo.
[9] National Artificial Intelligence Strategy of the Czech Republic, [online], 2019. Forrás: mpo.cz [2022. 07. 29.]

összefogásának támogatása, különös tekintettel egy digitális innovációs európai kiválósági központ kialakítására. A stratégia mindemellett megemlíti, hogy a mesterséges intelligenciával foglalkozó központok között globális szintű együttműködésre kell törekedni, megőrizve a hazai intellektuális potenciált, valamint egyszerűbbé és vonzóbbá téve a külföldi tehetségek számára a csehországi munkavégzést a kutatások finanszírozásának biztosításával, start-upok, illetve a kis- és magánvállalkozások indításának elősegítésével és támogatásával, a fejlődésükhöz és az innovációhoz szükséges erőforrások biztosításával.

A legfrissebb releváns stratégiai dokumentumoknak a cseh Nemzeti Űrterv 2020-2025[10], a Nemzeti Kiberbiztonsági Stratégia 2021-2025[11], és a hozzá tartozó Akcióterv[12], valamint a Hibrid Beavatkozások Elleni Fellépésről szóló Stratégia[13] tekinthetők. Ugyanakkor megemlítendő még a megújításra váró Kibervédelmi Stratégia 2018-2022[14] is, mely szerint Csehország a kibervédelmet önálló területként fogja fel a kiberbiztonságon belül, és azon országok közé tartozik, melyek nyilvánosan is kijelentették, hogy offenzív kiberképességek kifejlesztésén dolgoznak.[15]

A NATO tallinni Kibervédelmi Kiválósági Központjának (*Cooperative Cyber Defence Centre of Excellence*, CCDCoE)[16] működésében szerepet vállaló tagállamokról készült országjelentések alapján egészen megbízható képet kaphatunk az adott ország kiberbiztonsági kormányzati struktúrájáról és annak működéséről. Ezek ugyanis felvázolják a kormányzati szervezetek, ügynökségek és hivatalok közötti szerepmegosztást, ismertetik a feladatköreiket, kompetenciáikat, és leírják a közöttük lévő koordináció kereteit. Így a jelentések kiterjednek a politikai és a stratégiai menedzsment kérdéseire, a kiberbiztonsági műveleti képességekre és az incidenskezelésre, a katonai kibervédelemre, továbbá a válságkezelés és megelőzés kiberbiztonsági aspektusaira. Bemutatják tehát az adott ország digitális ökoszisztémáját és összefoglalják a Nemzeti Kiberbiztonsági Stratégiában foglalt célokat, tágabb kontextusba helyezve a szervezeti megközelítés kialakítását.[17]

Csehország esetében a legutóbbi ilyen országjelentés már elavultnak tekinthető, hiszen azóta már megjelentek a jelentés kiadásakor még csak előkészítés alatt álló új stratégiai dokumentumok, az ugyanakkor világosan kiolvasható belőle, hogy milyen releváns adottságokkal rendelkezik Csehország, illetve, hogy vezető szerepet szeretne elérni a kiberbiztonság területén a közép-európai régióban a szakértelem és a tudásfelhalmozás tekintetében is. A cseh kiberbiztonsági stratégia végrehajtásának folyamatát hathavonta felülvizsgálják, melynek keretében egy munkacsoport külön-külön értékeli az egyes feladatok végrehajtásának szintjét, majd szükség szerint ajánlásokat tesz az akcióterv módosítására. A stratégia végrehajtásáról készült jelentést pedig csatolják az évente kiadott Kiberbiztonsági Jelentéshez, melyből a legutóbbi, a 2021-es jelentés épp 2022 nyarán készült el.[18] A stratégia végrehajtásáról készülő jelentés a

[10] National Space Plan 2020-2025 (NSP), [online] Forrás: czechspaceportal.cz [2022. 06. 30.]
[11] National Cyber Security Strategy of the Czech Republic 2021-2025, [online] 2021. 03. 18. Forrás: nukib.cz [2022. 06. 30.]
[12] Action Plan for the National Cybersecurity Strategy of the Czech Republic from 2021 to 2025 (AP), [online] 2022. 11. 22. Forrás: nukib.cz [2022. 06. 30.]
[13] National Strategy for Countering Hybrid Interference of the Czech Republic, [online] 2021. Forrás: army.cz [2022. 06. 30.]
[14] Cyber Defence Strategy of the Czech Republic 2018-2022, [online] 2018. Forrás: vzcr.cz [2022. 07. 17.]
[15] Az államok jellemzően nem vállalják fel nyilvánosan az offenzív kiberképességeiket, az ezirányú fejlesztéseikről pedig nem árulnak el részleteket, ezért erre vonatkozóan nem állnak rendelkezésünkre pontos adatok. Azonban megjegyzendő, hogy az offenzív kiberképességek nem csupán a támadási képességek meglétét vagy azok alkalmazását jelentik, hiszen egy kibertámadás végrehajtása előtt – és annak sikerességének biztosítása érdekében – számos egyéb tevékenységet is végre kell hajtani. Kovács László szerint az offenzív kiberképességek három területre oszthatók: 1. információszerző és feldolgozó képesség; 2. a kibertámadási képesség; 3. a hatások értékelésének képessége. Kovács László: Offenzív kiberműveletek 1.: Az offenzív kiberműveletek természete. *Hadmérnök*, 16. évf., 2021/2, 190-194.
[16] A NATO Kooperatív Kibervédelmi Kiválósági Központja egy 2008 májusában létrehozott, kutatásra, oktatásra és gyakorlatokra koncentráló, NATO által akkreditált, a Szövetség teljesjogú szervezeteként működő kibervédelmi központ. Működésében 27 tagállam vesz részt szponzoráló nemzetként, további 5 állam pedig közreműködő résztvevőként. Bővebben lásd: a Központ hivatalos oldalát. Magyarország 2010-ben a nyolcadik szponzoráló nemzetként kapcsolódott be a Kibervédelmi Kiválósági Központ munkájába. Hungary joins the Centre, [online], 2010. 06. 23. Forrás: ccdcoe.org [2022. 07. 28.]
[17] Tomáš Minárik: National Cyber Security Organisation: CZECHIA, [online] 2019. Forrás: ccdcoe.org [2022. 07. 28.]
[18] 2021 Report on Cyber Security in the Czech Republic, [online], 2022. 07. 01. Forrás: nukib.cz [2022. 07. 29.]

nyilvánosság számára nem elérhető. A szakértők szerint azonban az eddigi tapasztalatok alapján a cseh kiberbiztonsági stratégiába foglalt célok végrehajtásának folyamata kielégítőnek tekinthető.[19]

A védelem pillérei

Csehország Védelmi Stratégiája kimondja, hogy az ország védelmének három pillére az állam, a fegyveres erők és az állampolgárok. Az első pillérnek részét képezi a védelmi ipar, amely egyúttal a cseh nemzeti biztonsági struktúrának is az egyik sarokköve. A cseh kormány állami vállalatokon keresztül is igyekszik támogatni a kiemelt fontosságú, pótolhatatlan képességeket az ipari termelés és a kutatás-fejlesztés vonatkozásában. Ebben a tekintetben a kormány biztosítja a cseh fegyveres erők folyamatos fejlődését azokon a területeken, ahol a fejlesztés valóban megvalósítható. Csehország fegyverkezési és védelmi ipari fejlesztési támogatási stratégiája részleteiben határozza meg a terület feladatait, a legutóbbi fejlesztési koncepció[20] pedig 2030-ig kijelöli a fegyveres erők fejlesztésének irányait.

A cseh biztonsági struktúra első pillérének a regionális együttműködés is fontos része. Ennek keretében a cseh kormány támogatja a bilaterális és multilaterális védelmi együttműködés fejlesztését, különösen a szomszédos országokkal, és aktívan közreműködik az ezirányú erőfeszítésekben. A regionális együttműködésnek kiemelt részét képezi a Németországgal ápolt kapcsolat és a Visegrádi Együttműködés is, melynek keretében folyamatos a katonai együttműködés.[21]

A második pillért a fegyveres erők adják, melynek alapeleme a személyi állomány. Csehországnak ezért kiemelt célja, hogy a fegyveres erők sorai motivált, jól képzett, mindenre felkészült és jól felszerelt katonákkal legyenek feltöltve. Ehhez pedig a kormány igyekszik biztosítani a szükséges feltételeket, beleértve az oktatást, a kiképzést és az egyéb felkészítést. Ugyancsak a második pillér részét képezi a megfelelő felszerelés és fegyverzet biztosítása; a kitűzött célok és katonai ambíciók eléréséhez szükséges szervezeti struktúrák, képességek és kapacitások; a szövetségi együttműködés keretei; a kiberbiztonsági és kibervédelmi képességek aktív fejlesztése; valamint szükség esetén a fegyveres erők katasztrófavédelmi közreműködése.[22]

Csehország védelmének harmadik pillére az állampolgári honvédelmi kötelezettség, amit az önkéntes haderő kialakításakor sem töröltek el, így a mai napig érvényben van, a mindenkori kormány pedig igyekszik felhívni az állampolgárok figyelmét arra, hogy milyen fontos a személyes felelősségük a haza védelme érdekében. Jelenleg az erre vonatkozó felkészülés önkéntes alapon zajlik, és a védelmi szolgálat csupán veszélyhelyzet vagy hadiállapot esetén válik kötelezővé, a cseh fegyveres erők szervezeti struktúrájának háborús helyzetre történő átállásával párhuzamosan. Az erre való felkészülést hivatott biztosítani békeidőben az Aktív Tartalékos Erő. Mindemellett az ország védelméhez az állampolgárok az önkéntes tevékenységeik révén is nagymértékben hozzájárulhatnak, például a fegyverhasználathoz kapcsolódó tudás és gyakorlat – hatályos jogszabályok által rögzített keretek közötti –, vagy az elsősegélynyújtásban és az egészségügyi ellátásban megszerzett jártasság elsajátításával.[23]

Fókuszban a kiberbiztonság

Csehország arra törekszik, hogy jobban megértse és átlássa az új biztonsági fenyegetéseket, miközben igyekszik fokozni ellenálló képességét és harci képességeit. A cseh Kiberbiztonsági Stratégia külön kiemeli, hogy a biztonsági környezet alapvető változásokon megy keresztül, amit a modern technológiák rohamos fejlődése is gyorsít. A mesterséges intelligencia, a kvantumtechnológia, és az egyéb újonnan megjelenő technológiai fejlesztések a kiberbiztonság területén is paradigmaváltáshoz fognak vezetni. Mindeközben azonban azzal is számolni kell, hogy még tovább fog fokozódni az államok és a társadalmak modern technológiáktól való függősége, így a támadók lehetőségei is ki fognak szélesedni.[24]

[19] MINÁRIK: National Cyber Security Organisation: CZECHIA, i.m., 10.
[20] The Czech Armed Forces Development Concept 2030, [online], 2019. 10. 31. Forrás: army.cz [2022. 07. 25.]
[21] Defence Strategy of the Czech Republic, i.m., 11.
[22] Defence Strategy of the Czech Republic, i.m., 11-13.
[23] Uo. 14.
[24] National Cyber Security Strategy of the Czech Republic 2021-2025, i.m., 14.

Csehország lakossága 10,7 millió fő, melyből az internethasználók száma meghaladja a 9,3 milliót, ami közel 88 százalékot jelenti. A National Cyber Security Indexben Görögország, Litvánia, Belgium és Észtország után 2020-ban az 5. helyen rangsorolták, megelőzve a 6. helyen szereplő Németországot.[25] A Global Cybersecurity Indexben pedig a 68. helyen végzett,[26] habár a nemzetközi felmérésekkel kapcsolatban mindig érdemes szem előtt tartani, hogy azok többnyire változó módszertannal és széles skálán mozgó források alapján készülnek.

Csehország három kategóriába sorolja a biztonsági érdekeit, így azok fontossága szerint megkülönböztet *létfontosságú*, *stratégiai* és *fontos* érdekeket. A regionális együttműködés támogatása és fejlesztése, valamint az ország kiberbiztonságának és védelmének szavatolása Csehország stratégiai érdekei közé tartozik, míg az új technológiákra fókuszáló tudományos kutatások és fejlesztések fontos érdekként szerepelnek.[27]

Amióta 2016-ban a kiberteret is hadműveleti térnek nyilvánították[28], a NATO-tagállamok is egyre komolyabb forrásokat fordítanak erre a területre a katonai költségvetésükből, és ennek megfelelően a fejlődés üteme is egyre gyorsabb. Az állami szereplők számára az egyik legnagyobb kihívás a folyamatosan változó biztonsági környezethez történő alkalmazkodáshoz szükséges képességek kialakítása és fenntartása annak érdekében, hogy szembe tudjanak nézni a jelenlegi és a jövőben várható kiberbiztonsági fenyegetésekkel.

Az elmúlt években jellemzővé vált, hogy az állami szereplők a kiberteret is igénybe veszik a külpolitikai érdekeik érvényesítésére, és ennek a trendnek Csehország is áldozatául esett, hiszen számos alkalommal volt már például orosz és kínai „kiber kémkedés" célpontja is.[29] Mindemellett azonban gyakorlatilag folyamatosan zajlanak állami és nem állami szereplők által végrehajtott offenzív kiberműveletek is.

A kormányzati irányítási struktúra

Csehország igyekszik proaktívan és határozottan fellépni a kiberbiztonsági fenyegetésekkel szemben, melynek része a korai észlelés, a szakértői elemzés és a megfelelő ellenintézkedések megtétele. Ellenálló képességének növelése érdekében az elrettentési koncepció alkalmazására törekszik. Ebben a tekintetben a Kiberbiztonsági Stratégia megjegyzi, hogy komoly kihívást jelent az egyes kibertámadások végrehajtása mögött álló szereplők kilétének pontos azonosítása (attribúciója), hiszen enélkül nem lehet azokra megfelelő választ adni, a kibertér sajátosságai miatt azonban jellemzően nehéz ezt a beazonosítást minden kétséget kizáróan elvégezni.[30]

A cseh kormány a kritikus infrastruktúrák és információs rendszerek védelmét a Nemzeti Kiber- és Információbiztonsági Ügynökség (NCISA)[31] 2017-ben létrehozott reagáló csoportjának (*Computer Emergency Response Team* – CERT) segítségével látja el. Maga az ügynökség koordináló szerepet is betölt egy kiberbiztonsági vészhelyzet esetén[32], de feladata többek között a megelőzés, a fenyegetések és a kockázatok felmérése és elemzése, valamint az oktatásban és képzésekben való részvétel is.

2021 júliusában lépett hatályba a katonai hírszerzésről szóló törvény módosítása, amely a katonai hírszerzést határozta meg a kibervédelemért felelős nemzetbiztonsági szervként, melynek keretein belül

[25] National Cyber Security Index (NCSI), [online], 2020. Forrás: ncsi.ega.ee [2022. 07. 28.]
[26] Global Cybersecurity Index, [online], 2020. Forrás: itu.int [2022. 07. 28.]
[27] Security Strategy of the Czech Republic, i.m., 8-9.
[28] Cyber Defence Pledge, [online] 2016. 07. 08. Forrás: nato.int [2022. 07. 17.]
[29] Catalin CIMPANU: Czech authorities dismantle alleged Russian cyber-espionage network, [online], 2019. 10. 22. Forrás: zdnet.com [2022. 10. 04.]; Czech National Cyber Security Agency Warns of Cyber Attacks Connected To War In Ukraine, [online], 2022. 04. 20. Forrás: brnodaily.com [2022. 10. 04.]
[30] National Cyber Security Strategy of the Czech Republic 2021-2025, i.m., 13.
[31] Csehországban a Nemzeti Kiber- és Információbiztonsági Ügynökség (*National Cyber and Information Security Agency* – NCISA) a kiberbiztonság központi igazgatási szerve, mely felel az információs és kommunikációs rendszerekben található minősített információk védelméért is. Bővebben lásd: a Központ honlapját. [online], 2022. 04. 20. Forrás: nukib.cz [2022. 10. 04.]
[32] A cseh kiberbiztonsági törvény lehetőséget ad úgynevezett „kiberbiztonsági vészhelyzet" vagy „kibervészhelyzet" kihirdetésére, amennyiben a nemzeti érdekeket nagymértékben veszélyezteti egy információs biztonsági fenyegetés, vagy az elektronikai kommunikációs szolgáltatások fenyegetettsége. Cyber Security Act (ACT No 181/2014 Coll.), Chapter III, Section 21, [online], 2014. 07. 23. Forrás: nukib.cz [2022. 08. 07.]

működik az Országos Kiberműveletek Központja. Ennek a központnak a feladata, hogy hatékony kibervédelmi rendszert fejlesszen a kibertámadások kivédése és megállítása érdekében, biztosítva ezáltal a civilek és az infrastruktúra védelmét.

2019-ben a haderő hozta létre a Kibererők Parancsnokságát (VeKySIO)[33], amely a kiberműveletekhez fejleszt képességeket. Ezt követően a kiberbiztonsági incidensekre reagálni hivatott központ (*Computer Incident Response Capability Center* – CIRC)[34] 2022-ben a VeKySIO alárendeltségébe került, és jelenleg is felelős a kiberbiztonsági fenyegetések és incidensek proaktív azonosításáért a Honvédelmi Minisztérium adathálózatainak folyamatos felügyeletén keresztül, valamint feladata továbbá a fenyegetések és támadások elemzése, értékelése és jelentése is az érintett partnerek felé. A cseh hadsereg kibervédelemmel foglalkozó parancsnoksága nem fejleszt támadóképességeket, szerepe csak támogató, amikor nem került sor rendkívüli vagy hadiállapot kihirdetésére.

Széleskörű kiberbiztonsági együttműködés

A modern technológiák alkalmazása mára már megkerülhetetlen része lett az életünknek, és az államok is egyre jobban függenek a kibertér biztonságos működésétől. A társadalmak fokozatos „digitalizálódása" azonban mindeközben egyre komolyabb kihívás elé állítja a kiberbiztonsággal foglalkozó szakembereket. Ennek megfelelően a Cseh Köztásaság kiberbiztonsági szemlélete valamennyi érintett szereplő együttműködésének szükségességére épül, az országos és a nemzetközi szinteket is beleértve. A kiberbiztonság területének jelentőségét többek között az adja, hogy kiemelt fontosságú a kritikus infrastruktúrák és egyéb hálózatok és rendszerek védelme szempontjából.[35]

Csehország tehát egy komplex kiberbiztonsági rendszert dolgozott ki és működtet, valamennyi érintett intézményt és szereplőt bevonva, melyek számára világos feladatköröket határoztak meg. A cseh kiberbiztonsági stratégia kiemeli, hogy minden intézménynek, magáncégnek és állampolgárnak megvan a maga szerepe a kiberbiztonság szavatolásában. Mindemellett a kibertér védelméhez elengedhetetlen a civil–katonai együttműködés is, melynek érdekében a cseh nemzeti védelmi koncepcióban szerepel a fegyveres erők és a polgári lakosság, illetve civil társadalom közötti kölcsönös támogatás szükségessége is.[36]

A Cseh Köztársaság támogatja olyan rendszerek fejlesztését, amelyek lehetővé teszik valamennyi érintett szereplő széleskörű együttműködését, beleértve a közszférán kívüli szereplőket is, akik hozzájárulhatnak a kiberbiztonsági incidensekkel kapcsolatos országos és nemzetközi tapasztalatcseréhez. Csehország előnyben részesíti a rugalmas ellenállású rendszereket, amelyek egyszerre képesek mérsékelni a kibertámadások hatásait, valamint gyorsan helyreállítani a rendszer működőképességét. Prága mindemellett támogatja a kiber- és információbiztonsággal kapcsolatos lakossági figyelemfelkeltő kampányokat is, mivel ők tekinthetők a rendszer legsebezhetőbb elemének, továbbá aktívan hozzájárul a kiberfenyegetések elleni intézkedések kidolgozásához olyan nemzetközi szervezeteken belül, mint az EU és a NATO.[37]

Csehország komoly előrehaladást ért el a kiberbiztonsági gyakorlatok[38] terén, melyek az elmúlt években a szervezeti struktúra sarokköveivé váltak.[39] 2019-ben a kormányzati, ipari és akadémiai tagokból álló cseh kiberbiztonsági csoportok sikeresen vettek részt nagyszabású nemzetközi gyakorlatokon, mint például a Locked Shields, a Cyber Coalition, CMX és a Cyber Europe. A kiberbiztonsági ügynökség pedig

[33] A Kibernetikai és Információs Erők biztosítják Csehország biztonságát és védelmét a kibertérben és az információs műveletek terén. Képesek akár önállóan, akár belföldi vagy szövetséges keretek között is tevékenykedni, a szárazföldi, légi és különleges erőkkel szorosan együttműködve. Harcászati szinten felügyelik, tervezik és irányítják a kiber- és információs műveleteket. Bővebben lásd: a Cyber Forces Command hivatalos oldalát. [online], 2022. 04. 20. Forrás: Armiy.cz [2022. 10. 04.]
[34] Bővebben lásd: a Központ honlapját. [online], 2022. 04. 20. Forrás: circ.army.cz [2022. 10. 04.]
[35] National Cyber Security Strategy of the Czech Republic 2021-2025, i.m., 3.
[36] Uo. 7-10.
[37] Security Strategy of the Czech Republic, i.m., 18-19.
[38] Bővebben lásd: a cseh kiberbiztonsági ügynökség honlapján. [online], 2020. 08. 08. Forrás: nukib.cz [2022. 08. 08.].
[39] Helen WARRELL: Czech Republic turns to war-games to build cyber defences, [online], 2021. 02. 18. Forrás: ft.com [2022. 07. 30.]

külföldre is képes volt egyéni gyakorlatokat összeállítani, például az amerikai Kongresszus, az Afrikai Unió országai és a Nyugat-Balkán nemzeti hatóságai számára.[40]

A kormányzat és a magánszektor közötti együttműködés – például egyetemekkel, bankokkal és más intézményekkel – sokáig elsősorban informális alapú volt, ugyanakkor azóta kibővült, és a hosszútávú bizalomerősítő lépések révén is pozitívnak bizonyult. A 2015-ben hatályba lépett kiberbiztonsági törvény már formális kötelezettségeket rótt a magánszektorra, így például kötelezővé tette az incidensek bejelentését, egy kiberbiztonsági vészhelyzet esetén pedig a magánszektor szereplőinek is kötelessége bizonyos kormányzati utasításokat végrehajtani annak elhárítása érdekében.[41]

A cseh Nemzeti Kiber- és Információbiztonsági Ügynökség és az amerikai Microsoft között együttműködési megállapodás jött létre 2015-ben, melynek keretében lehetővé vált az információmegosztás a felek között, valamint a prágai Nemzetbiztonsági Hatóság hozzáférést kapott a Microsoft termékeinek forráskódjához és egyéb dokumentációkhoz is.[42] Emellett 2017-ben hasonló együttműködési megállapodás született a cseh kormányzat és a Cisco között is a legutóbbi kiberbiztonsági trendekkel és fenyegetésekkel kapcsolatos kölcsönös információmegosztásról.[43]

Csehországnak hasznára válik az Európai Unióval fenntartott szoros együttműködés is, többek között például a kritikus infrastruktúrák védelme és a kiberbiztonság területén. A nemzetközi szervezetekben való részvétel mellett Csehország a biztonsági érdekeit kétoldalú kapcsolatok megerősítésén keresztül is igyekszik képviselni, különös tekintettel a vele szomszédos államokra, beleértve a Visegrádi Együttműködés országait is.[44]

Mindezek mellett a Biztonsági Stratégia hangsúlyozza, hogy a NATO és az EU jóvoltából megvalósuló, a stratégiai képességek fejlesztését szolgáló közös eszközbeszerzési és fegyverkezési programok olyan képességeket tesznek elérhetővé Csehország számára, melyek máshogy elérhetetlenek lennének. Csehország stratégiai partnerséget ápol az Egyesült Államokkal, és több regionális és kétoldalú együttműködési projektben is részt vesz, a nemzetközi szervezetekben való tagsága mellett. Ezeknek a projekteknek köszönhetően könnyebb az eszközök karbantartása, hatékonyabb a képességfejlesztés, és javul a katonai interoperabilitás is.[45]

Az elmúlt év kiberbiztonsági eseményei Csehországban

A cseh Nemzeti Kiber- és Információbiztonsági Ügynökség legutóbb 2022 nyarán adta ki éves jelentését a legutóbbi év kiberbiztonsági eseményeiről.[46] Már ennek vezetői összefoglalója is rámutat, hogy 2021-ben Csehországban növekedés volt tapasztalható a rosszindulatú kibertevékenységek terén, emelkedett a regisztrált kiberbiztonsági incidensek száma, és a rendőrség szerint a kiberbűnözők által végrehajtott bűncselekmények is növekvő trendet mutatnak.

Míg 2020-ban 99 incidenst, addig 2020-ban már 157 kiberbiztonsági eseményt jelentettek a releváns szerveknek, 2021-ben pedig a leggyakrabban előforduló támadás típus szerint az adathalászat (*phishing*), az e-mailes csalás (*scam mail*), és a külső hálózatok szkennelése (*external network scanning*) volt. A legkomolyabb kiberfenyegetések között szerepeltek újonnan publikált sérülékenységek, zsaroló programok és adathalász támadások is. A cseh intézményeket és vállalatokat elsősorban a ProxyLogon[47] (21

[40] MINÁRIK: National Cyber Security Organisation: CZECHIA, i.m., 11.
[41] Cyber Security Act (ACT No 181/2014 Coll.), Chapter III, Sections 8 and 11, [online], 2014. 07. 23. Forrás: nukib.cz [2022. 08. 07.]
[42] NSA and Microsoft have signed a crucial agreement on information sharing and exchange, [online], 2015. 04. 08. Forrás: govcert.cz [2022. 08. 07.]
[43] Národní úřad pro kybernetickou a informační bezpečnost ČR spolupracuje se společností Cisco na vyšší bezpečnosti, [online], 2017. Forrás: cisco.com [2022. 08. 07.]
[44] Security Strategy of the Czech Republic, i.m., 16.
[45] Uo. 23.
[46] 2021 Report on Cyber Security in the Czech Republic, [online], 2022. Forrás: nukib.cz [2022. 08. 07.] 6.
[47] Elizabeth MONTALBANO: Espionage Group Wields Steganographic Backdoor Against Govs, Stock Exchange, [online], 2022. 09. 29. Forrás: darkreading.com [2022. 10. 04.]; Alex SCROXTON: Microsoft Exchange ProxyLogon attacks spike 10 times in four days, [online], 2021. 03. 15. Forrás: computerweekly.com [2022. 10. 04.]

incidens), ProxyShell[48] (5 incidens) és a Log4Shell[49] (2 incidens) sérülékenységek kihasználásán alapuló támadások érintették, melyek együttesen a cseh kiberbiztonsági intézet által regisztrált incidensek ötödéért feleltek. A zsarolóprogramok közül pedig a RaaS[50] (*ransomware-as-a-service*) előfordulása volt a leggyakoribb. Mindemellett az adathalászat évről évre előkelő helyen végez az éves jelentésekben, ráadásul az ilyen típusú támadások is folyamatosan fejlődnek és egyre kifinomultabbá válnak.

A Nemzeti Kiber- és Információbiztonsági Ügynökség a külügyminisztériummal és a cseh kormánnyal együttműködve 2021-ben harmadszorra szervezte meg a prágai 5G biztonsági konferenciát, amely az 5G hálózat és a forradalmi technológiákkal kapcsolatos biztonsági kérdésekre fókuszált, záróakkordjaként pedig a Nemzeti Kiber- és Információbiztonsági Ügynökség (NCISA) bemutatta a forradalmi technológiák kiberbiztonsági kérdéseivel kapcsolatos javaslatait.[51] A prágai javaslatokat összefoglaló dokumentum előszava emlékeztet rá, hogy a vezeték nélküli 5G hálózati infrastruktúra alkotja majd a digitális gazdaság gerincét, ami sokkal gyorsabb és nagyon alacsony látenciájú összeköttetéseket tesz majd lehetővé. Mindemellett a forradalmi technológiákban rejlő lehetőségek kiaknázásában is fontos szerepet fog majd betölteni, így a mesterséges intelligencia, a kvantum kommunikációs infrastruktúra, az adatelemzés vagy az autonóm rendszerek működésének terén. Ezek a technológiák jelentős hatással lesznek majd a nemzet biztonsága szempontjából kiemelt fontosságú ágazatok (energiaipar, bankrendszer, egészségügyi rendszer, kormányzati szervek) működésére. Mindeközben azonban a modern társadalmi berendezkedés egyre inkább rá lesz utalva ezeknek a technológiáknak a működésére, ami komoly biztonsági kockázatot hordoz magában.[52] Éppen ezért, Prága szerint kiemelt fontosságú a biztonságos és megbízható – például külföldi kormányok vagy pártok befolyásától mentes –, valamint átláthatóan működő és diverzifikált ellátási láncok kialakítása, a forradalmi technológiák alkalmazása során pedig a demokratikus értékek, az emberi jogok érvényesülésének és az etikai előírások betartásának szem előtt tartása.[53]

A 2021-es év folyamán az NCISA folytatta a közszolgálati dolgozók kiberbiztonsági felkészítését is, melynek eredményeként már több mint 26500 felhasználó teljesítette a vonatkozó e-learning kurzusokat (Get Cyber Skilled!, Manage Cyberspace!), valamint több mint 2800-an végezték el a biztonságos internethasználattal kapcsolatos (Stay Safe in Cyberspace!) képzést. A tavalyi évben nagyobb figyelmet igyekeztek szentelni a kórházi dolgozók felkészítésére, ezért a számukra külön e-learning kurzust is indítottak (Cyber Hospital!), melyen több mint 4400 dolgozó vett részt.

2021-ben újra megtarthatóvá váltak a kiberbiztonsági gyakorlatok személyesen is, így összesen 14 gyakorlatot rendeztek országos és nemzetközi szinten, melyek közül kiemelendő az első, az egészségügyi szektor számára megrendezett gyakorlat (Health Czech). A Csehországot képviselő csapat a harmadik helyet szerezte meg a Locked Shields 2021-es gyakorlatán.[54]

Űrtechnológia

A forradalmi technológiák kapcsán egy másik kiemelten fontos terület az űrtechnológia fejlesztése. Az űrtechnológiát illetően a Cseh Köztársaság igyekszik folyamatosan fejleszteni képességeit, stratégiáját és

[48] Kelly Sheridan: CISA Warns of Ongoing Attacks Targeting ProxyShell Vulnerabilities, [online], 2021. 08. 24. Forrás: darkreading.com [2022. 10. 04.]
[49] Andreas Berger: What is Log4Shell? The Log4j vulnerability explained (and what tod o about it), [online], 2021. 12. 17. Forrás: dynatrace.com [2022. 10. 10.]; Alert (AA21-356A), Mitigating Log4Shell and Other Log4j-Related Vulnerabilities, [online], 2021. 12. 22. Forrás: cisa.gov [2022. 10. 10.]
[50] Kurt Baker: Ransomware as a Service (RaaS) Explained, [online], 2022. 02. 07. Forrás: crowdstrike.com [2022. 10. 10.]
[51] The Prague Proposals, [online], 2021. 12. 01. Forrás: nukib.cz [2022. 08. 07.]
[52] Az 5G technológiát illetően a Nemzeti Kiber- és Információbiztonsági Ügynökség 2018 decemberében potenciális nemzeti biztonsági fenyegetésnek minősítette a Huawei-t, kiszorítva ezzel a kínai vállalatot a csehországi 5G infrastruktúra-fejlesztési projektekből. Az Egyesült Államok az 5G technológiát és az azzal kapcsolatos fejlesztéseket nemzeti biztonsági kérdésnek tekinti, és igyekszik korlátozni a kínai vállalatok, elsősorban pedig a Huawei szerepét ezen a területen, különösen a vele szoros szövetséges kapcsolatokat ápoló országokban. A Huawei-jel szembeni cseh lépés így Prága nyugati re-orientációjának megerősítését is jelezte. Marc Santora – Hana de Goeij: Huawei Was a Czech Favorite. Now? It's a National Security Threat, [online], 2019. 02. 12. Forrás: nytimes.com [2022. 10. 08.]
[53] The Prague Proposals, i.m., 1, 4-6.
[54] Sweden Scored Highest at the Cyber Defence Exercise Locked Shields 2021, [online], 2021. Forrás: ccdcoe.org [2022. 08. 08.]

doktrínáit. A jelentős állami és magán tőkebefektetéseknek köszönhetően a cseh űripar gyorsan fejlődik.[55] Prágában található az Európai Unió Űrprogram Ügynöksége (*EU Space Program Agency* – EUSPA)[56], amely többek között a Galileo navigációs rendszer biztonságáért is felel.[57] Emellett 2021 nyarán az Európai Űrügynökség (*European Space Agency* – ESA) ajánlásával támogatta Csehország egyik űrkutatási projektjét (*Space Laboratory for Advanced Variable Instruments and Applications* – SLAVIA), amely nyersanyagok aszteroidákból történő kivonásának lehetőségeit hivatott vizsgálni.[58]

Az űrrel kapcsolatos tevékenységek nagy részét a Közlekedési Minisztérium felügyeli. Cseh cégek dolgoznak a Meteosat[59] és a Galileo[60] műholdak hardverén, például a hűtéssel kapcsolatos különféle megoldásokon, optikai eszközökön, a szükséges mikroelektronikai elemek egyes részein, de a műholdakat vezérlő szoftvereken is. Csehország több mint harminc ESA-misszióban vesz részt, és vannak olyan vállalatai, amelyek közreműködnek az Arianespace által az ESA számára kifejlesztett és üzemeltetett európai hordozórakéták alkatrészeinek gyártásában. A Cseh Űrkutatási Központ (VZLÚ) részt vesz rakétatesztelési projektekben, és már negyedik éve sikeresen üzemelteti saját VZLUSAT-1 műholdját, miközben már dolgozik egy második generációs műholdon is.[61]

A Cseh Köztársaság számos, az űrtechnológia békés alkalmazására összpontosító, teljes mértékben polgári projektek mellett a világűr katonai felhasználásával kapcsolatos programokat is működtet. A Cseh Köztársaság Műholdközpontját (CZE SATCEN)[62] – a katonai hírszerzés vezetésével – 2020-ban alapították a NATO-kötelezettség részeként, és videó közvetítést kínál katonai és polgári államigazgatási hatóságok számára. Emellett vannak még más említésre méltó katonai hírszerzési projektek is Csehországban, mint például a GOLEM katonai műhold, ami várhatóan 2025-re lesz kész, és lehetővé teszi majd az érdeklődésre számot tartó földrajzi területek folyamatos megfigyelését teljes egészében cseh eszközökkel.[63] Ehhez kapcsolódik a STRATOM stratégiai képalkotó rendszer is.

Összegzés

A romló nemzetközi biztonsági környezet miatt egyre sürgetőbbé válik az Európai Unió tagállamainak felkészültségében megmutatkozó hiányosságok kérdése mellett a gyors és független reagálóképesség fejlesztése is, miközben a kiberbiztonság is egyre fontosabb része a nemzetközi biztonságnak. Hiszen a kiberbiztonsági kihívásokkal gyakorlatilag csak szoros és hatékony kétoldalú, illetve minél szélesebb körű nemzetközi együttműködéssel lehet felvenni a versenyt: civilek és katonák, a közszféra és a magánszektor, valamint az akadémiai szereplők között is szükségessé teszik a szoros együttműködést.[64]

A nemzetközi együttműködés fontosságát szem előtt tartva Csehország stratégiai partnerséget ápol az Egyesült Államokkal, melynek keretében 2015-ben együttműködési megállapodás jött létre a cseh Nemzeti Kiber- és Információbiztonsági Ügynökség és az amerikai Microsoft között, lehetővé téve a felek között a kiberbiztonsági információmegosztást. Emellett hasonló együttműködési megállapodás született a cseh

[55] National Space Plan (2020-2025). [online] 2020 Forrás: czechspaceportal.cz [2022. 06. 30.], 4-8.
[56] Bővebben lásd: az EUSPA hivatalos oldalát. [online], 2022. 10. 04. Forrás: euspa.europa.eu [2022. 10. 04.]
[57] Galileo Headquarters To Be in Prague, [online], 2010. 12. 14. Forrás: praha.eu [2022. 07. 22.]
[58] The first Czech space mission will explore mining possibilities on asteroids, [online], 2021. 07. 19. Forrás: mdcr.cz [2022. 07. 22.]; Tom McEnchroe: Czech scientists planning to create map of resources in space, [online], 2022. 01. 14. Forrás: englich.radio.cz [2022. 07. 22.]
[59] Meteosat satellites, [online]. Forrás: esa.int [2022. 07. 22.]
[60] A Galileo az EU globális navigációs műholdrendszere (*Global Navigation Satellite System*), amely az Európai Űrprogram három kiemelt programjának (Copernicus, Galileo, EGNOS) egyike. Jobb helymeghatározási és időzítési információkat biztosít, így jelentős pozitív hatással van számos európai szolgáltatásra és azok felhasználóira. Lehetővé teszi számukra, hogy a többi rendelkezésre álló rendszernél nagyobb pontossággal meg tudják határozni pontos helyzetüket, vészhelyzet esetén pedig hatékonyabb reagálást tesz lehetővé a releváns szervek számára, illetve támogatja a kutató-mentő feladatok végrehajtását. A Galileo emellett új termékek, szolgáltatások és munkahelyek teremtéséhez hozzájárulva elősegíti az európai innovációt. Bővebben lásd: The EU Space Programme, [online], 2021. 05. 11. Forrás: euspa.europa.eu [2022. 07. 22.].
[61] Bővebben lásd a Cseh Űrkutatási Központ hivatalos oldalát. [online], 2022. 10. 04. Forrás: vzlu.cz [2022. 10. 04.]
[62] Bővebben lásd a Cseh Köztársaság Műholdközpontjának hivatalos oldalát. [online], 2022. 10. 04. Forrás: vzcr.cz [2022. 10. 04.]
[63] Czech Republic will launch own satellites, [online], 2020. 01. 21. Forrás: milmag.pl [2022. 07. 22.]
[64] National Cyber Security Strategy of the Czech Republic 2021-2025, i.m., 15.

kormányzat és a Cisco között is 2017-ben, méghozzá a legutóbbi kiberbiztonsági trendekkel és fenyegetésekkel kapcsolatos kölcsönös információmegosztásról. Az ezekhez hasonló, kormányzati szervek és vezető technológiai vállalatok közötti megállapodások pedig jelentős mértékben hozzájárulhatnak az adott ország biztonságának szavatolásához.

Megjegyzendő, hogy Csehország védelmi stratégiájában Oroszország kiemelt fenyegetésként szerepel, miután Moszkva a katonai erő alkalmazásától sem riadt vissza hatalmi ambícióinak elérése érdekében. Az Oroszországi Föderáció ráadásul hibrid műveleteket is végrehajtott már az Európai Unió országai és NATO-tagállamok ellen, beleértve a célzott dezinformációs kampányokat és a kibertámadásokat is.

Az 5G minden bizonnyal a forradalmi technológiákban rejlő lehetőségek kiaknázásában is fontos szerepet fog majd betölteni, így pedig várhatóan jelentős hatással lesz a nemzeti biztonsági szempontból kiemelt fontosságú ágazatok működésére. Mindeközben azonban a modern társadalmi berendezkedés egyre inkább rá lesz utalva ezeknek a technológiáknak az alkalmazására, ami nem elhanyagolható biztonsági kockázatot hordoz magában. Ezért, Prága értékközpontú megközelítése szerint kiemelt fontosságú a biztonságos és megbízható, átláthatóan működő és diverzifikált ellátási láncok kialakítása, a forradalmi technológiák alkalmazása során pedig elengedhetetlen a demokratikus értékek, az emberi jogok érvényesülésének és az etikai előírások betartásának szem előtt tartása. Ezzel összhangban Csehország az 5G technológia fejlesztése és az ahhoz kapcsolódó infrastruktúra kiépítése kapcsán nyugati orientációt mutat, a kínai Huawei szerepvállalását pedig – biztonsági kockázatnak tekintve azt – korlátozta.

Az „SVKK Elemzések” 2003 óta a kutatóintézet munkatársainak tematikus szakpolitikai elemzéseit megjelentető időszakos kiadvány, melyben a szerzők független kutatói álláspontjukat közlik.

Kiadó: NKE Eötvös József Kutatóközpont Stratégiai Védelmi Kutatóintézet

Szerkesztés, korrektúra és tördelés:
Csiki Varga Tamás, Tálas Péter

A kiadó elérhetősége:

1581 Budapest, Pf. 15.

Tel: 00 36 1 432-90-92

E-mail: svkk@uni-nke.hu

2019– : NKE Stratégiai Védelmi Kutatóintézet Elemzések (ISSN 2063-4862)

2012–2019: NKE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4862)
2011–2012: ZMNE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4854)
2007–2011: ZMNE Stratégiai Védelmi Kutatóintézet Elemzések (ISSN 2063-4854)
2003–2007: ZMNE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4854)