

KATONAI NEMZETBIZTONSÁGI
SZOLGÁLAT

S Z A K M A I
S Z E M L E



XXIII. évfolyam 1. szám

ALAPÍTVÁ: 2003
BUDAPEST
2025

**A Katonai Nemzetbiztonsági Szolgálat
tudományos-szakmai folyóirata**

Felelős kiadó

Tajti Norbert vezérőrnagy, főigazgató

Szerkesztőbizottság

Elnök:	Tajti Norbert	vezérőrnagy
Tagok:	Dr. Farkas Ádám, PhD	alezredes
	Dr. Fürjes János Norbert, PhD	alezredes
	Dr. Kassai Károly, PhD	ezredes
	Dr. Kenedli Tamás, PhD	ezredes
	Dr. Magyar Sándor, PhD	ezredes
	Dr. Puskás Béla, PhD	ezredes
	Simon László	alezredes
	Szabó Károly	vezérőrnagy
	Tóth Csaba Mihály	ezredes
	Dr. Varga Sándor Gábor	ezredes
	Dr. Vida Csaba, PhD	ezredes
Felelős szerkesztők:	Dr. Kenedli Tamás, PhD	ezredes
	Simon László	alezredes
Olvasószerkesztő:	Tóth Csaba Mihály	ezredes
Tördelőszerkesztő:	Szabó Beatrix	

Elérhetőségeink

Postacím:	Katonai Nemzetbiztonsági Szolgálat Tudományos Tanácsa 1021 Budapest, Budakeszi út 99-101. 1502 Budapest, Pf. 117
Telefon:	Dr. Kenedli Tamás 30/738-7925 Simon László 30/999-5205
E-mail:	szakmai.szemle@knbsz.gov.hu
Weblap:	https://www.knbsz.gov.hu/hu/publikaciok.html

HU ISSN 1785-1181

TARTALOM

NEMZETBIZTONSÁG ELMÉLETE

Dr. Pál István

„Megkímélt állapotban”

A londoni magyar hírszerző rezidentúra tevékenysége és biztonsági helyzete az 1980-as évek elején.....5

BIZTONSÁG- ÉS VÉDELEMPOLITIKA

Neuspiller Ferenc

„Leggyengébb láncszemből” a NATO „déli fellegvára”

Olaszország helyzete a NATO-n belül 1975-1985.....26

TECHNIKAI RENDSZEREK

Griffiths Dániel

A kognitív számítástechnika-alapú automatizáció szükségessége a biztonsági műveleti központokban.....64

Knapp Gábor – Pozderka Gábor

A kibertéri műveletek fejlődésének áttekintő vizsgálata a megváltozott nemzetközi rendszer tükrében.....95

Kotsis Levente

Korszerű, gyors feldolgozást lehetővé tévő mesterségesintelligencia-alapú képfeldolgozási technológiák..... 106

FÓRUM

Dr. Magyar Sándor – Dr. Bányász Péter – Bányász-Váczi Kincső Boróka – Pál Anita

Magyarország Kibervédelmi Stratégiáinak összehasonlítása és fejlődési íve 2013 és 2025 között 127

Földes Tibor

A biztonság szerepe és fontossága a szövetségi kritikus infrastruktúra szabályozásának kialakításában 145

Dr. Bartkó Róbert

A bűnüldözési célú titkos információszerzés és a nemzetbiztonsági szolgálatok kapcsolata Magyarországon 164

SZERZŐINK 178

E SZÁMUNKAT LEKTORÁLTÁK 179

A PUBLIKÁLÁS FELTÉTELEI 180

NEMZETBIZTONSÁG ELMÉLETE

DR. PÁL ISTVÁN¹

„MEGKÍMÉLT ÁLLAPOTBAN”

A LONDONI MAGYAR HÍRSZERZŐ REZIDENTÚRA TEVÉKENYSÉGE ÉS BIZTONSÁGI HELYZETE AZ 1980–AS ÉVEK ELEJÉN

Az 1977-ben megtartott londoni külügyminiszeri találkozón Puja Frigyes és David Owen egyaránt problémamentesnek minősítette a Magyarország és Nagy-Britannia közötti viszonyt, ez azonban nem párosult a kétoldalú együttműködés dinamizálásával. A munkáspárti kormány folyamatosan csökkenő parlamenti többsége és választói támogatottsága mellett már nem akart hosszú távú külpolitikai elkötelezettségeket vállalni. Az 1967-es magyar-angol tudományos-technológiai egyezményt ugyan 1978-ban megújították, de a munkaterv kidolgozására már nem került sor. Az intézményesült tudományos kapcsolatok szintje alacsony maradt, az angol fél a csereprogramon kívüli kapcsolatok bővítésére törekedett.² Ezen a téren a Konzervatív Párt 1979-es választási győzelme még nem hozott automatikus áttörést, mégis elindult az a közeledés, amelynek jóvoltából 1984-re Magyarország jelentősen felértékelődött a brit külpolitikában.³ Megítélésünk szerint ezt jelentős mértékben előmozdította, hogy magyar viszonylatban egyszer sem pattant ki kémbotrány, ugyanakkor a Belügyminisztérium (BM) III/I. (Hírszerző) Csoportfőnökség részint az átszervezésre, részint a nagykövetség felújítására való tekintettel korlátozta londoni tevékenységét. A brit kormányzatban így még hangsúlyosabban az az álláspont alakult ki, hogy Magyarország – szigorúan a hidegháborús keretek közötti értelmezésben – a „lojális ellenfél”.

Kulcsszavak: magyar-angol kapcsolatok, 1980-as évek, hírszerzés, elhárítás

„IN SPARED STATE”

THE ACTIVITIES AND THE SAFETY SITUATION OF THE HUNGARIAN INTELLIGENCE RESIDENCY IN THE EARLY 1980s.

At the 1977 meeting of Foreign Ministers in London, both Frigyes Puja and David Owen described the relationship between Hungary and Britain as unproblematic, but this was not matched by a dynamism in the bilateral cooperation. The Labour government, with its steadily declining parliamentary majority and electoral support, was no longer

¹ ORCID-azonosító: 0000-0002-7388-0868

² ARDAY Lajos: *Az Egyesült Királyság és Magyarország. Nagy-Britannia és a magyar-angol kapcsolatok a 20. században.* Mundus Magyar Egyetemi Kiadó, Budapest, 2005., 171–172. o.

³ BÁTONYI, Gábor: 'Creative Ferment in Eastern Europe': Thatcher's Diplomacy and the Transformation of Hungary in the Mid-1980's. *Diplomacy & Statecraft*, 2018/4. 638–645. o.

willing to make long-term foreign policy commitments. The 1967 Hungarian-English Science and Technology Agreement was renewed in 1978, but the work schedule was not developed. The level of institutionalised scientific relations remained low, and the British side sought to expand contacts outside the exchange programme. The Conservative Party's electoral victory in 1979 did not bring an automatic breakthrough in this area, but it did initiate a rapprochement, which by 1984 had helped Hungary to gain considerable ground in British foreign policy. In our view, this was significantly facilitated by the fact that no spying scandal broke out in Britain with Hungarian involvement, while the First (Intelligence) Directorate of 3rd Main-Directorate of the Ministry of the Interior (BM) restricted its activities in London, partly due to its reorganisation and partly due to the renovation of the embassy. Thus, the British government's view that Hungary was the "loyal adversary" – strictly within the Cold War framework – became even more pronounced.

Keywords: British-Hungarian relations, the 1980's, intelligence, counter-intelligence

A rezidentúra személyzeti változásai

A londoni rezidentúra 1980-ban a BM III/1-11-es Osztály alárendeltségében működött egyetlen hivatásos tiszttel (fedőneve „Tolnai”), akinek nevét személyiségi jogi okok miatt nem közöljük. Az MNVK2 (Magyar Néphadsereg Vezérkari Főnökség 2-es Főcsoportfőnökség) londoni attaséhivatalához – a parancsnok, Mozsik Imre alezredes, Hajdú László őrnagy és Mészáros Gábor főhadnagy⁴ – mellett három tartalékos katonatiszt, azaz dr. Bánlaki György sajtóattasé, dr. Mohácsi István gazdaságpolitikai titkár és Horváth István tartozott.⁵ A brit fővárosban az emigráció ügyeivel foglalkozó követségi első titkár volt a biztonsági felelős. 1976-tól 1980-ig Szekeres Ferenc⁶ (fn. „Elek Sándor”),⁷ majd 1981-től Blahó Béla⁸ (fn. „Bozsóki”) titkos munkatárs felelt a védelemért – biztonsági tiszt kihelyezésére a vizsgált időszakban nem került sor⁹ –,

⁴ Állambiztonsági Szolgálatok Történeti Levéltára (ÁBTL) 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme–3/2–11/80. sz. jelentés – Tárgy: A londoni magyar kolónia. – London, 1980. március 17. 13.o.

⁵ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 4/2 – 2/81. sz. jelentés. – Tárgy: A biztonsági jelzőberendezés figyelése. – London, 1981. április 21. 87–88.o.

⁶ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 3/2–11/80. sz. jelentés – 67/53–890/80 – 130/416/80 – Tárgy: A londoni magyar kolónia. – London, 1980. március 17. 6.o.

⁷ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – Tárgy: Az angol rendőrség intézkedései a külképviseletek védelmére – Adta: „Elek Sándor” – Vette: Károlyi Gyula r. alez. – jelentés. Budapest, 1980. október 6. 50–52.o.

⁸ Magyar Nemzeti Levéltár Országos Levéltára (MNL OL)–XIX–J–1–j – SZT Iratok, 1981 – 26. doboz – 004390 – 9/7/1981 – Tárgy: A londoni nagykövetség konzuli osztálya vezetőjének évi beszámoló jelentése. – London, 1981. június 18. 5.o.

⁹ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 2/7.–2/82. sz. utasítás! – Tolnai elvtársnak! London. – Tárgy: Kettes vonali tevékenység fejlesztése. – Budapest, 1982. február 16. 214.o.

amelyre 1981-ben négyfős társadalmi rezidentúra alakult. Bornemissza Károlyné, a kereskedelmi kirendeltség titkárnője (fn. „Szilánk”), Gyüszü János konzulátusi ügyfélfogadó (fn. „Gyimesi Lajos”), Guttyán József gazdasági előadó (fn. „Gajda”)¹⁰ és Csoóry Tamás, a Hungarocamion londoni képviselője (fn. „Arabell”) a III/I-2-es (külföldi elhárítási) Osztályhoz tartozott. A másik hat titkos munkatárs Demus László (fn. „Drégen Péter”), Gyenesei László gépkocsivezető (fn. „Györgydeák Béla”), Kallós Péter konzul (fn. „Tarasz Zsolt”), Szabados László műszaki-tudományos attasé (fn. „Meder Dániel”), dr. Palotai András II. osztályú kereskedelmi titkár (fn. „Lunette”)¹¹ és Buda Ferenc rejtjelező (fn. „Gulács Ernő”)¹² – a III/I-3. Osztály alárendeltségébe került,¹³ ahogy 1981-től a rezidentúra irányításáért az európai NATO-tagországok elleni hírszerzés terén illetékes részleg lett a felelős.¹⁴

A működésre vonatkozó utasítás

A BM III/I. Csoportfőnökség a feszült nemzetközi helyzetre való tekintettel előtérbe helyezte a rezidentúrák, a külföldi kolóniák és az általuk őrzött állam- és szolgálati titkok védelmét, továbbá az ellenséges speciális szolgálatok elleni operatív akciók hatékonyabbá tételét. A Központ a 2-es „vonalon” az ügyszerű, tippkutató – tanulmányozó, operatív feldolgozó és beszerző tevékenység felgyorsítására adott utasítást az ellenséges hírszerző- és elhárítószervek ügynöki hálózatába történő beépülés végett. Mindehhez folyamatosan vizsgálni kellett a rezidentúra hálózati személyeinek kapcsolatait, elsősorban azokat az idegen állampolgárokat, akik a behatolás céljából számításba vehetők. Ide tartoztak a rendőrség emberei, ahonnan a káderutánpótlás történt; karrierben megrekedt, erkölcsi, politikai, egzisztenciális okokból elégedetlen hivatásos elhárítók és hírszerzők; a külképviseletek idegen állampolgárságú alkalmazottai; ez utóbbiak rokoni és baráti köre; utazási irodák dolgozói, ingatlanügynökök. Az erre irányuló törekvések között második helyen szerepelt – a magyar emigráció második-harmadik generációjához sorolt¹⁵ – perspektivikus jelöltek felkutatása, megnyerése, majd hosszú távon a speciális szolgálatok felé történő irányítása az olyan felsőoktatási intézmények hallgatói, fiatal oktatói, szakértői közül, amelyek a nyugati országok állambiztonsági szerveinek a személyzeti bázisát jelentik. A rezidentúra magyar állampolgárságú hálózati személyei közül ki kellett választani a tálalásra, a támadólagos operatív tevékenységre és

¹⁰ ÁBTL 3.2.1–Bt–3080 – „Gajda” (Guttyán József) – Évkör: 1980–1986.

¹¹ ÁBTL 3.2.1–Bt–2249/2 – „Lunette” (dr. Palotai András). Évkör: 1976–1987. 40 oldal.

¹² ÁBTL 3.2.5–O–8–126/5/2–15–OD–2808/5 – „Liliom” – Párizsi Magyar Követség és Konzulátus – Melléklet. – Budapest, 1965. június 4. 33–34.o.

¹³ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – Tárgy: Angliai kolónia védelmi terv – Budapest, 1981. szeptember 15. 138.o.

¹⁴ TÓTH Eszter 2013: A politikai és gazdasági hírszerzés szervezettörténete, 1945–1990. In: CSEH Gergő Bendegúz–OKVÁTH Imre (szerk.): *A megtorlás szervezete. A politikai rendőrség újjászervezése és működése, 1956–1962.* Állambiztonsági Szolgálatok Történeti Levéltára–L’Harmattan, Budapest, 2013. 432–445.o.

¹⁵ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 2/1–2/80. sz. utasítás! – Tolnai elvtársnak! London – Tárgy: Emlékeztető Tolnai elvtárs részére. – Budapest, 1980. augusztus 18. 45–48.o.

játszmákra alkalmas embereket, akik az ellenfél látókörébe hozhatók. Ezzel egy időben a Központ számított rá, hogy az ellenséges hírszerző és elhárító szolgálatok nagyobb hangsúlyt helyeznek a magyar külképviseleti szervek és a külföldi magyar kolóniák tagjainak tanulmányozására, kompromittálására, beszerzésére vagy átállítására. A biztonsági tisztek feladata itt az volt, hogy a rend és a fegyelem, az operatív és védelmi szabályok megsértésére utaló jelzéseket, eseményeket azonnal hozzák felszínre, és akadályozzanak minden erre irányuló törekvést. Az elhárító és hírszerző szervek által a rezidentúra munkáját zavaró, akadályozó, illetve leleplezését célzó hálózati, operatív, technikai, figyelési tevékenységéről, valamint a rezidentúra területén működő ellenséges szolgálatok személyi állományára, ügynökségére, módszereire, hírigényeire vonatkozóan folyamatos adat- és információgyűjtés szerepelt az általános munkatervben.¹⁶

Megfigyelés és zaklatás a '70-es évek második felében

Simonyi Ernő (fn. „Szalmási”) 1980. március közepén jelentést készített az angol elhárítás által a magyar kolónia tagjai irányában folytatott tevékenységéről. A diplomata azzal kezdte a beszámolót, hogy a korábbi évek tapasztalatai és a gyakorlat azt igazolták, hogy az angol hivatalos szervek a többi szocialista országhoz képest másképp kezelik a MNK képviselőit, hiszen általános felfogásukkal összhangban állt, hogy a lojálisnak nevezett Magyarországgal eltérő módon kell kommunikálni. Mindettől függetlenül, a rezidentúra meg volt győződve arról, hogy az MI5 (Military Intelligence Section 5 vagy Security Service – a brit kémelhárítás)¹⁷ nem hagyta abba az MNK nagykövetségének feltérképezését. Az 1976-os Hajma-ügy – a helyettes katonai attasénak és titkárnak a brit atomfegyvereket összeszerelő üzemnél történt letartóztatása¹⁸ – óta eltelt időszakban nem került sor magyar diplomata vagy kihelyezett dolgozó elleni nyílt támadásra, a brit speciális szolgálatok emberei viszont folyamatosan látogatták a szolgálati lakásokat, és erőszakos behatolások színlelésével tudatosították, hogy a MNK küldötteivel is foglalkoznak. A Simonyi Ernő, Molnár Imre kereskedelmi titkár vagy a Mozsik család sérelmére végrehajtott betörések ugyan nem okoztak komoly anyagi kárt, de lélektanilag célba találtak. A kolóniához tartozó gépkocsikat a legkülönbözőbb módszerekkel megrongálták, többen szenvedtek csak anyagi károkkal járó karambolt, de arra is akadt precedens, hogy az ellopott jármű használhatatlan állapotban került vissza tulajdonosához. Az időszakos szerviz ugyanakkor kiváló alkalommal szolgált a lehallgatási technika beszereléséhez. Személyes ráépülést nem tapasztaltak, ugyanis a modern technikának köszönhetően a hírszerzés és az elhárítás nagyobb távolságból is

¹⁶ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 3/1-2/80. sz. utasítás. – Tolnai elvtársnak! London – Tárgy: A rezidentúrák 2-es vonalon folytatott tevékenységének felmérése, speciális szolgálatok elleni munka erősítésének feladatai. – Budapest, 1980. március 14. 75–81.o.

¹⁷ ANDREW, Christopher: *The Defence of the Realm. The Authorized History of MI5*. Allan Lane, London, 2009. 3–109.o.

¹⁸ The National Archives Foreign and Commonwealth Office (TNA FCO) TNA FCO 28/2885 NH 380/548/ 2. – Detention of the Hungarian Assistant Military Attache in Basingstoke. April 22–May 7 1976. 17–35.o.

figyelemmel kísérhette a diplomatákat. A vidéki utazásokról először – a BBC által végzett tényfeltárás szerint a nemzetbiztonság és a terrorizmus elleni harc valós szükségleténél sokkal szélesebb körű¹⁹ – telefonlehallgatások révén szereztek tudomást, majd a hálózat jóvoltából kísérték figyelemmel a nagykövetség munkatársait.²⁰ A figyelés sokkal inkább csak a helyszínen kezdődött, ugyanis az MI5 a '80-as évek elején már legtöbbször a nagyobb helyismerettel rendelkező, területileg illetékes rendőri szerv keretében működő Special Branch (Különleges Ügyosztály) segítségére alapozott.²¹ Az MI5 jólétesültségének másik forrása a brit állampolgárok jelentéstartalmi kötelezettsége révén a mindenkori beszélgetőpartner volt. A magyar származású kapcsolatok cinikusan közölték, hogy mely hivatalos személlyel állnak összeköttetésben. A legveszélyesebb szituáció mégis akkor állt elő, amikor a beszerzett informátor többet kívánt nyújtani, mint amiről megállapodás szólt. Az 1970-es évek közepétől érezni lehetett, hogy brit részről egyre kitérőbb figyelemmel fordultak a magyar kolónia fiatalabb tagjai felé, még akkor is, ha ezeket az évfolyamtársi, baráti kapcsolatokat csak évekkel később gondolták gyümölcösztetni. A hivatalos kiküldöttekkel szemben már nem nyúltak az áruházi tolvajlás kedvenc módszeréhez, ám ezt az alkalmi delegátusok továbbra is megszenvedték. Szekeres elmondta, hogy többször is névtelen hívásokkal zaklatták őket, míg az 1979-es esztendő folyamán egy alkalommal be is törtek hozzájuk. Szabados László telefonvonala egy alkalommal egész hétvégére elnémult, ami Buda Ferenc rádióssal is megtörtént. Időről időre az utóbbit is névtelen hívásokkal idegesítették. Az ismeretlen, „Liptói” fedőnevű ösztöndíjas számtalan jelből arra következtetett, hogy szorosabban figyelik, mint azelőtt, íróasztalát is gyakran átnézik, valamint elzárták előle az olyan anyagokat, amelyekhez korábban szabadon hozzáfért. Az ugyanígy azonosíthatatlan „Sziklai” vendégkutató lakását nem sokkal azelőtt átkutatták, miközben készakarva hagytak nyomokat maguk után – a bőröndök elhúzva, a szekrényajtó nyitva, a villany égve maradt. Bornemissza Károlynéhoz rendszeresen bejártak, mivel a portásnak és a takarítónőnek is kulcsa volt a szolgálati lakásához. Miután felkérte az egyik gépirónójukat, hogy tanítsa meg angolul, a hölgy nyelvgyakorlás címén félreérthetetlenül tanulmányozási célból tett fel kérdéseket. Palotait párszor megállították a rendőrök, de saját bevallása szerint nem jogtalanul. Az 1980-as év első két hónapjában az elhárítás fokozottabb figyelemmel fordult az MNK nagykövetsége felé, és nagyobb energiát fordított a magyar kolóniával történő foglalkozásra, mint régebben. „Tolnai” azt valószínűsítette, hogy most éppen a magyar nagykövetség van terítéken, ugyanakkor nem zárta ki, hogy a többi szocialista ország is hasonló tapasztalatokat szerzett. Mozsik katonai attasé megerősítette a rezidens álláspontját, minthogy a szovjetek és a lengyelek is ugyanezzel találkoztak. „Tolnai” úgy vélte, hogy a direkt figyelemfelkeltéssel a kolónia tagjait akarják idegesíteni, ezek az akciók ugyanakkor a preventív elrettentés céljára is kiválóan alkalmasak. A megelőző

¹⁹ EGEDY Gergely: *Nagy-Britannia története*. Aula, Budapest, 1998. 453–454.o.

²⁰ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 3/2–11/80. sz. jelentés – Tárgy: Az angol speciális szervek velünk szembeni magatartása. – London, 1980. március 17. 57–59.o.

²¹ DORRIL, Stephen: *The Silent Conspiracy. Inside the Intelligence Services in the 1990's*. Heinemann, London, 1993. 161–165. o.

hetekben Mozsik lábtörlőjét összetépték, Hajdúnál a villanyt égve, a szekrényt nyitva hagyták, Bulath új kocsjába parkolás közben beletolattak, Bánlaki lakásában használták a WC-t, de nem húzták le, ugyanakkor Mészáros Gábor főhadnagy autóját alkatrészhiányra való hivatkozással heteken keresztül nem voltak hajlandók megjavítani. A – Juhász Ferenc, Károlyi Amy, Nemes Nagy Ágnes, Pilinszky János, Vas István és Weöres Sándor részvételével 1980. március 9-től 20-ig tartó²² – költői felolvasóköriút alatt Pilinszky Jánost a környék néhány piti bűnözője leütötte és kirabolta. Miután a SOHO piroslámpás negyedében vacsorázott angol fordítójával, többet ivott a kelleténél, majd egyedül indult vissza a szállodájába.²³ Weöres Sándor és Károlyi Amy szobájában hajnali 3 és 5 óra között kábítószer tartalmazó bőrönd után kutatott a rendőrség, a tulajdonos csak később került elő. Ezzel egy időben „Tolnai” kétszer találkozott demonstratív figyeléssel,²⁴ majd április közepéig négyszer jártak a lakásában úgy, hogy ennek nyoma maradt. A lakhelye és a nagykövetség közötti útvonalon több rejtett megfigyelőpont létesült, március közepén Londonban kétszer figyelte az elhárítás. A négynapos cornwalli látogatása alatt az MI5 konspiráltan és agresszív követési technikával végig ellenőrzés alatt tartotta. Szekeres, aki Wales területén kirándult, ugyancsak figyelést észlelt az országutakon.²⁵

A behatolás

1980. április 14-én fél egy körül „Tolnai” rezidens az Eaton Place 35. szám alatti nagykövetség harmadik emeletén található rejtjelszobából lefelé mozgást érzelt a második emeleten lévő irodája és a katonai attasé hivatala körül. A rezidens meggyorsította lépteit, de a folyosón már csak annyit látott, hogy két munkás külsejű férfi mindenáron igyekszik kikerülni a látóköréből. A kíséret nélkül a nagykövetség épületében tartózkodó két idegen azt állította magáról, hogy szerelők, akik eltévedtek. A hadnagy ekkor felajánlotta a segítségét, azonban az egyik behatoló az első emeleti szalonon keresztül, a hátsó kijárat felé próbált távozni azzal a megjegyzéssel, hogy ott engedték be őket. A rendőrtiszt ehhez nem járult hozzá, majd amint Lőrincz Nagy János nagykövet²⁶ jelenlétében a főbejáraton kiengedte őket, elkezdődött az épület átvizsgálása. Mivel erőszakos behatolásra semmi nem utalt, úgy tűnt, hogy csak a hátsó bejáratot vagy a konzuli átjárót használhatták. Az ügy kivizsgálásával Simonyi Ernő tanácsos és Szekeres Ferenc biztonsági felelős foglalkozott, akik kiderítették, hogy a nyitott hátsó bejáraton keresztül zajlott a behatolás. A sajtóiroda, a szomszédos raktár

²² MNL OL-XIX-J-1-j – SZT Iratok Anglia – 26. doboz. – 003136/1 – 41/1980 – Tárgy: Magyar költők látogatása Nagy-Britanniában. – London, 1980. április 15. 1–4.o.

²³ Interjú Sárközi Máttyással, a BBC Magyar Osztályának 2006-ban nyugállományba vonult vezetőjével. Készítette: Pál István. Budapest, 2018. január 18.

²⁴ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 3/2–11/80. sz. jelentés – Tárgy: Az angol speciális szervek velünk szembeni magatartása. – London, 1980. március 17. 57–62. o.

²⁵ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 4/2–11/80. sz. jelentés – Tárgy: Ügynöki operatív helyzetünk. – London, 1980. április 14. 63–64.o.

²⁶ TNA FCO 28/2887 NH 400/548/1 – Diplomatic Representation of Hungary in the United Kingdom 1976. 24/9/76.

és a garázs megközelítésére a beosztottak sokszor ezt vették igénybe, ráadásul nem sokkal az esemény előtt Bulath Károly²⁷ nagykövetségi számadó is a hátsó ajtón közlekedett. Ezzel egy időben a belső biztonsági láncot rapszodikusán használták, miközben reggel 8:00 és 8:30 között a kulcs kényelmi szempontból a szomszédos hivatalsegédi lakás ablakában maradt. A biztonsági körletnek nem esett bántódása, a berendezési tárgyakból semmit nem vittek el. Mohácsi István gazdasági titkár azonban jelezte, hogy a szobájában nyitva talált páncélszekrényéből 180 font készpénz és 150 font értékű csekk tűnt el.²⁸ A másnap Londonba érkező dr. Meggyesi Sándor rendőr alezredes úgy nyilatkozott, hogy a behatolás egyértelműen a brit titkosszolgálat akciójaként értelmezendő, hiszen az állítólagos szerelők felbukkanása az ebédszünet alatt történt, amikor a munkatársak többsége házon kívül volt, ráadásul a két idegen a katonai attasé hivatala, a biztonsági körlet és a rejtjelező szoba körül mozgott. Ezzel egy időben az is az elhárítás akciójára utalt, hogy az előző időszak folyamán megnőtt a diplomaták lakásai elleni színlelt betörések száma. Az alezredes ugyanakkor elismerte, hogy a helyzet kialakulásában tekintélyes szerepe volt annak, hogy a nagykövetséggel szemben lévő olasz konzulátust egy terrorista csoport felrobbantotta, amelynek nyomán az Eaton Place 35. szám alatti épület is megrongálódott. A sérülések javítására villany- és gázszerelők, üvegesek jártak a külképviseletre, így a meglepetésen kívül „Tolnai” ezért tudta olyan könnyen elfogadni a két férfi magyarázatát.²⁹ A behatolás óhatatlanul rossz érzést generált a magyar külképviselet munkatársaiban, ugyanis 1980. április 30-án Irán londoni nagykövetségét elfoglalta a „Demokratikus Front Arabisztán Felszabadításáért” nevű terrorista csoport. A túsziámának, amely az egyik diplomata életébe került, hat nappal később a SAS (Special Air Service – Különleges Légi Szolgálat) rajtaütése vetett véget.³⁰ A rezidens a két idegent azért terelte a főbejárathoz, hogy amennyiben kiderül, hogy rossz szándékú behatolásról van szó, a portán lévő fegyvernek köszönhetően kiegyenlítetté váljanak az erőviszonyok. Amíg nem tudott beszélni Kiss Tibor portással és Kejla Antal hivatalsegéddel, nem vehette biztosra, hogy nem ők engedték-e be a szerelőket, hiszen az elmúlt egy év alatt már többször találkozott az épületben csellengő karbantartókkal. A rezidens április végén a Belgrave Place 3. számú ház bejáratánál dolgozó munkásban felismerte az egyik látogatót, aki rövid beszélgetés során elmondta, hogy a hátsó kapun sikerült bejutniuk.³¹ A biztonsági helyzet gyors javulására viszont már csak azért sem lehetett

²⁷ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 3/2–11/80. sz. jelentés – Tárgy: A londoni magyar kolónia. – London, 1980. március 17. 8. o.

²⁸ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 5/6/1980. – Tárgy: Idegen személyek a Nagykövetség épületében. – London, 1980. április 17. 24–27. o.

²⁹ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – Tárgy: A londoni nagykövetségünkre történt behatolásról jelentés. Budapest, 1980. április 24. 53–54. o.

³⁰ ASHER, Michael: *The Regiment. The Real Story of the SAS*. Penguin Books, London, 2008. 1–21. o.

³¹ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 4/1 – 2/80. sz. jelentés. – 67/53 – 608/80 – Tárgy: Behatolás a nagykövetségre. – London, 1980. május 12. 40–43. o.

számítani, mert a Külügyminisztérium (KÜM) döntése értelmében a Szombathelyi Állami Építőipari Vállalat hozzákezdett a londoni nagykövetség átfogó felújításához, így a külképviseleti intézmény átköltözött a Charles Street 48. szám alatti irodaházba. A nagykövet elismerte, hogy ez biztonsági szempontból nem a legjobb megoldás, de a rövid távú bérleti jogviszony korlátozottsága miatt pénzügyi szempontból csak ez volt vállalható. A legnagyobb gondot az okozta, hogy az épület hátsó része a „környezetvédelmi minisztériummal” érintkezett, amely teljesen zárt és védett objektumnak számított.³²

A lektor kalandjai 1980-ban

Az elhárítás figyelme azonban nem kizárólag a rezidentúra és a katonai attasé hivatalának hivatásos állományú tagjaira korlátozódott. A londoni Szláv Intézet magyar lektora, Rapcsák János³³ (fn. „Láposi Előd”) saját biztonsági helyzetéről úgy nyilatkozott, hogy tudtán kívül biztosan megfigyelték és megszendázták, de állandó zaklatásról nem lehet beszélni. Az első két évben (1977–1978) egy, illetve két alkalommal vett észre rendkívül feltűnő, zavaró jellegű figyelést. A lektor úgy érezte, hogy a brit elhárítás a viselkedését tanulmányozza, erről azonban nem vett tudomást, hiszen a járműveken olvasott, gyalogosan pedig elsietett a helyszínről. 1979-ben egy nyomozónő négy-öt napra állandó kísérőként mellé szegődött, ám 1980 márciusától egymást érték az éjszakai telefonhívások, becsengetések, majd közel két hétig agresszív megfigyelés alatt állt. Az elhárítók főleg munkahelye környékén bukkantak fel, de néhány alkalommal a lakásánál várta a „fogadóbizottság”, általában egy, párszor két személy. Egyik alkalommal a Southampton Row-n lévő Tavola Calda étteremben az asztala mellé ültek le, azzal a nyilvánvaló céllal, hogy jelenlétük zavarja Rapcsák Jánost. Mivel a lektor nem rémült meg tőlük, a zaklatás abbamaradt, vagy átment fel nem fedhető formába, bár ezt nem tartotta valószínűnek. Rapcsák találkozásaival és viselkedésével nem adott gyanúra okot, így nem is zavarta, talán még élvezte is a játszmákat. Egyedül a hajnalban két és három óra közötti becsengetéssorozat volt kellemetlen, mivel a kapucsengő beragadt, és le kellett mennie, hogy kipiszkálja a kapcsolót. A próbálkozásoknak azonban vége lett, miután többször is sokáig fenn volt, és az ablakból a függönyön keresztül az utcát figyelte. Egyik alkalommal egy jól öltözött fiatalember 10-15 percig fel-alá sétált az utca mindkét oldalán, megnyitott egy-két kaput, majd Rapcsák házához jött. Mielőtt becsengetett volna, a lektor teljesen nyugodt hangon megkérdezte, hogy miben lehet a segítségére. Az angol nagyon természetesen azt mondta, hogy egy partira jött, de nem találja a címet. Rapcsák sajnálkozott, amiért nem tud segíteni, miközben megjegyezte, hogy egy kicsit azért már késő van. Ezt követően még egyszer becsöngettek, többször nem. A lakásában semmilyen gyanús jellel nem találkozott, hiszen nehéz is lett volna bejutni hozzá.

³² ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – B – 0043/1980 – Tárgy: Londoni nagykövetségnek bérelt épület ügye. – Budapest, 1980. május 13. 32/36–39. o.

³³ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 3/2–11/80. sz. jelentés – Tárgy: A londoni magyar kolónia. – London, 1980. március 17. 17. o.

Rapcsák az épület legfelső szintjén élt, a behatoláshoz három ajtót kellett volna felfeszíteni, ám ezekre az olasz tulajdonos különleges biztonsági zárat szereltetett. A ház ugyanakkor soha nem maradt hosszú időre üresen. A munkahelye az összes házon kívüli telefonhívást feljegyezte, könyveit takarítást követően a helyén találta, igaz, az íróasztalát olyan pasztával fényezték, amelyen akkor is megmaradt az írás, ha vastag papírt tett alá. A kollégáihoz fűződő viszonyában nem történt negatív irányú változás, a nem azonosítható „William Taylor” fedőnevű személyétől eltekintve semmi gyanúsat nem észlelt. A diákok részéről többé-kevésbé nyílt provokáció csak Lázár Ádám és Viola Finn részéről történt. Az utóbbi először megpróbált nőként közeledni a lektorhoz, majd arra állt rá, hogy kellemetlen légkört teremtsen az órákon.³⁴ Rapcsák 1980. június 9-én és 10-én a British Council szervezésében a Norwich-i University of East Anglia vendége volt, ahol John Coates professzor kalauzolta.³⁵ Coates 1968 óta volt Dean of Students (a dékán hallgatói ügyekkel foglalkozó helyettese), aki egy meglehetősen nagy létszámú hivatali apparátus élén állt, jól ismerte hallgatók anyagi helyzetét, gondoskodott elhelyezésükről, ugyanakkor ő döntött az ösztöndíjakról, és ellenőrizte a diákszervezeteket.³⁶ A lektor és a dékánhelyettes találkozásai szívélyes légkörben zajlottak, Coates maximálisan igyekezett Rapcsák segítségére lenni, ugyanakkor kissé szokatlan módon kétszer is meghívta magához. Az első nap estéjén Coates elintézte, hogy a lektor is ott lehessen az egyik arisztokrata ismerősének Tudor-korabeli villájában tartandó összejövetelen a Múzeumok Világszövetségének vezetőivel együtt. A dékánhelyettes ezután Kelet-Anglia egyik legrégebbi kocsmájába vitte el magyar ismerősét, ahol hosszasan beszélgettek. Rapcsák megkérdezte, hogy Coates hogyan került kapcsolatba a magyar, illetve a Szovjetunióban beszélt finnugor nyelvekkel.³⁷ A professzor egy idő után elárulta, hogy a második világháború alatt a hírszerzés tisztje volt. 1944-ben a kanadai Mike Thomas (Turk) és Joe Gordon (Gelleny) társaságában ejtőernyővel ledobták Magyarországra, de árulás következtében pillanatokon belül mindannyian fogságba estek. Turk kórházba került, Coatest és Joe Gellenyt, a Hadik laktanyából a VKF2 (Vezérkari Főnökség 2. Osztály, a Magyar Királyi Honvédség hírszerző-és elhárító szervezete) meg nem nevezett angolbarát tisztjei a zugligeti internálótáborba csempészték, majd védett lakásokba vitték őket. A nyilas hatalomátvételt követően a németek mind a hármukat elfogták, de végül mindannyian túléltek a háborút.³⁸ Coates 1945 után diplomáciai pályára lépett – Rapcsák előtt öniróniával megjegyezte, hogy

³⁴ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – Tárgy: „Láposi Előd” fn. tm. biztonsági helyzetéről jelentés. – Adta: „Láposi Előd” fn. tm. – Vette: Károlyi Gyula r. alez. – Budapest, 1980. augusztus 18. 69–71. o.

³⁵ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – Tárgy: Dr. John Coates-ról jelentés. – Adta: „Láposi Előd” fn. tm. – Vette: Károlyi Gyula r. alez. – Budapest, 1980. augusztus 18. 66. o.

³⁶ SANDERSON, Michael: *The History of the University of East Anglia Norwich*. Continuum, London, 2002. 207–210. o.

³⁷ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – Tárgy: Dr. John Coates-ról jelentés. – Adta: „Láposi Előd” fn. tm. – Vette: Károlyi Gyula r. alez. – Budapest, 1980. augusztus 18. 66–68. o.

³⁸ HORN, Bernd: *A Most Ungentlemanly Way of War. The SOE and the Canadian Connection*. Dundurn, Toronto, 2016. 168–171. o.

többé-kevésbé a régi szakmáját folytatta –, amikor a hágai, a bécsi, a moszkvai, végül a helsinki brit nagykövetségen volt az állomáshelye. 1962-ben kilépett a külügyi szolgálatból, majd Cambridge-ben doktorált.³⁹ Állítása szerint megszakította kapcsolatát korábbi cégével, azt viszont nem tagadta, hogy diplomáciai téren szerzett tapasztalata és főleg kapcsolatai számos esetben a segítségére vannak. Coates hangsúlyozta, hogy már csak a tudomány érdeklí, jó viszonyt ápol szovjet és magyar tudósokkal, mint pl. Domokos Péterrel. 1977-ben nagyon jól érezte magát Magyarországon, így megkérte a lektort: érdeklődjön róla, hogy a következő évben elfogadnák-e látogatását. Végül, de nem utolsósorban, magánlátogatásra hívta Rapcsák Jánost és feleségét. Károlyi Gyula alezredes viszont egyértelműen úgy vélte, hogy John Coates a brit hírszerzés régi, kipróbált és igencsak felkészült tagja, aki szoros kapcsolatban áll a Magyar Tudományos Akadémia (MTA) Nyelvtudományi Intézet munkatársaival.⁴⁰

A Sziklai-ügy

1980. szeptember 5-én „Tolnai” autójában fordítva szerelték vissza a rádió egyik gombját, amíg a diplomata a szakszervezeti konferencián volt. Három héttel később hajnali fél kettőkor a rezidens lakásában megszólalt a telefon, ám senki nem szólt bele, majd kisvártatva letették a kagylót. Október 2-án feltörték Patkó András lakását, de nem vittek el semmit,⁴¹ viszont 3-án 14 órakor rendkívüli eseményre került sor: Newcastle városában áruházi lopás vádjával őrizetbe vették „Sziklai” és feleségét, akik csak jó két órával később hívhatták fel a konzulátust. A házaspár hajnali három órakor szabadon távozhatott a rendőrségről, ám addig egy közel tíz órán át zajló kihallgatásnak vetették alá mindkettőjüket, amelynek égisze alatt ígéretessel és fenyegetéssel próbálták elérni a beismerő vallomást. A férj kihallgatásán a Special Branch tisztje is jelen volt, miközben egy nyomozócsoport átkutatta „Sziklai” lakását, irodáját, munkahelyi felszerelését és iratait, de még a kutatóintézet számítástechnikai rendszerében is végig nézték a tevékenysége nyomait. Szabadlábra helyezésük előtt egy terjedelmes jegyzőkönyvet írtak velük alá, de bűnösségüket nem ismerték el. A tárgyalást október 20-ra tűzték ki, az ügyészség 9 font 20 penny értékű lopással vádolta a házaspárt. A rezidens úgy vélte, hogy a rendőrség által felvonultatott tanúk és bizonyítékok ismeretében a bíróság részéről elmarasztaló ítélet születik. „Sziklai” a megelőző hetek folyamán erős figyelést tapasztalt, valamint többen is átállásra próbálták rávenni. A nagykövetség és a rezidentúra késlekedés nélkül akcióba lépett, így nagy valószínűséggel sikerült kizárni annak a lehetőségét, hogy a brit hatóságoknak bizonyító erejű dokumentum lenne a kezében a vendégkutató és a hírszerzés kapcsolatáról. „Sziklainak” azt tanácsolták, hogy mielőbb fogadjon ügyvédet, miközben

³⁹ TILLOTSON, Michael (szerk.): *SOE and the Resistance. As told in The Times Obituaries*. Bloomsbury, London, 2011. 275–277. o.

⁴⁰ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – Tárgy: Dr. John Coates-róljelentés. – Adta: „Láposi Előd” fn. tm. – Vette: Károlyi Gyula r. alez. – Budapest, 1980. augusztus 18. 66–68. o.

⁴¹ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 7/1–2/80. sz. jelentés – Tárgy: Biztonsági jelentés. – London, 1980. október 27. 67. o.

eltiltották az addig általa folytatott illegális tevékenységtől. Ezzel párhuzamosan Kallós Péter konzul megbeszélte „Sziklaival”, hogy milyen magatartást tanúsítson. A bíró a tárgyalást elnapolta, mivel a rendőrség nem volt képes a rendelkezésre álló 17 nap alatt megfelelő bizonyítékot produkálni, majd 1980. november 24-én zárt tárgyalást rendelt el. A bizonyítási eljárás reggel fél tíztől este fél hatig tartott, amit két, szemmel láthatóan idegen férfi folyamatosan jegyzetelve mindvégig nyomon kísért. Az ügyvéd összehívta a vád tanúit, így a bíró végül mindkét vádlottat felmentette. „Sziklai” tavasszal vette át „Liptói” helyét, akinek az idegei felmondták a szolgálatot. Az ügy a tudós zaklatása miatt elég nagy port vert fel. „Sziklai” nemzetközi hírű szakembernek számított, akinek többször is tettek rá célzást, hogy ha kint marad, sokkal nagyobb karrier vár rá, mint otthon. Azt, hogy a provokációval disszidálásra tervezték rávenni, „Tolnai” sem bizonyítani, sem cáfolni nem tudta. A véletlen gyanú szinte kizárt volt, ugyanis a letartóztatással egy időben zajló házkutatásból és az iroda felforgatásából kitűnt, hogy az akció mögött az angol speciális szervek valamelyike áll. Igaz, ha kémper lett volna a cél, eldughattak volna valamit Sziklai holmijában, ami a szabadon bocsátást követően előkerül. A hosszadalmas vallatások alatt viszont még csak utalás sem történt a munkájára, és kapcsolatairól sem érdeklődtek. „Tolnai” szerint nagy valószínűséggel kizárható volt, hogy a rendőri fellépés Sziklai illegális tevékenységével volt összefüggésben. A provokáció minden bizonnyal a kompromittálást szolgálhatta vagy a kutató teljes ujjlenyomatának megszerzését az USA-ban viselt dolgai (feltehetően a magyar hírszerzés számára nyújtott segítsége) miatt. Az angolok biztosra mentek a tekintetben, hogy ez sikerülni fog, de nem számoltak a nagykövetség tiltakozásával, és azzal, hogy ellentmondásokba keverednek. A tettenérés és bizonyítékgyártás ügyetlenül és pontos forgatókönyv híján zajlott. Amikor a rendőrség színre lépett, az áruház rendészeinek tevékenysége tudatos és célirányosra vált, amely azt a célt szolgálta, hogy „Sziklait” hosszan tartó lelki nyomásnak vessék alá. Az asszonyt letartóztatták, miközben a férjét el akarták kergetni a helyszínről. A bíróságon kiderült, hogy „Sziklai” nem is volt gyanúsított, hiszen kollégája feleségének a tárgyalás előtt a rendőrtiszt azt mondta: „most már látom, a fiút fel fogják menteni, de a felesége nem ússza meg.” Az ügyész egész végig módfelett agresszívan viselkedett. „Tolnai” végül a legvalószínűbb forgatókönyvként a következőt vázolta fel. „Sziklai” több olyan projekten dolgozott, amelyek a hadiipar számára is fontosak lettek volna, ám két kísérletnél megállt a végső fázis előtt. A kutató minden bizonnyal saját jogon szerette volna learatni a sikert felfedezéseierért, míg az angol fél érdemi eredményeket akart, ezért gátolta a távozását. Az is elképzelhetőnek tűnt, hogy fontos katonai projektekbe is szeretnék volna bevonni, ám ez előtt a magyar állampolgárság leküzdhetetlen akadályként tornyosult. „Sziklai” viszont elutasítóan reagált, ezért dönthettek úgy az angolok, hogy más eszközökkel veszik rá az ottmaradásra. A tudós nem volt anyagi, és a káros szenvedélyektől mentes maradt, ugyanakkor élt-halt a feleségeért, amely végső soron sebezhetővé tette. Amennyiben az asszonyt elítélik, férje nem utazott volna haza a szerződés lejártával, hanem kint maradt volna Angliában, hogy párja szabadon bocsátásáért harcoljon. Az sem volt véletlen, hogy megvárták, amíg a feleség egyedül maradt. Terveiket megzavarta, hogy „Sziklai” pont akkor ért a helyszínre, amikor az asszonyt el akarták tüntetni a szeme

elől. Az angolok azt mondhatták volna, hogy a nő menedéket kért tőlük, és ha találkozni akar velem, ő is álljon át hozzánk.⁴²

A lektor tapasztalatai 1981-ben

Rapcsák 1981. április 6-án vendégül látta Sárközi Mátyást, a BBC Magyar Osztályának vezetőjét és feleségét, akiknek 30 percesre tervezett látogatásából négyórás diskurzus kerekedett. Az asszony nem sokkal azelőtt galériájában arról panaszkodott a Szláv Intézet magyar lektorának, hogy férje nagyon fáradt, hiszen a BBC állandóan berendeli, ugyanakkor a Magyarországról érkezők időről időre lehetetlen kérésekkel zaklatják, ráadásul a hónap első hete volt, amikor jelentést kell készítenie az amerikaiaknak. Rapcsák értetlenkedett, mire Sárköziné igen naivan elmagyarázta, hogy férjének minden hónap 10-én részletesen be kell számolnia azokról a magyarokról, akik kaptak tőle a CIA által rendelkezésre bocsátott könyvekből, vagy akik az e célra elkülönített forrásokat felhasználva vettek szakirodalmat. Sárközi egyre türelmetlenebbé vált a CIA irányában, de azoktól az egykori honfitársaitól sem volt elragadtatva, akik rajta keresztül szerettek volna nagy tömegben hozzájutni a tiltott művekhez.⁴³ A BBC magyar adásának akkori főszerkesztője a New York-i International Book Center révén beszerzett könyvek és folyóiratok révén a Londonban tartózkodó vagy a brit fővárosba látogató honfitársait próbálta megismertetni Márai Sándor, Cs. Szabó László és Szabó Zoltán otthon indexen lévő munkásságával, miközben a szélsőséges, hamis állításokkal operáló propagandaanyagokat kiselejtezte. Sárközi Mátyásnak nem volt kifogása a New York-i központ munkatársai ellen, a hazai látogatókkal is szívesen elbeszélgetett, de tény, hogy sokan hajnali 3 óráig ott voltak nála, és a vendégek hatékony közreműködésével két-három üveg whisky is elfogyott. A havi elszámolási kötelezettség nem volt titok, mert Rómában Triznya Mátyásné, Szőnyi Zsuzsa vagy Párizsban Pél Albert visszaélt a kínálkozó csalási lehetőségekkel. Rapcsák és Sárközi vitája azonban mindenekelőtt David Irving *Uprising* című könyvéről szólt. A szerző szakmaiatlan megközelítéssel Mindszenty József hercegprímást kiáltotta ki az '56-os forradalom szellemi vezérének, ugyanakkor a forradalom előkészítésének valódi szereplőit származásuk szerint listázta, ezért Sárközi nem óhajtott vele diskurzust folytatni. Irving ezért egy cambridge-i doktoranduszt kért fel a megkönyvékezésére. A főszerkesztő bedőlt a trükknek, így a szélsőjobboldali történész fel tudta használni a tőle kapott információkat, kétszer is megemlítve a nevét. Sárközi meg volt róla győződve, hogy Irving, akárcsak Chapman Pincher, a *Daily Mail* újságírója az MI6 (Military Intelligence Section 6 – a brit hírszerzés)⁴⁴ számára dolgozik. Schöpflin György a *Times* és Mikes György az *Observer* hasábjain élesen reagált arra az állításra, hogy 1956 a zsidó származású vezetés ellen robbant ki, figyelmen kívül hagyva

⁴² ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 1/1–5/80. sz. jelentés – Tárgy: A Sziklai ügye. – London, 1980. december 3. 74–79. o.

⁴³ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890– „BOBY” – Angliai magyar kolónia operatív védelme – 4/4 – 11/81. sz. jelentés – Tárgy: Sárközi Mátyás ügye. – London, 1981. április 17. 103–104. o.

⁴⁴ JEFFERY, Keith: *MI6. The History of the Secret Intelligence Service*. Bloomsbury, London, 2011. 8–22. o.

a zsidóság forradalomban játszott szerepét.⁴⁵ Az este folyamán mind a kettőjük részéről elhangzott, hogy senkinek nem szóltak a lektornál teendő látogatásukról, nehogy jelentés menjen erről Magyarországra. Rapcsák kikérte magának, Sárközi viszont egyből rávágta, hogy a kinti magyarok között mindig akad valaki, aki jelentéseket küld a BM számára. A főszerkesztő Nagy Kázmért vádolta árulással, de azt is szóvá tette, hogy Magyarországra látogató ismerőseit a BM emberei magukhoz rendelték, vagy legalább egy presszóban elbeszélgettek velük. Sokan nem zárkóztak el az ilyen típusú meghívásoktól, de a visszatérést követően mindent elmondtak a brit elhárító szervezetnek. A londoni magyar lektorról Sárközi azt mondta, hogy „a legszimpatikusabb kém”, amit Rapcsák határozottan, de viccesen visszautasított. Sárközi szerint az egész csak tréfa volt, bár a jelenleg nem azonosítható „Donga” hírszerzői szerepéről viselkedése és az általa végzett adatgyűjtés árulkodott. A gyanú utódjával szemben is megmaradt, bár ezt az új lektor sikeresen próbálta eloszlatni. A rezidens az összegzésben elismerte, hogy Nagy Kázmér módfelett veszélyes helyzetbe került, így a hazatérés előtt álló „Indra” (feltehetően Horász Júlia első osztályú titkár)⁴⁶ utasítást kapott rá, hogy a távozása előtti búcsúlátogatáson túl ne találkozzon az érintettel.⁴⁷ Nagy Kázmér (1920–1985) egykori miniszterelnökségi sajtótitkár, aki 1951-től a Sydney-ben megjelent Dél keresztje, majd a Független Magyarország főszerkesztője volt, 1968-tól Londonban élt, 1981-ben tényleg hazatelepült.⁴⁸

Rapcsák nem sokkal később észrevette, hogy a brit elhárító szervek megfigyelés alá helyezték. Kísérői nem is próbálkoztak azzal, hogy tevékenységüket leplezzék, a figyelőköcsi a lakása előtt parkolt, együtt indultak vele, időként a hazavezető út is közös volt. Május 5-én egy sötét BMW és egy régi típusú piros Rover várakozott az utcájukban. Amikor Rapcsák Jánosné délelőtt gyalog indult el az Angol–Magyar Baráti Társaság (AMBT) irodájába, a BMW utánaeredt, miközben vezetője állandóan kiszólt az autóból. Mivel kedveskedő szavaira az asszony nem felelt, a sofőr kiszállt az autóból és megállította. Rapcsák felesége udvariasan, ám határozottan megkérte, hogy hagyja békén, mert nem akar neki kellemetlenséget. Az illető visszaült az autójába, de egészen az AMBT épületéig követte. Az asszony megdöbbenően konstataulta, hogy május 2-án szombaton betörték a társasághoz. A tettesek a tetőről hatoltak be, majd feltörték az iroda ajtaját. Míg Charles Ringrose, az AMBT elnöke Spanyolországban tartózkodott, az elkövetők felfeszítették íróasztalát, átkutatták és széthányták a dossziéit. Az irodából pusztán egy tranzistoros rádió tűnt el, pedig más műszaki cikket is el tudtak volna vinni. Rapcsák óvatos érdeklődésére Ringrose egyértelműen kijelentette: nem volt olyan dokumentum az irodában, amely elárulhatná, hogy az AMBT főleg a

⁴⁵ Interjú Sárközi Mátyással Budapest, 2018. január 18.

⁴⁶ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 3/2–11/80. sz. jelentés – Tárgy: A londoni magyar kolónia. – London, 1980. március 17. 6–8. o.

⁴⁷ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 4/4 – 11/81. sz. jelentés – Tárgy: Sárközi Mátyás ügye. – London, 1981. április 17. 104–105. o.

⁴⁸ KENYERES Ágnes (főszerk.): *Magyar Életrajzi Lexikon (1978–1991)*. Akadémiai Kiadó, Budapest, 1994. 652.o.

Magyarországról jött pénzekből működik. Rapcsák úgy vélte, nagy valószínűséggel álbetörésről van szó, mivel az elkövetők bizalmas iratokat kerestek. A rádió azért tűnt el, hogy a bűncselekmény hitelesnek látszon, ugyanakkor a jóval nagyobb értéket képviselő vetítőgépet és az igen drága sokszorosítót érintetlenül hagyták. Mindazonáltal, a lektor megjegyzete: nem árt felhívni az AMBT elnökének figyelmét, hogy semmilyen Magyarországról jött pénzről nem vezethet írásos kimutatást. Tudniillik, Ringrose irodájába az utcára nyíló méretes ablakok miatt nem volt nehéz behatolni, ugyanakkor az AMBT a Co-operative Society (Szövetkezeti Társulás) folyamatos megfigyelés alatt álló székházában működött.⁴⁹ A Munkáspártnál radikálisabb baloldali mozgalom kivette a részét az Augusto Pinochet tábornok diktatúrája elleni tiltakozásokat koordináló Chile Solidarity Campaign (Chilei Szolidaritási Kampány) tevékenységéből,⁵⁰ így Rapcsák tudomása szerint központjuk már többször is betörés áldozata lett. A lektor viszont az MI5 folyamatos jelenléte ellenére sem változtatott viselkedésén, igyekezett tudomást sem venni róluk, ám feleségének séta közben jelzett, hogy távolléte alatt ismeretlen ember számára ne nyisson ajtót. A hónap közepe felé már nem vett észre figyelést, ugyanakkor nem tudta kizárni sem.⁵¹

Az operatív helyzet alakulása 1981-ben

„Tolnai” május végén úgy nyilatkozott, hogy Nagy-Britanniában a nemzetközi légkör alakulásán túl két tényező befolyásolja lényegesen az operatív helyzet változását: a gazdasági helyzet romlása és Észak-Írország. A recesszió mindenekelőtt a munkanélküliség növekedésével párhuzamosan a közbiztonság alakulására volt hatással, míg a sztrájkmozgalmak – az év elején az útlevelhatóság munkabeszüntetése, a vámosságok sztrájkja⁵² – a hivatali ügyvitelt befolyásolta negatívan. Az északir helyzet ugyanakkor érezhetően idegességgel járt a biztonsági erőknél. A metró utasait az őrizetlenül hagyott csomagok veszélyére figyelmeztették, de a terrortámadás veszélyére való tekintettel a Scotland Yard megerősítette a rendőrfárőröket. „Tolnai” szolgálati járművének bal hátsó kereke május 16-án kétszer is defektet kapott, pedig 1979–1980-ban erre egyszer sem volt példa. A hónap végéig hívatlan látogatók többször is tiszteletüket tették a lakásában, ugyanakkor a rezidens három alkalommal is tapasztalta, hogy rejtett figyelés alatt áll.⁵³ 1981. augusztus 11-én Kovács Endre

⁴⁹ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 5/4–11/81. sz. jelentés – Tárgy: Láposiék operatív helyzete. – London, 1981. május 19. 106–107.o.

⁵⁰ WILKINSON, Micahel D: The Chile Solidarity Campaign and British Government Policy towards Chile, 1973-1990. *European Review of Latin American and Caribbean Studies*, June 1992. 57–74.o.

⁵¹ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 5/4–11/81. sz. jelentés – Tárgy: Láposiék operatív helyzete. – London, 1981. május 19. 106–108.o.

⁵² EGEDY 1998, 390–400.

⁵³ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 5/3–2/81. sz. jelentés – Tárgy: Az operatív helyzet alakulása. – London, 1981. május 21. 98–99. o.

kereskedelmi kirendeltségvezető feleségét egy Christopher John néven bemutatkozó férfi zaklatta. Kovács Endréné egy padon pihent a nagykövetséghez közeli parkban, amikor az úriember odament hozzá, és ismerkedési jelleggel társalogni kezdett vele, ám egyszer csak a vallása után érdeklődött. Először egy témába vágó, magyar nyelvű könyvet mutatott, majd politikai témákkal huzakodott elő, végül későbbi találkozásra és vacsorameghívásra célozgatott. Kovácsné megpróbálta elhárítani az illető törekvéseit, hangsúlyozta, hogy nem vallásos, ezért nem kíván a témáról beszélgetni, és nem akar a jövőben az illetővel találkozni. A férfi másfél órán keresztül feltartóztatta, miközben egy nő rájuk szólt, hogy ne beszélgessenek ily hangosan. A Kovács házaspár ezt egyértelmű provokációként interpretálta, amit nem véletlenül, hanem tervszerűen hajtottak végre. Megállapításukat azzal támasztották alá, hogy a szabadságukról visszatérve lakásukban idegenek nyomait és a falon többfelé is sérüléseket fedeztek fel. Blahó a beszámolóról úgy vélte, hogy az figyelemreméltó, ám csak ebből még nem tud hitelt érdemlő következtetést levonni. „Tolnai” viszont egyértelműen nyílt provokációként tekintett a történetekre.⁵⁴

Nem sokkal később a FCO kiutasította Viktor Lazin szovjet nagykövetségi első titkárt, aki Liverpoolban kapcsolatba lépett az PIRA (Provisional Irish Republican Army – a szakadár Ideiglenes Ír Köztársasági Hadsereg) egyik tagjával, aki az MI6 informátora volt.⁵⁵ A feszültté vált helyzetben a nagyjából 160 fős magyar kolónia – a nagykövetség, kereskedelmi kirendeltség és vegyes vállalatok delegáltjai, valamint az ösztöndíjasok és munkavállalók – ellenőrzését egyébiránt alaposan megnehezítette, hogy tagjai nem alkottak egységes közösséget, munka- és lakóhelyük területileg szétszórtan helyezkedett el. Az elszigetelődés különösen a magányos titkárnőkre volt veszélyes, akik, mint azt konkrét esetek is bizonyították, erőteljesen ki voltak téve a brit és az amerikai különleges szolgálatok támadásainak. A kint élő magyarok körében erős angol befolyás érvényesült, amely a fogadó ország kultúrája és politikai modellje iránti elfogultságot jelentette. Ezzel egy időben a brit hírközlő szervek propagandája, amely mindenekelőtt a lengyelországi eseményekre koncentrált, sem maradt hatástalan.⁵⁶ Az MI5 ekkor a terrorizmus elleni küzdelemre való tekintettel egy időre eltűnt a rezidentúra látóköréből, miután október 10-én az IRA az Irish Guard (a Királyi Ír Gárda) főhadiszállásának (Chelsea Barracks) közvetlen közelében szöges bombát robbantott. A merényletben ketten meghaltak, ötvenen megsebesültek.⁵⁷ Igaz, a Kovács házaspár lakásában talált nyomok tüzetesebb vizsgálatából ekkorra egyértelműen kiderült, hogy távollétükben többször hivatlan látogatók jártak náluk.⁵⁸

⁵⁴ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 7/3–2/81. sz. jelentés – 67/53–1768/81– 439–163/81 – Tárgy: Kovácsék ügye. – London, 1981. augusztus. 14. 117–118. o.

⁵⁵ DEACON, Richard: 'C'. *Maurice Oldfield. Head of MI6*. Futura Book, London, 1985. 235. o.

⁵⁶ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – Tárgy: Anglia kolónia védelmi terv. – Budapest, 1981. szeptember 15. 135–138.o.

⁵⁷ WILSON, Ray – ADAMS, Ian: *Special Branch: A History: 1883–2006*. Biteback Publishing Ltd., London, 2015. 326–329. o.

⁵⁸ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 9/7–2/81. sz. jelentés – Tárgy: Kovácsné ügye. – London, 1981. október 13. 119/158. o.

Az elhárítás aktivizálódása 1982-ben

A biztonsági helyzettel kapcsolatos felvetés korántsem volt alaptalan, tudniillik 1982. január 22-én Kádár László MEDIMPEX képviselő bejelentette az ügyeleten, hogy betörték a lakásukba, amiről már értesítette a rendőrséget. Kádár a nagykövetség biztonsági felelősének úgy nyilatkozott, hogy aznap este egy fél nyolckor kezdődő tévéműsor miatt siettek a hazatéréssel, de már távolról feltűnt, hogy ég a villany. A szemmel láthatóan sérült ajtót nyitva, lakásukat pedig feldúlt állapotban találták. A tettes mindössze két ékszerszett vitt magával, amelyek családi emlékek voltak. A rendőrség öt percen belül megérkezett, de a helyszínelésre két napot kellett várni. Kádár az ingatlan átvizsgálásakor lehallgató készüléket nem talált, ezért a behatolásra köztörvényes bűncselekményként tekintett, „Tolnai” azonban az égve hagyott villanyra és a csekély értékű kárra való tekintettel az elhárítás figyelmeztetését vélte az akció mögött felfedezni.⁵⁹ 1982. március 23-án délelőtt az EYT 153 V rendszámú gépkocsi megállt a nagykövetség előtt a Belgravia felőli oldalon. A jármű utasa kiszállt, és a szemközti sarokból több felvételt is készített az épületről. A rezidens szerint az MI5 felbukkanása nem véletlenül történt,⁶⁰ ugyanis április 5-től a nagykövetség fokozatosan visszaköltözött az Eaton Place 35. szám alatti palotába.⁶¹ Időközben az MNVK2-t súlyos veszteség érte, ti. John Szmolka, a US Army (az USA hadserege) híradós tiszthelyetteséről kiderült, hogy az INSCOM (Intelligence and Security Command – az Egyesült Államok Hadseregének Hírszerző és Védelmi Parancsnoksága) irányítása alatt álló kettős ügynök volt. Gilbert Attila 1956-os emigránst, aki összekötői feladatot látott el Szmolka és az MNVK2 között, 1982. április 19-én a Georgia állambeli Augusta-ban az FBI, az amerikai katonai elhárítás és a városi rendőrség kémkedés gyanújával őrizetbe vette.⁶² Az eseményt követően a londoni rezidentúra biztonsági helyzete is negatívan változott. A titkos munkatársak egyre inkább azt tapasztalták, hogy a két évvel azelőtti eseményekhez hasonlóan ismét a magyar kolónia került célkeresztbe. Április 13-án Kovács Katalin, a Kereskedelmi Kirendeltség egyedülálló munkatársnője lakásáról eltűnt az összes, 12-én vásárolt hetilap. Egy héttel később pedig azt konstataálta, hogy egy nem sokkal azelőtt megbontott üveg ital tartalma egyik pillanatról a másikra szinte teljesen eltűnt. „Tolnai” április 26-tól egyre több alkalommal is érezte, hogy konspiráltan követik. Az elhárítást csak akkor sikerült tetten érnie, amikor a május 8-i KISZ-rendezvényre indult volna, de gépkocsijának bal hátsó kerekéből – amely egy év alatt már ötször volt lyukas – egy három centiméteres facsavar állt ki. Az autó délután négy és fél hat között álló helyzetben kapott defektet, ugyanakkor valaki a belső visszapillantó tükört időnként eltekerte. Május 9-én este az ügyeletesi szolgálatban 11 körül többször is felhívták, majd anélkül, hogy beleszóltak

⁵⁹ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 2/3–2/82. sz. jelentés – Tárty: Behatolás egy magyar lakásba. – London, 1982. február 23. 201–202. o.

⁶⁰ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 4/8–2/82. sz. jelentés – Tárty: A követség fényképezése. – London, 1982. május 13. 247.o.

⁶¹ TNA FCO 28/4901 ENH 400/1 Hungarian Diplomatic Representation in UK. No. 70/1982 4th April 1982.

⁶² MOZSIK Imre: *Washingtoni emberünk. Hírszerző voltam Amerikában.* Más Könyvek, Budapest, 1995. 37-49. o.

volna, letették a telefont. Másnap este Fodor László, az új sajtóattasé,⁶³ ugyanezt tapasztalta: őt 9:30-kor, 11:20-kor, végül hajnali egy órakor keresték, de a hívó fél egyből kilépett a vonalból, amint felvette a kagylót. Két nappal később „Tolnai” lakását távollétében valaki megtisztelte látogatásával, aki ráadásul a mosdó használatával gondoskodott arról, hogy ottlétének nyoma maradjon. 1982. május 13-án, pénteken ismét Kovács Katalin volt az áldozat, akit ebédidőben lakásán megkeresett egy Thomson nevű férfi. Ő azt állította, hogy a titkárnője által megbeszélte találkozóra jött. Ám a kirendeltség dolgozója átlátott a szitán, és rákérdezett, hogy miről van szó. A férfi ekkor zavarba jött, és tisztességes válasz helyett kijelentette, hogy újabb időpontot fog kérni a titkárnőjén keresztül, majd eltávozott. A rezidens május 16-án vasárnap délelőtt a Victoria pályaudvarra ment újságért, amikor az állomás előtt elhaladva arra lett figyelmes, hogy valaki azt mondja angolul: „itt megy a harmincötös”. Ahogy később hátrafordult, és észrevette, hogy egy 50-55 év körüli férfi egy kávéspohárral a kezében a fal mellett állt, és úgy beszélt, hogy senki nem volt ott rajta kívül. Hajdút aznap éjjel 11:30-kor háromszor is felhívták. Először egy női hang jelentkezett, aki egy bizonyos személlyel óhajtott volna beszélni, ám a másik két alkalommal már nem szólalt meg, hanem rövid úton kilépett a vonalból. Május 16-án vasárnap délután négy óra és negyed öt között, amikor a Buckingham-palota környéke tele volt turistákkal, az ismeretlen tettes kővel betörte Fodor autóján az első ablakot, és elvitte Fodorné táskáját. Három nappal később az islingtoni rendőrös hajnali három órakor felhívta a nagykövetségi ügyeleten Tállai Benedek kereskedelmi titkárt (fn. „Bedési”),⁶⁴ akivel közölték, hogy felesége táskája és a háromdarabos kulcskészlet átvehető náluk. Az új hivatalvezető Biliczki László (fn. „Borsos”) gépkocsiját május 19-én és 20-án egész nap követte egy fekete Mini Morris, amelyben egy fiatal férfi és egy nő ült. Szabadosné eközben arról panaszkodott, hogy nemrég eltűnt egy csirke a hűtőszekrényükből. Reggel még többen látták, de mire meg akarta főzni, már híre-hamva sem volt. Kallós feleségének egyszer csak a baloldalon sikerült parkolni, és ott is csak hosszas manőverezés után, viszont reggel az autót az utca másik oldalán találta. Kallós egy másik esetben azzal szembesült, hogy a vezető melletti ülés háttámláját rögzítő csavar kiesett, ami így hátradőlt, pedig este még érintetlen volt. Június elsején Sütő Katalin telefonkezelőt⁶⁵ éjjel fél egy után többször is felhívták, de nem szóltak bele a készülékbe, ami egy héttel később a rezidenssel is megismétlődött az éjszakai ügyelet folyamán. Lukács doktornőt, aki négy hónapos ösztöndíjjal dolgozott egy londoni kórházban, május 9-én éjjel a telefonközpont értesítette, hogy magyarországi hívást kapcsol, ám egy artikulálatlan hang hosszabb időn keresztül zaklatta, végül június 10-én a dolgozószobájának asztaláról ellopták a retiküljét. A rezidens szerint a fenti eseménysor egyértelműen azt igazolta, hogy a brit elhárítás 1982 áprilisától aktív, időszakos ellenőrzés alá vonta a magyar külképviselet és a kirendeltség személyi állományát, amely a szokatlan események gyakoriságából és sűrűsödéséből

⁶³ MNL OL–XIX–J–1–j – SZT Iratok Anglia 1982 – 26. doboz – 003869 – 53/661982 – Tárgy: Fodor László elvtárs 1982. évi beszámoló jelentése. – London, 1982. május 21. 1–6. o.

⁶⁴ ÁBTL 3.2.1–Bt2114 – „Bedési” (Tállai Benedek) – Évkör: 1980–1987.

⁶⁵ ÁBTL 3.2.5–O–8–0467/2–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 3/2–11/80. sz. jelentés – Tárgy: A londoni magyar kolónia. – London, 1980. március 17. 8. o.

következett. Az MI5 létszámgondjai miatt csak félévente, míg az átfogó, hosszabb ideig tartó elhárítási műveletekre másfél–kétévente került sor. A rezidentúra és a katonai attaséi hivatal a szakmai tevékenységet korlátozó intézkedésekkel tervezte folytatni, miközben az elhárítás feltételezett lépéseinek elemzésével döntött arról, hogy szüksége van-e az operatív műveletek felfüggesztésére.⁶⁶

Az 1982-es év legfontosabb konzuli ügyei

Június első napjaiban „Tolnai” a Gay Hussar (Vidám Huszár) nevű magyar étteremben – amely korrekciós árjai és az udvarias kiszolgálás jóvoltából komoly népszerűségnek örvendett, ugyanakkor Mr. Albert – a tévesen magyar származásúnak vélt – baloldali érzelmű tulajdonos jóvoltából évtizedek óta a brit Munkáspárt és a szak szervezeti vezetők törzshelyeként működött⁶⁷ – összefutott egy akkor 22 esztendő, győri születésű felszolgálóval. Horváth Péter az iránt érdeklődött: igaz-e, hogy amnesztiában részesítették a disszidenseket, azaz öt év letelte előtt is hazautazhatnak. A rezidens türelmet kért, majd pár héttel később cáfolta az értesülést. A pincér nagyon el volt keseredve, hogy 1985 előtt nem utazhat be Magyarországra. „Tolnai” azt vette ki a fiatalember megnyilatkozásaiból, hogy a politika nem érdeklődik, ellenséges megnyilvánulásai nincsenek, viszont könnyen befolyásolható. Ezért azt javasolta, hogy otthon minél előbb készítsék el a róla szóló környezettanulmányt, amely, ha pozitív eredményt hoz, érdemes lenne Horváth személyével foglalkozni.⁶⁸

A rezidentúra ugyanakkor felterjesztette Peter Coello köztisztviselő személyét, aki a volt iskolatársnő, Fasching Andrea – Fasching Iván II. osztályú kereskedelmi titkár lánya⁶⁹ – budapesti címén tartózkodott magyarországi útja alkalmával.⁷⁰ A konzuli kutatómunka jelentős hangsúlyt helyezett a brit rendőrség tisztviselőire, azonban a félfogadás keretében mindössze egy személy tűnt érdekesnek. Kátay Imre József a Metropolitan Police polgári alkalmazottja, építészmérnök volt, akinek operatív meghallgatását Szabó Gellért a KEOKH (Külföldiek Ellenőrző Országos Központi Hatóság) fedésében végezte. Kátay az 1956-os menekülthullámmal érkezett Ausztráliába. Az első két és fél év alatt egy építőipari magánvállalkozásnál dolgozott Canberrában, ahonnan az állami tulajdonú vízművekhez került. 1969-ben Angliába költözött, ahol a Scotland Yardnál karbantartási és átépítési feladatokkal foglalkozott, más kötődése azonban nem volt a rendőrséghez. A korára való tekintettel évente kellett kérvényeznie, hogy tovább dolgozhasson, mivel már elmúlt 60 éves. A két lánya Budapesten járt orvosi egyetemre, így ő maga is kötődött Magyarországhoz, de

⁶⁶ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 5/2–2/82. sz. jelentés – Tárgy: Biztonsági helyzetünk. – London, 1982. június 16. 260–267/241–243. o.

⁶⁷ Interjú Sárközi Mátyással, 2018. január 18.

⁶⁸ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 5/7–2/82. sz. jelentés – Tárgy: Horváth Péter ügye. – London, 1982. június 16. 275–276. o.

⁶⁹ TNA FCO 28/2887 NH 400/548/1 – Diplomatic Representation of Hungary in the United Kingdom 1976. 18/10/76.

⁷⁰ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – 5/4–2/82. sz. jelentés – Tárgy: Peter Coello ügye. – London, 1982. szeptember 17. 298. o.

apolitikus magatartására és a nyugati életformához alkalmazkodó gondolkodásmódjára való tekintettel Szabó főhadnagy nem tartotta célszerűnek, hogy perspektivikus céllal foglalkozzanak az építéssel.⁷¹

Utószó

Amellett, hogy a jelen tanulmány bizonyos képet ad a londoni rezidentúra mindennapi életéről, korlátozott hírszerzési lehetőségeiről és szakmai kihívásairól a 80-as évek elején, az olvasó könnyen úgy érezheti, hogy közvetlen előzmény nélküli pillanatképpel van dolga, mivel a történetből a 70-es évek előzményei és az 1982 utáni szűk egy évtized krónikája egyaránt kimaradt. A kritika egyáltalán nem alaptalan, de a rendelkezésre forrásanyag hiányosságai következtében szélesebb ív felvázolására nem volt lehetőség. A magyarázat a következő.

Míg az 1951-től 1965-ig Nagy-Britannia az állambiztonság égisze alatt működő hírszerzőszolgálat második legfontosabb célpontjának számított,⁷² 1973 novemberétől a londoni rezidentúra a III/I-11-es Osztályhoz került,⁷³ amely harmadik országos és hazai bázison végzett hírszerzést.⁷⁴ 1975-től Takács Dezső rendőr őrnagy, a nagykövetség műszaki-tudományos titkára volt az egyetlen hivatásos tiszt a rezidentúrán, aki a jellemzése szerint a nehézségek ellenére is jó kapcsolatot alakított ki a brit egyetemekkel és az ott dolgozó szakemberekkel.⁷⁵ Takács őrnagy tevékenysége mindenekelőtt az agrárfelsőoktatásra irányult,⁷⁶ így könnyen lehetséges, hogy Stella Rimington emlékiratában róla tesz említést. *„Egy keleteurópai hírszerző például a tartós ételek elkészítésének technológiáját kísérte meg megszerezni. Bár kész volt nagyobb összeget kifizetni, sok nehézsége támadt az információforrásokkal. Ezek a «csirkekrém»-akciók komoly károkat ugyan nem okoztak, de veszélyeztették az érintett társaságokat, cégeket”.*⁷⁷ Az ÁBTL brit vonatkozó iratanyaga a 70-es évek második felét illetően igencsak szórványos, ebből általános következtetést nem lehet levonni. A „Boby” fedőnevű iratcsoportból a harmadik és a negyedik kötet már kutatható, a második viszont nem került a levéltárba, feltehetően a benne lévő minősített információk miatt. Tudniillik, Belovai Istvánt, a londoni magyar katonai attasé helyettesét 1985-ben a CIA számára

⁷¹ ÁBTL 3.2.5–O–8–0467/1–15–OD–4890 – „BOBY” – Angliai magyar kolónia operatív védelme – Belügyminisztérium III/I. Csfség 2-es Osztálya – Tárgy: Kátay Imre meghallgatásáról. – Jelentés. Budapest, 1982. október 5. 326–328. o.

⁷² UNGVÁRY Krisztián: „Anglia a második legnagyobb ellensége Magyarországnak”. A londoni magyar hírszerző rezidentúra saját jelentései tükrében 1951 és 1965 között. *Századok*, 2013/6. 1513–1561. o.

⁷³ ÁBTL – 3. 2. 5 – O – 8 – 016/6/3 – 15 – OD – 2810 – „Medúza” – Londoni Magyar Követség és Konzulátus – Tárgy: Dosszié megszüntetésére JAVASLAT. – Budapest, 1974. VII. 30. 210. o.

⁷⁴ TÓTH 2013, 425.

⁷⁵ ÁBTL – 2. 8. 2. 1 – 469 – Takács Dezső r. alez. – Minősítés. – Budapest, 1979. IV. 9. 11–12. o.

⁷⁶ MNL OL – XIX – J – 1 – j – Anglia 1975 – 32 – es d. – I – 19 – 004343 – Tárgy: Takács Dezső műszaki – tudományos beosztott beszámoló jelentése. – London, 1975. VII. 4. 1–7. o.

⁷⁷ RIMINGTON, Stella: *Nyílt titok. A brit kémelhárítás volt főigazgatójának emlékiratai*. Geopen Könyvkiadó, Budapest, 2004. 164–165. o.

folytatott kémkedés miatt a Legfelsőbb Bíróság Katonai Tanácsa életfogytiglani börtönbüntetésre ítélte. Az egykor alezredes 1990-ben kegyelemmel szabadult, majd az USA-ba távozott,⁷⁸ végül 2009. november 6-án hunyt el a Colorado állambeli Denverben.⁷⁹

Felhasznált irodalom

ANDREW, Christopher: *The Defence of the Realm. The Authorized History of MI5*. Allan Lane, London, 2009. ISBN: 978 0 71399885 6

ARDAY Lajos: *Az Egyesült Királyság és Magyarország. Nagy-Britannia és a magyar-angol kapcsolatok a 20. században*. Mundus Magyar Egyetemi Kiadó, Budapest, 2005. ISBN: 963 9501 40 9

ASHER, Michael: *The Regiment. The Real Story of the SAS*. Penguin Books, London, 2008. ISBN: 978-0-141-02652-7

BÁTONYI, Gábor: 'Creative Ferment in Eastern Europe': Thatcher's Diplomacy and the Transformation of Hungary in the Mid-1980's. *Diplomacy & Statecraft*, 2018/4.

BELOVAI István: *Fedőneve: SCORPION*. Belovai István, Budapest, 1998. ISBN: 963 550 672 4

DEACON, Richard: 'C'. *Maurice Oldfield. Head of MI6*. Futura Book, London, 1985. ISBN: 0 7088 2878 7

DORRIL, Stephen: *The Silent Conspiracy. Inside the Intelligence Services in the 1990's*. Heinemann, London, 1993. ISBN: 0 434 20162 6

EGEDY Gergely: *Nagy-Britannia története*. Aula, Budapest, 1998. ISBN: 963 9078 85 9

HORN, Bernd: *A Most Ungentlemanly Way of War. The SOE and the Canadian Connection*. Dundurn, Toronto, 2016. ISBN: 978-1459732797

JEFFERY, Keith: *MI6. The History of the Secret Intelligence Service*. Bloomsbury, London, 2011. ISBN: 978-1-4088-10057.

KENYERES Ágnes (főszerk.): *Magyar Életrajzi Lexikon (1978–1991)*. Akadémiai Kiadó, Budapest, 1994. ISBN: 963-05-6422x

MOZSIK Imre: *Washingtoni emberünk. Hírszerző voltam Amerikában*. Más Könyvek, Budapest, 1995. ISBN: 9632083458

RIMINGTON, Stella: *Nyílt titok. A brit kémelhárítás volt főigazgatójának emlékiratai*. Geopen Könyvkiadó, Budapest, 2004. ISBN: 0219003733475 2

⁷⁸ BELOVAI István: *Fedőneve: SCORPION*. Belovai István, Budapest, 1998.

⁷⁹ Sz.n.: *Meghalt Belovai István, az első magyar NATO-kém. Heti Világgazdaság*, 2009. november 6.

SANDERSON, Michael: *The History of the University of East Anglia Norwich*. Continuum, London, 2002. ISBN: 978-1852853365

Sz.n.: Meghalt Belovai István, az első magyar NATO-kém. *Heti Világgazdaság*, 2009. november 6. Elérhető: https://hvg.hu/itthon/20091106_meghalt_belovai_istvan (Letöltés ideje: 2025.01.31)

TILLOTSON, Michael (szerk.): *SOE and the Resistance. As told in The Times Obituaries*. Bloomsbury, London, 2011. ISBN: 978-1441119711

TÓTH Eszter 2013: A politikai és gazdasági hírszerzés szervezettörténete, 1945–1990. In: CSEH Gergő Bendegúz–OKVÁTH Imre (szerk.): *A megtorlás szervezete. A politikai rendőrség újjászervezése és működése, 1956–1962*. Állambiztonsági Szolgálatok Történelmi Levéltára–L'Harmattan, Budapest, 2013. ISBN: 1586 9784

UNGVÁRY Krisztián: „Anglia a második legnagyobb ellensége Magyarországnak”. A londoni magyar hírszerző rezidentúra saját jelentései tükrében 1951 és 1965 között. *Századok*, 2013/6.

WILKINSON, Micahel D: The Chile Solidarity Campaign and British Government Policy towards Chile, 1973-1990. *European Review of Latin American and Caribbean Studies*, June 1992.

WILSON, Ray – ADAMS, Ian: *Special Branch: A History: 1883–2006*. Biteback Publishing Ltd., London, 2015. ISBN: 978-1-84954-910-3

NEUSPILLER FERENC¹

„LEGGYENGÉBB LÁNCZEMBŐL” A NATO „DÉLI FELLEGVÁRA” OLASZORSZÁG HELYZETE A NATO-N BELÜL 1975-1985.

A hidegháborús enyhülés csúcspontja az 1975-ben záródó helsinki konferencia volt. Ezt követően az Egyesült Államok és a Szovjetunió kapcsolata negatív irányt vett, ami azt eredményezte, hogy minkét szuperhatalom igyekezett megerősíteni pozícióit a nemzetközi térben. Ez természetesen hatással volt a két katonai blokk, a Varsói Szerződés és a NATO tagállamaira is. A NATO egyik alapító tagjaként Olaszország komoly fejlesztéseket hajtott végre az 1970-es évek végén és az 1980-as évek elején, ami elsősorban légierőjének és haditengerészetének a modernizálását eredményezte. Ennek eredménye olyan vadászrepülő és hadihajó megalkotása lett, amelyek még a 2010-es években is szolgálatban álltak. A fejlesztések, az amerikai és német támaszpontok bővítése, majd az 1980-as évek elején az országba telepített amerikai rakéták következtében Olaszország a NATO „déli fellegvárává” vált. A tanulmány azt mutatja be, hogyan lett Olaszország az Atlanti Szövetség egyik meghatározó állama, és mindeközben hogyan alakultak az amerikai–olasz, illetve a német–olasz kapcsolatok.

Kulcsszavak: Olaszország, NATO, kis hidegháború, fegyverkezés, nemzetközi kapcsolatok

FROM „THE WEAKEST LINK” TO NATO’S „SOUTHERN CITADEL” THE POSITION OF ITALY WITHIN THE NATO 1975-1985.

The peak of the Cold War’s détente was the Helsinki Summit, which ended in 1975. Afterwards, the relationship between the United States and the Soviet Union took a negative turn, resulting in both superpowers seeking to strengthen their positions in the international arena. This of course had an impact on the two military blocs, the Warsaw Pact and on the member states of the NATO. As one of the founding members of NATO, Italy undertook major developments in the late 1970s and early 1980s, which resulted in the modernisation of its air force and navy in particular. The result was the creation of such fighter aircrafts and warships that were still in service in 2010. Developments, expansion of US and German bases, and the US missiles deployed in the early 1980s made Italy NATO’s „southern citadel”. The study shows how Italy became a significant state in the Atlantic Alliance, and how American-Italian and German-Italian relations have evolved in the meantime.

Keywords: Italy, NATO, Little Cold War, armaments, international relations

¹ ORCID-azonosító: 0009-0006-9191-3279

Bevezetés

1973. július 3-án Helsinkiben harminchárom európai és két amerikai ország jelenlétében megnyitották az Európai Biztonsági és Együttműködési Értekezletet (a továbbiakban: EBEÉ). A július 3-7-ig tartó nyitó szakaszon a jelenlévők kifejtették elképzeléseiket az európai biztonság modelljéről, majd az 1973. szeptember 10-től 1975. július 21-ig Genfben megrendezett második szakaszban a 35 állam közötti kapcsolatok irányító elveiről és előírásairól állapodtak meg. Az EBEÉ ünnepélyes zárószakaszára megint csak a finn fővárosban került sor 1975. július 31. és augusztus 1. között. A záróokmány első kosarába biztonságpolitikai és katonai aspektusok kerültek, a második kosár a gazdasági, technikai, környezetvédelmi együttműködésről, míg a harmadik kosár a humanitárius területekről, emberi jogokról és a mediterrán térségben való együttműködésről szólt.²

Helsinki után még számos utókonferencia következett annak érdekében, hogy a részleteket és a további együttműködés feltételeit tisztázni tudják. Az első utókonferenciát 1977. október 4. és 1978. március 8. között Belgrádban, a másodikat 1980. szeptember 9. és 1983. szeptember 6. között Madridban rendezték. Ez a két konferencia azonban nem váltotta be a hozzá fűzött reményeket. A jugoszláv fővárosban rendezett találkozón a 109 betervezett javaslat nagy részét nem fogadták el, míg a spanyol fővárosban a vitákat több alkalommal is fel kellett függeszteni a feszült nemzetközi viszony miatt. Áttörést csak a harmadik utótalálkozón sikerült elérni, amit 1986. november 4. és 1989. január 19. között Bécsben rendeztek.³ A találkozó helyszínei jól jelzik, hogy a konferenciákat igyekeztek olyan országokban megrendezni, amelyek nem álltak szoros kapcsolatban egyik blokkal sem. Ez alól kivétel a spanyol főváros, hiszen Spanyolország pont a konferencia alatt, 1982-ben csatlakozott a NATO-hoz. Ez természetesen azt eredményezte, hogy a spanyol elhárítás komolyabb ellenőrzés alá vonta az ott tevékenykedő kelet-európai diplomatákat.⁴

Időközben ráadásul egyre feszültebbé vált a nemzetközi helyzet. Az Afganisztánban zajló polgárháborúra reagálva a Szovjetunió 1979. december 12-én döntött a katonai megszállás mellett. 15 nappal később, december 27-én meg is indult a szovjet támadás Szokolov marsall vezetésével, és bár a városokat megszállták, a kommunikációs központokat és közlekedési csomópontokat elfoglalták, illetve sikeresen lefejezték az afgán kormányt, a lakosság országos felkelést robbantott ki a megszállók ellen. Mivel a szovjet hadsereg nem volt felkészülve a terepviszonyokra, az éghajlatra és az ellenséges erők ellenállására, az afganisztáni háború tíz évig elhúzódott. Ez többek között a korábban az afgán lázadóknak amerikai pénzen vásárolt fegyvereknek, illetve

² HORVÁTH Jenő – PARAGI Beáta – CSICSMANN László: *Nemzetközi kapcsolatok története 1941-1991*. Antall József Tudásközpont, Budapest, 2014. 212-214. o.

³ GHEBALI, Victor-Yves: Az EBEÉ fejlődése Helsinkitől Párizsig (1975-1990.) In: DUNAY Pál – GAZDAG Ferenc (szerk.): *A helsinki folyamat: az első húsz év. Tanulmányok és dokumentumok*. Zrínyi Kiadó, Budapest, 1995. 38-45. o.

⁴ PÁL István: A madridi rezidentúra – A magyar hírszerzés Spanyolországban a detente csúcspontjától a kishidegháború végéig 1976-1984. *Nemzet és Biztonság*, 2020/3. 119-120. o.

a vidéki papság által kihirdetett dzsihadnak volt köszönhető, amelynek következtében a mudzsahedineknek nevezett afgán harcosok sikerrel vették fel a küzdelmet a szovjet hadsereggel szemben.⁵ Az afganisztán szovjet támadás után alig fél évvel Lengyelországban, 1980 júliusában sztrájkok kezdődtek, majd egy hónappal később megalakult az Üzemközi Sztrájkbizottság Lech Walesa vezetésével. Augusztus végén az Üzemközi Sztrájkbizottság és a kormány megállapodásának értelmében független szakszervezetek jöhettek létre, melyek később egy szervezetben egyesültek, a Szolidaritás Független Önkormányzó Szakszervezetben. A Szolidaritás népszerűségét jelzi, hogy 1981 októberében már tízmillió tagja volt. Az eseményekre válaszul Jaruzelski miniszterelnök 1981. december 13-án hadiállapotot vezetett be az országban, amelynek során tízezer embert internáltak.⁶

A feszült nemzetközi helyzet miatt a két szuperhatalom kapcsolata megromlott, ami hatással volt mind a Varsói Szerződés, mind a NATO tagállamaira, így Olaszországra is. Olaszországra a NATO-nak és az Egyesült Államoknak szüksége volt annak érdekében, hogy a földközi-tengeri pozícióit meg tudja erősíteni. Ezt a helyzetet Róma igyekezett kihasználni, és elsősorban amerikai és német segítséggel erősítette hadseregét, illetve megpróbálta súlyát és szerepét növelni a Szövetségben belül. Ennek köszönhetően, míg az 1970-es évek elején Olaszországot még többen a NATO leggyengébb láncszemének tartották, addig az 1980-as évekre az Atlanti Szövetség egyik meghatározó államává nőtte ki magát.

Olaszország növekvő szerepe

A feszült nemzetközi helyzet következtében kiemelt jelentőségűvé vált a Földközi-tenger térsége, amely több korabeli jelentés szerint is a NATO erőinek leggyengébb pontja volt. A mediterrán országok belső problémái miatt az Atlanti Szövetség déli szárnyának legerősebb állama Olaszország volt, amelyet katonai potenciáljának növelésével Brüsszel igyekezett egyfajta „katonai fellegvárrá” alakítani. Az ország meglehetősen nagy katonai súlyát stratégiai jelentősége és NATO-ban betöltött szerepe szolgáltatta, hiszen közel fekszik mind a Varsói Szerződés déli szárnyához, mind Jugoszláviához, és összekötő kapocsként szolgál a NATO középső és déli szárnya között.⁷

Ezeket a szempontokat figyelembe véve nem meglepő, hogy Magyarországon megnőtt az érdeklődés Olaszország irányába. A magyar felsővezetés két forrásból számíthatott információra Olaszország vonatkozásában. Az egyik a római magyar nagykövetség volt, amely elsősorban az olasz sajtóból és olasz politikusokkal folytatott magánbeszélgetésekből szerzett értesüléseket. Ebből kifolyólag a nagykövetség nyílt információkat szállított. Ennek háttérében az állhatott, hogy 1970-ben elhagyta Magyarországot a korábbi római nagykövet, Száll József, akiről kiderült, hogy tagja volt

⁵ VARGA Csaba Béla: Afganisztán a legyőzhetetlen. Kelet Kiadó Kft., Budapest, 2010. 190-198. o.

⁶ BURAKOWSKI, Adam – GUBRYNOWICZ, Aleksander – UKIELSKI, Pawel: 1989. *A kommunista diktatúra végnapjai Közép-és Kelet-Európában*. Rézbong Kiadó, Budapest, 2014. 50-52. o.

⁷ Magyar Nemzeti Levéltár Országos Levéltára (MNL OL) XIX-J-1-j Olaszország KÜM TÜK 1975/109. Feljegyzés, Budapest, 1975. október 20. 3-4. o.

a P2 nevű, olasz politikusokat, államtitkárokat, újságírókat és az olasz kémelhárítás magas rangú személyiségeit magába tömörítő szabadkőműves páholynak,⁸ így félt volt, hogy az olasz kémelhárítás alaposabban szemmel tartja a magyar nagykövetség dolgozóit. A másik forrás egy a magyar hírszerzésnek dolgozó német újságíró volt, aki a „Von Schiller” fedőnevet kapta. „Von Schiller” kapcsolatait kihasználva nem csak az olasz kormány és a római amerikai nagykövetség munkatársaival ápolt szoros viszonyt, de bejárása volt az olaszországi NATO-körökbe is, így titkos, belső adatokat tudott szivároztatni a magyar vezetésnek.

Olaszország fontosságát hangsúlyozta Ford amerikai elnök, aki a NATO egyik ülésén a Földközi-tenger kérdéseinek vizsgálata közben kijelentette, hogy a térség haditengerészeti fejlesztésében egyedül Olaszország vállal szerepet, illetve Luns, a NATO főtitkára is, amikor 1975-ben az országba látogatott.⁹ Látogatása során Luns Nápolyban tartott sajtótájékoztatóján a CINCSOUTH¹⁰ és az AFSOUTH¹¹ vizsgálatok kijelentette, hogy a déli térségben a NATO célja a légi fölény biztosítása, mely védelmet jelent mind a katonai célpontoknak, mind a civil lakosságnak, mind a hadiiparnak. Az itt elhelyezkedő egységek ismertetésekor kitért arra, hogy a déli térségben elhelyezkedő nemzeti haderők öt alparancsnokság alá tartoznak. Az alparancsnokságok öt központja közül három található Olaszországban: Veronában a Szárazföldi Szövetséges Haderők Parancsnoksága, amely elsősorban Észak-Olaszország védelméért felelős, Nápolyban a Dél-Európai Haditengerészeti Erők Szövetséges Parancsnoksága, amelynek feladata a NATO kommunikációs vonalainak védelme a Földközi-tengeren, illetve szintén Nápolyban a Dél-Európai Szövetséges Légierők Parancsnoksága, amely a légvédelemért felel. Ezeket kiegészíti a Földközi-tenger haditengerészeti és tengeralattjáró elhárításáért felelős Dél-Európai Tengerészeti Parancsnokság (Commander of Naval Forces Southern Europe), vagyis a COMNAVSOUTH.¹²

Luns a beszédében ismertette a Földközi-tenger térségében szemben álló erők arányait is. Ezek szerint szárazföldi erők szempontjából az arány a NATO és a Varsói Szerződés között 1:2-höz, hiszen bár a szocialista országok hadosztályai kisebb méretűek, páncélozott egységeiknek köszönhetően mégis nagyobb ütőerőt képviselnek, míg a nyugati szövetség szárazföldi erejének régebbi a felszerelése, és kevésbé motorizált alakulatai vannak. Légierő esetében még rosszabb a helyzet, ugyanis itt 1:2,5-hez az arány, hiszen a Varsói Szerződés egységesített, modernebb

⁸ ANDREIDES Gábor: *Egy megbízható elvtárs. Száll József útja az MKP-tól a P2-ig*. NEB Könyvtár, Budapest, 2019. 211-212. o.

⁹ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1975/109. Jelentés, Róma, 1975. április 11. 4-7. o.

¹⁰ A CINCSOUTH (Commander-in-Chief Allied Forces Southern Europe) a Szövetséges Fegyveres Erők Dél-Európai Főparancsnoka. Lásd: DR. TÁLAS Péter (szerk.): *NATO kézikönyv*. HM Stratégiai Védelmi Kutató Hivatal, Budapest, 2001. 523. o.

¹¹ Az AFSOUTH (Allied Forces Southern Europe) a dél-európai szövetséges erők elnevezése. Lásd: KERESZTY András: *Tények könyve: NATO*. Greger-Delacroix, Budapest, 1997. 16. o.

¹² A COMNAVSOUTH a Dél-Európai Tengerészeti Parancsnokság (Commander of Naval Forces Southern Europe). Lásd: Sz.n.: *Allied Naval Forces Southern Europe (NAVSOUTH)*. GlobalSecurity.org, é.n.

felszerelésével minőségi fölényt képes kialakítani. Ennek ellensúlyozására a NATO erőfeszítéseket tesz, például modern gépeket szerez be, illetve kiépíti a NATO légvédelmi rendszerét, a NADGE-t (NATO Air Defence Ground Environment).¹³ A NATO főtitkára szerint az egyetlen fegyvernem, amiben a NATO jobban áll a Varsói Szerződésnél, az a haditengerészet, ahol az arány 3:2-höz. Annak érdekében, hogy a NATO csökkentsen hátrányát, a főtitkár szerint fejleszteni kell a logisztikát, a kiképzést, a gyakorlatokat, az összeköttetést, a légvédelmet és a felderítést is, majd kijelentette, hogy a rugalmas válasz doktrínája három tényezőtől függ: a magas fokú harckészültségen, az állóképességen és az atomerőn.¹⁴

A NATO megerősítése

A főtitkár által említett hátrány leküzdése azért is bírt nagy jelentőséggel, mert a magyar hírszerzéshez eljutott információk szerint a NATO azon munkálkodott, hogy a Földközi-tenger környékén kiterjessze érdekeltségi zónáját. Szakértők véleménye alapján ugyanis az azt megelőző két évben a NATO déli szárnya sebezhetővé vált, és a Védelmi Tervező Bizottság, illetve a Katonai Bizottság attól félt, hogy a görög–török helyzet¹⁵ és az összeköttetés, utánpótlás bizonytalansága miatt a Földközi-tenger keleti és középső övezete veszélyben van. A helyzetet tovább bonyolította, hogy az AFSOUTH számára megnehezült a szovjet hadiflotta figyelemmel kísérése. Ezen problémák kiküszöbölése érdekében „Von Schiller” szerint a NATO évente közel 200 hadgyakorlatot rendez, amelyeknek legalább a fele a Földközi-tengeren zajlik,¹⁶ míg az Egyesült Államok egy haditengerészeti készenléti osztag felállításán munkálkodik. A 6. flottától független egység az olasz partok mentén működne, és kapcsolódna a készenléti haditengerészeti egységhez, a NAVOCFORMED-hez (Naval On-Call Force Mediterranean). A tervek szerint az angol török, francia és olasz egységekkel kiegészített osztag repülőgép-hordozóval, torpedórombolóval, atom-tengeralattjáróval és hagyományos tengeralattjáróval rendelkezne.¹⁷

¹³ KERESZTY, 1997, 20.

¹⁴ Állambiztonsági Szolgálatok Történeti Levéltára (ÁBTL) 3.2.3 Mt-867/13. 46-56. o. Információs jelentés, Budapest, 1975. augusztus 2.

¹⁵ A két ország viszonya Ciprus kérdése miatt romlott meg. A szigeten a két etnikum között rendszeresek voltak a gyakran fegyveres összetűzésekbe torkolló konfliktusok, ezért 1963-ban létrehozták a „Zöld vonalat”, amely elválasztotta egymástól a görögök és a törökök által lakott területeket. 1974 júliusában viszont a görögországi katonai junta által támogatott ciprusi görög katonatisztek államcsínyt kíséreltek meg azzal a céllal, hogy Makarioszt megbuktassák és a szigetet egyesítsék Görögországgal. Pár nappal később az ott élő törökök védelmére hivatkozva Törökország csapatokat küldött Ciprusra, amelyek megkezdték az ország megszállását. Az 1974 júliusában a görög, török és brit részvétellel megrendezett genfi tárgyalásokon végül abban állapodtak meg, hogy a görögök és a ciprusi görög erők elhagyják a töröklakta területeket, és két autonóm adminisztrációt alakítanak ki Cipruson. Lásd: STEPHEN, Michael: *The Cyprus question. A concise to the history, politics, and law of the Cyprus Question*. Meto Print, London, 2001. 44-46. o.

¹⁶ ÁBTL 3.2.3 Mt-867/13. 76-79. o. Információs jelentés, Budapest, 1975. szeptember 23.

¹⁷ ÁBTL 3.2.3 Mt 867/13. 96. o. Információs jelentés, Budapest, 1975. október 27.

A NATO déli szárnyának válsága miatt a Szövetségnek és az Egyesült Államoknak fontos volt, hogy Olaszország stabil bázis maradjon, ami már csak az amerikai támaszpontok és a 6. flotta szempontjából is meghatározó lehetett. Mivel az olasz kormány azon az állásponton volt, hogy a NATO-nak ütőképesnek kell lennie egy váratlan agresszió esetén, és Róma a „védelem és enyhülés” kettős elgondolás pártján állt, ezért az ország légierője amerikai gépek vásárlásába kezdett, illetve érdekelt volt a Szövetségen belüli fegyverkereskedelemben. A korszakban Olaszország hadi költségvetése nem csökkent, és bár súlyos gazdasági és pénzügyi válsággal küzdött, a haderőfejlesztésre mégis kiemelt figyelmet fordított. A NATO terveinek megfelelően Róma belekezdett a fegyveres erők átszervezésébe, és haditengerészetének, illetve légierőjének korszerűsítése után napirenden volt a szárazföldi erők modernizálása is. Ezek a lépések bizonyítják, hogy a belpolitikai problémáktól függetlenül az olasz kormány a katonapolitikájában igyekezett a brüsszeli döntéseket a gyakorlatban megvalósítani.

A NATO déli szárnyának gyengülése miatt a Szövetség rendszeresen tartott hadgyakorlatokat a tengeren és Észak-Kelet-Olaszországban, amikkel bizonyítani szeretne volna, hogy a NATO és az amerikai haderők gyorsan bevetethetők, míg az NSZK egy római összefogás során megígérte, hogy katonai, technikai és pénzügyi segítséget nyújt Olaszországnak, és megerősíti szardíniai jelenlétét.¹⁸ A NATO és Olaszország közötti kapcsolatok megerősítése érdekében az egyik 1976-os tanácskozáson a Szövetség Olaszország megmentését hangsúlyozta, Lattanzio olasz hadügyminiszter pedig szorosabb katonai együttműködést és hadseregfejlesztést ígért. Ennek értelmében az olasz parlamentben döntés született német–angol–olasz kooperációban Tornado repülőgépek gyártásáról, míg a katonai költségvetést 1977-re 3560 milliárd lírára emelték, ami 1976-hoz képest 20%-os növekedést jelentett. Eközben a parlament előtt volt egy tervezet, ami a NATO terveivel összefüggésben a haditengerészet után a légierő és a szárazföldi csapatok korszerű átfegyverzését tartalmazta. Bár a számok és ígérek szépen néznek ki, de a római magyar nagykövetség jelentése szerint a 20%-os költségvetés-emelés megegyezik az ország inflációs rátájával, és az olasz kormány a NATO tudomására hozta, hogy a fennálló gazdasági helyzetben Olaszország nem tudja vállalni a megemelt kiadásokat.¹⁹

Olasz fejlesztések német és amerikai segítséggel

Az olasz gazdasági problémák miatt a magyar hírszerzéshez eljutott információk szerint az NSZK az 1975 januári brüsszeli NATO-ülésemelől kötött megállapodás értelmében nem hivatalos formában 1000 milliárd dolláros hitelt nyújtott Olaszországnak az olasz tengeri erők megújítására és megerősítésére. A megállapodás bizonyítja az erősödő olasz–német kapcsolatokat, amelyet kihasználva az NSZK támaszpontokat létesített Szardíniában, bázist tervezett létesíteni Puglia déli részén, és tervbe vette tengeri egységei egy részének áthelyezését La Speziába és Tarantóba.²⁰ Nem sokkal később a római német nagykövetség tartott értekezleten olasz és német katonai szakértők

¹⁸ ÁBTL 3.2.3 Mt 867/13. 151-155. o. Információs jelentés, Budapest, 1976. április 26.

¹⁹ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1976/108. Jelentés, Róma, 1976. december 17. 1-3. o.

²⁰ ÁBTL 3.2.3 Mt 867/12. 273-277. o. Információs jelentés, Budapest, 1975. március 25.

megállapodtak a NATO déli szárnyának megerősítésében. Ennek értelmében Olaszország azzal a kéréssel fordult a német kormányhoz, hogy nyújtson anyagi juttatásokat az olasz hadiiparnak, amelyet elsősorban elektrotechnikai és hadihajó-fejlesztési beruházásokba fognak fektetni, és az ANTISOM-on keresztül növelje katonai jelenlétét az országban.²¹

A két ország közötti egyre intenzívebb kapcsolatokat alátámasztja Andreotti útja, amelynek során a német kormány ígéretet tett arra, hogy támogatni fogja az Olaszországnak adandó IMF-kölcsön megszavazását, és rendszeresek lesznek a csúcstalálkozók a német és az olasz politikusok között, illetve az EGK-n belül is hatékonyabban fognak a jövőben együttműködni. Ez a siker elsősorban Andreottinak köszönhető, akiről Schmidt azt mondta, hogy „ez az első olyan olasz, aki európai és akivel konkrétan lehet tárgyalni”.²² A találkozó során tett német ígéretek meglepőnek tűnhetnek annak fényében, hogy nem sokkal korábban az NSZK megvétózta az Olaszországnak adandó 500 millió dolláros EGK-kölcsönt, Schmidt pedig fenyegetően kijelentette, hogy „amennyiben az Olasz Kommunista Párt kormányra fog lépni, Olaszország semmilyen gazdasági segítséget sem kap a fejlett tőkés országoktól”.²³ A német kancellár kijelentése sokat elárul arról, hogy Nyugaton valójában hogyan tekintettek Olaszországra. A NATO-nak szüksége volt egy erős szövetségesre a Földközi-tengeren, amelynek mind gazdasági, mind katonai ereje megvan ahhoz, hogy hatékonyan tudjon segíteni egy szovjet előrenyomulás esetén, ezért hajlandóak voltak gazdasági és pénzügyi támogatást adni Rómának. A kölcsönöket azonban feltételekhez kötötték. Az egyik feltétel gazdasági, vagyis az olasz kormány saját gazdaságának fejlesztésére költi a pénzt, és záros határidőn belül elkezd törleszteni, a másik pedig politikai, mégpedig a PCI távoltartása a hatalomtól.²⁴ Ezek a feltételek bizonyítják, hogy a NATO-nak, és azon belül is elsősorban az NSZK-nak és az Egyesült Államoknak céljai voltak Olaszországgal. Ez a cél pedig nem más, mint a Földközi-tenger biztosítása a Varsói Szerződés előretörésével szemben.

Olaszország ezt a szerepet külső segítség nélkül nem tudta volna betölteni, ezért az olasz vezető politikusok rendszeresen tárgyaltak vagy német, vagy amerikai vezetőkkel. Andreotti nem csak Schmidtet kereste fel, hanem az Egyesült Államokba is elutazott, és igyekezett megértetni az ottani politikusokkal, hogy Olaszországnak szüksége van az amerikai segítségre. Válaszként ígéretet kapott arra, hogy az IMF 530 millió dollár kölcsönt fog folyósítani Rómának, és esetleg Washington is hajlandó újabb kölcsönt adni.²⁵ A német és amerikai vezetés viszont kilátásba helyezte, hogy amennyiben az olasz kormánynak nem sikerül úrrá lennie a zavargásokon, a NATO

²¹ ÁBTL 3.2.3 Mt 867/13. 20. o. Információs jelentés, Budapest, 1975. május 27.

²² MNL OL XIX-J-1-j Olaszország KÜM TÜK 1977/103. Jelentés, Róma, 1977. január 27. p. 1.

²³ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1977/103. Jelentés, Róma, 1977. január 27. 1-4. o.

²⁴ Az Olasz Kommunista Párt (Partito Comunista Italiano-PCI) az 1960-as és 1970-es években folyamatosan erősödött (1968-ban a PCI a szavazatok 26,9%-át kapta, 1972-ben már 28,3, az 1975-ös tartományi választáson pedig már 33,4% eredménnyel zárt).

Lásd: MAMMARELLA, Giuseppe – CACACE, Paolo: *La politica estera dell'Italia. Dallo stato unitario ai gorni nostri*. Editori Laterza, Róma, 2010. 390. o.

²⁵ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1976/108. Jelentés, Róma, 1976. december 17. 1. o.

be fog avatkozni a rend helyreállítása érdekében.²⁶ A feltétel érthető volt, hiszen 1974-ben folytatódott Olaszországban a baloldali és jobboldali terrorakciók. 1974. április 18-án a Brigate Rosse tagjai elrabolták Mario Sassi genovai bírót, akit csak hosszas tárgyalások és engedmények után voltak hajlandók elengedni. Alig egy hónappal később az Ordine Nero nevű szélsőjobboldali szervezet Bresciában, a Piazza della Loggia közelében robbantásos merényletet hajtott végre, amelynek következtében hatan életüket veszítették, több mint kilencvenen pedig megsebesültek.

A szélsőjobboldal pár hónappal később újabb akciót követett el. Augusztus 4-én a Firenze-Bologna vonalon közlekedő Italicus vonaton robbantottak. Ebben a merényletben 16-an haltak meg.²⁷ A zavargások, illetve az olasz baloldal előretörése miatt a német kancellár kilátásba helyezte, hogy amennyiben Olaszország NATO-tagsága veszélybe kerülne, abban az esetben a Szövetség katonai beavatkozást hajt végre az atlanti csapatok segítségével, és az Egyesült Államokkal közösen kijelentették, hogy a jövőben csak a Kereszténydemokrata Pártból (Democrazia Cristiana-DC), vagy esetleg a DC-ből, a PSDI-ből, és a PLI-ből álló kormányt fogadják el, amelyet kívülről az MSI²⁸ támogathat. Az említett pártokból kiderül, hogy Nyugaton nem csak a PCI-től tartottak, de nem lelkesedtek a PSI hatalomra kerüléséért sem.

Olasz–amerikai kapcsolatok

Az olasz–amerikai kapcsolatokat több dolog is beárnyékolta. Egyrészt Moro ígérete és az Egyesült Államok sürgetése ellenére Olaszország nem volt hajlandó ratifikálni az atomsorompó-szerződést,²⁹ amelynek célja a nukleáris fegyverrel rendelkező országok lehetséges megsokszorozódásának megakadályozása volt.³⁰ Ennek háttérében minden bizonnyal az állt, hogy Olaszország képes volt atomfegyvert gyártani, és nem akart lemondani erről az erőről. Másrészt Róma szeretett volna részt venni egy alternatív egyesült Európa létrehozásában, ami szembement volna Washington

²⁶ ÁBTL 3.2.3 Mt 867/12. 235. o. Információs jelentés, Budapest, 1974. december 16.

²⁷ MAMMARELLA, Giuseppe: *L'Italia contemporanea (1943-2011)*. Società editrice il Mulino, Bologna, 2012. 372. o.

²⁸ Az MSI (Movimento Sociale Italiano-Olasz Szociális Mozgalom) egy újfasiszta párt volt a második világháború utáni Olaszországban. Az MSI-ről magyar nyelven lásd: CHIARINI, Roberto: A Movimento Sociale Italiano-történeti áttekintés. In: FEITL István (szerk.): *Jobboldali radikalizmusok tegnap és ma*. Napvilág Kiadó, Budapest, 1998. 89-113. o.

²⁹ Az atomsorompó-szerződést (Treaty on the Non-Proliferation of Nuclear Weapons-NNPT) 1968 júliusában írták alá, és 1970-ben lépett hatályba. A szerződés 3 pilléren nyugodott: a katonai célra használható nukleáris technológiák terjedésének megakadályozása, a nemzetközi felügyelet melletti leszerelés és az atomenergia békés célú felhasználása. Lásd: HORVÁTH – PARAGI – CSICSMANN 2013, 188.

³⁰ SILVESTRI, Stefano: Il dibattito sulla non-proliferazione nucleare. In: MERLINI, Cesare (szerk.): *La politica estera dell'Italia. Cinquant'anni dell'Istituto Affari Internazionali*. Società editrice il Mulino, Bologna, 2016. 72. o.

hegemóniájával.³¹ Ezek az események hozzájárulhattak ahhoz, hogy az amerikai vezetés a római nagykövetségén megfigyelő és elemző speciális csoport megerősítésén gondolkodott. Ennek feladata a magyar hírszerzés szerint az olasz helyzet felmérése, értékelése volt, és javaslatot tehetett esetleges beavatkozásra, amennyiben ennek szükségét látta. A beavatkozás főleg pártfinanszírozásban, gazdasági és politikai nyomásyakorlásban mutatkozott volna meg, melyhez az amerikai kormánynak hozzá kellett járulnia, majd a NATO-nak beleegyeznie az akció végrehajtásához. „Von Schiller” megerősítette azt az információt, miszerint Washington anyagi juttatásokban részesíti a DC-t, a PSDI-t, a PLI-t, és parlamenten kívüli baloldali pártokat annak érdekében, hogy mind a PCI-t, mind a PSI-t sikerüljön minél jobban meggyengíteni és távol tartani a kormánytól.³²

Mivel 1976-ban választásokat rendeztek Olaszországban, az azt megelőző voksolások alkalmával pedig a PCI egyre több szavazatot szerzett, ezért a kommunista párt kormányba kerülésétől való félelem további lépésekre ösztönözte mind a NATO-t, mind az olasz kereszténydemokrata politikusokat. A szövetségi rendszer kilátásba helyezte, hogy amennyiben a PCI bekerülne a kormányba, abban az esetben a Védelmi Kollégiumot elköltöztetnék az országból, a kényes objektumokat, mint például a Civitavecchiában található partizánharc-ellenes kiképző iskolát bezárnák.³³ Mindemellett a római magyar nagykövetség úgy értesült, hogy az Egyesült Államok és a NATO gazdasági, pénzügyi, katonai, és katonapolitikai szankciókat vezetne be az ország ellen, és Rómát kizárnák a NATO-titkokból.³⁴ A PCI-től való félelem miatt Forlani 1976-ban el is utazott Franciaországba, az NSZK-ba és az Egyesült Államokba, hogy anyagi és pénzügyi támogatást kérjen, Kennedy szenátor pedig Carter elnök beleegyezésével Rómában járt nem hivatalos úton, de találkozott az állami, és a gazdasági élet legmagasabb képviselőivel.³⁵ Ezek az események alátámasztják a római magyar nagykövetség értesüléseit, miszerint a júniusi választásoknak elsősorban külpolitikai jelentőségük van, ugyanis amennyiben a PCI kormányra kerülne, ez reakciókat váltana ki a nyugati szövetségesek részéről, és ha a NATO nyílt katonai beavatkozása nem is valószínű, de az országot kizárnák a szövetség titkaiból, a Közös Piac pedig gazdasági szankciókat léptetne életbe.³⁶

Az olaszországi félelmek hozzájárulhattak ahhoz, hogy „Von Schiller” szerint a NATO 1975 decemberi brüsszeli ülésén az Eurogroup az együttműködés fokozásáról döntött. A döntés értelmében a NATO-n belül nyílt és burkolt akciókat hajtanak majd végre, ha a helyzet úgy kívánja. Nyílt akciók közé tartozik például a törvények bevezetése a felforgató mozgalmakkal szemben, illetve az instabil országok politikai fejlődésének ellenőrzés alatt tartása, akár katonai intervenció végrehajtásával is. A burkolt akciók

³¹ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1975/108. Jelentés, Róma, 1975. január 27. 1-7. o.

³² ÁBTL 3.2.3 Mt 867/13. 30-32. o. Információs jelentés, Budapest, 1975. május 30.

³³ ÁBTL 3.2.3 Mt 867/13. 131. o. Információs jelentés, Budapest, 1976. április 27.

³⁴ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1976/107. Feljegyzés, Róma, 1976. május 12. 1. o.

³⁵ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1976/107. Jelentés, Róma, 1976. november 17. 1-2. o.

³⁶ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1976/107. Feljegyzés, Róma, 1976. június 14. 1. o.

közé sorolták a lélektani hadviselést, az információs szolgálatok újjászervezését és megbízható elemek beszivároztatását az ellenzéki mozgalmakba.³⁷

Az olasz belpolitikai, gazdasági és társadalmi problémák ellenére Garzó Ferenc,³⁸ a római nagykövetség tanácsosa elvetette egy lehetséges államcsíny végrehajtását Olaszországban, hiszen szerinte az ország nem kormányozhatatlan, illetve egy ilyen akciót még az MSI sem támogatna. Jelentésében kitért arra, hogy a „feszültség stratégiája”³⁹ folyamatosan táplálja a félelem és a bizonytalanság érzését, de senki sem támogatna egy chilei jellegű megoldást.⁴⁰ Az államcsíny lehetőségét Garzó azért is vetette el, mert szerinte Olaszországban akkor nem volt olyan erős és tekintélyes politikai vagy katonai személyiség, aki mögé felsorakoztak volna a fegyveres erők. A jelentés számunkra abból a szempontból is érdekes, mert ebben Garzó ismerteti az olasz fegyveres erők létszámát. Ezek szerint az olasz hadsereg kb. 350 ezer főből áll, akiknek a nagy része, 50-60 százaléka fiatal, ezért a PSI-t vagy a PCI-t támogatják, míg a felső katonai vezetés öreg konzervatívokból áll, akik feltétlenül hűségesek a NATO-hoz. Az olasz rendőrség (PS-Pubblica Sicurezza) 35 ezer főből áll, de a rendőrség főleg közigazgatási feladatokat lát el, így egy államcsínyben nem lehetne őket felhasználni. Ez alól egyedül a Celere⁴¹ osztag jelentene kivételt, amelyik egy félkatonai jellegű részleg az ország nagyvárosaiban, például Rómában, Padovában, Milánóban vagy Nápolyban elhelyezve, de mindössze 2600 főt számlál. A Celere katonai jellegét egy korábbi hírszerzési anyag megerősíti, amely szerint az egységet

³⁷ ÁBTL 3.2.3 Mt 867/13. 121. o. Információs jelentés, Budapest, 1976. április 26.

³⁸ „Fekete” fedőnéven a Belügyminisztérium III/I-3-D alosztályánál a római rezidentúra operatív tisztjének feladatkörét is betöltötte. Lásd: BOTTONI, Stefano: „Mozart” és „Fekete”. Egy hírszerzési dosszié különös története I. rész. *Betekintő*, 2014/4. 1. o.

³⁹ A „feszültség stratégiája” 1969. december 12-én egy milánói bombamerénnyel vette kezdetét. Célja Olaszország, illetve az olasz politikai intézmények destabilizálása volt. Az időszakban spontán, vagy az olasz titkosszolgálatok által befolyásoltan szélsőséges csoportok rendszeresen hajtottak végre terrorakciókat. A „feszültség stratégiája” nagymértékben hozzájárult ahhoz, hogy az 1970-es és 1980-as években a DC-kormányok fenn tudjanak maradni. Lásd: TRANFAGLIA, Nicola: *Anatomia dell'Italia repubblicana 1943-2009*. Passigli Editori, Firenze, 2010. 110-115. o.

⁴⁰ Chilében az 1960-as évek második felében széles balközép jellegű politikai szövetség jött létre. Ennek következtében 1969-ben a Népi Egység nevű hatpárti koalíció aratott győzelmet, és 1970-ben Salvador Allendét nevezték ki köztársasági elnöknek. A rendszert azonban mind szélsőbal, mind szélsőjobboldalról támadták, míg végül 1973-ban a kereszténydemokraták vezetésével a rézbányászok sztrájkba kezdtek. Szeptemberben végül egy amerikai részvétellel végrehajtott katonai puccs során meggyilkolták Allendét. A puccsban jelentős szerepet játszottak az amerikai támaszpontokon kiképzett elitegységek, vagyis a „zöldsapkások”. Allende meggyilkolása után Pinochet kezébe került a hatalom, aki durva diktatúrát vezetett be az országban. Lásd: ANDERLE Ádám: *Latin-Amerika története*. Pannonica Kiadó, 1998. 161. o.

⁴¹ A Celere, vagy hivatalos nevén a Reparto Mobile az olasz rendőrség egy különleges egysége, amelynek elsődleges feladata a sporteseményeken, utcai tömegrendezvényeken az állampolgárok védelme és a közbiztonság garantálása, de rendszeresen bevetik az alakulatot különböző vészhelyzetekben is. Az összesen 15 nagyvárosban működő alakulat tagjainak szigorú fizikai és pszichológiai alkalmassági vizsgán kell megfelelniük. Lásd: Sz.n.: *Reparti mobili*. Polizia di Stato – olasz nemzeti rendőrség hivatalos honlapja, é.n.

tankokkal, ágyúkkal és golyószórókkal szerelték fel, sőt, még ejtőernyős osztaga is van, amire egy rendőrségnek aligha lehet szüksége.⁴² Ezek mellett még létezik a kb 80 ezer fős, 4 ezer kiegészítővel és 1500 tiszttel kiegészített Arma dei carabinieri, amely különálló fegyvernemként tulajdonképpen egy szakképzett hadsereg.⁴³ Ők elsősorban a polgárok politikai ellenőrzésében, nyilvántartásában tevékenykednek, de ellátják a parlament, a köztársasági elnök, a Legfelsőbb Bíróság, illetve a miniszterek védelmét is.⁴⁴

A rakétatelepítés kezdetei

Miután az államcsíny elmaradt, és az olasz belpolitikai helyzet is stabilizálódott, 1977-ben a NATO úgy döntött, hogy nagy hatótávolságú rakétákat telepít Közép- és Dél-Európába, köztük Olaszországba. A rakéták három különböző típusúak lennének, földről, levegőből és tengerről kilőhetők, és 1980-tól ezek alkotnák a Földközi-tengeren a katonai helyzet gerincét. A magyar hírszerzés információi szerint ezeket a rakétákat, vagy legalább egy részüket neutronfejjel szerelnék fel.⁴⁵ Az esetleges neutronfejjel felszerelt rakéták és a neutronbomba azonban vitákat váltott ki az olasz politikai pártok körében, hiszen a Vatikánon kívül a baloldal is hevesen ellenezte ezek elhelyezését az országban, míg a kormány rendkívül óvatos nyilatkozatokat tett csak közzé. A NPG október 11-12-i ülésén például Ruffini hadügyminiszter annyit jelentett ki, hogy a neutronbombára Olaszország nem mond igent, se nemet.⁴⁶ A magyar hírszerzés információja összhangban állhat az 1977 márciusi londoni értekezlet óta napirenden lévő NATO hosszú távú védelmi programmal (LTDP), melyet Carter amerikai elnök javasolt. Ennek értelmében Európában végrehajtanák a nukleáris erők modernizációját, és célként tűzték ki egy, a NATO autoritásának alárendelt nemzeti erőkből álló egység felállítását, amely javítaná a szövetség képességeit és reakcióidejét. Ezt az utolsó javaslatot egyébként az olasz képviselők ellenezték, mert bár szerintük az egység felállítása valóban hatékonyabbá tehetné a NATO-t, de az elképzelés megvalósíthatatlan, így inkább csak meghívásként értelmezendő.⁴⁷

⁴² NEUSPILLER Ferenc: A római rezidentúra malacperselye. Miért támogatót a magyar hírszerzés egy olasz disznóhizlaldát? *Betekintő*, 2019/1. 29. o.

⁴³ Az Arma dei carabinieri a hadsereg részét képezi és a védelmi miniszterhez tartozik, ezért független bármely egyéb helyi rendőri szervtől, csak saját parancsnokságának köteles engedelmessé válni. Hivatalnokai ugyanazokkal a jogkörökkel és kiváltságokkal rendelkeznek, mint a PS hivatalnokai, ha azonban a carabinieri hivatalnokai közreműködik egy ügyben a PS hivatalnokaival, akkor előbbi átveszi a szolgálat irányítását. Az Arma dei carabinieri kiváltsága megmutatkozik abban is, hogy a rendőri szervek csak írásban és kérelem formájában fordulhatnak segítségért a carabinierihez. Lásd: SOARDI, Mario: *Manuale di polizia municipale*. Casa Editrice F. Apollonio&C, Brescia, 1962. 4-5. o.

⁴⁴ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1976/108. Jelentés, Róma, 1976. május 28. 1-5. o.

⁴⁵ ÁBTL 3.2.3 Mt 867/14. 8. o. Információs jelentés, Budapest, 1977. november 1.

⁴⁶ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1977/103. Jelentés, Róma, 1977. november 25. 1-2. o.

⁴⁷ Archivio Storico Istituto Luigi Sturzo Archivio Giulio Andreotti (ASILS AGA) NATO series Memorandum by Minister of Defense Attilio Ruffini for the Prime Minister Andreotti, 'Washington Summit -NATO's program for long-term defense (LTDP)' 1978. május. 30. 1-4. o.

Korábbi értesüléseikkel összhangban 1978-ban a magyar hírszerzést arról tájékoztatta „Von Schiller”, hogy a NATO-ban szó van cirkálórakéták olaszországi elhelyezéséről. Ezeket egy új kikötőbe telepítenék Camp Darbyn belül, és részét képeznék egy hadtáprendszernek, melyet cirkálórakéták és új nukleáris fegyverek számára hoznak létre. Az információ szerint a Camp Darbyt övező fenyevesekben a kilövőállomások építése a befejezéséhez közeledik, az új kikötő célja pedig egy amerikai ellenőrzés alatt álló nagyszabású támaszpont felépítése, amely hadtápbázisként szolgálhat a NATO déli szárnyának. „Von Schiller” szerint a rakétákon kívül a NATO egy mozgékony ütőerőt is igyekszik létrehozni, amely angol, amerikai és olasz egységekből állna, és légi, tengeri, illetve szárazföldi alakulatokat foglalna magába. Az ütőerő felállítása elvileg 1980-ra elkészül, ezzel pedig a NATO célja a Földközi-tengertől keletre és délre való terjeszkedés. Az ütőerő utánpótlásának biztosítása miatt azonban szükség van az AFSOUTH-ra, és az AWACS-rendszerre. Ez utóbbi az értesülés alapján 1979-ben már életbe lép, bázisa pedig Olaszországban lesz, a kormány javaslata alapján vagy Szardínián, vagy Szicílián.⁴⁸

1978 decemberében a NATO védelmi minisztereinek őszi szekciójának ülésén a jelen lévők aggodalmuknak adtak hangot a Varsói Szerződés hagyományos erőinek erősödése miatt. A jelen lévő miniszterek megegyeztek abban, hogy nem törekednek sem emberben, sem eszközökben szimmetriát kialakítani a Varsói Szerződéssel szemben, de a hadi kiadásokat minden tagállamban növelni kell évente 3%-kal. Ruffini szerint Olaszország képes vállalni ezt a növelést, de ez a maximum, mert a parlament és a közvélemény nehezen fogadja el a hadi kiadások növelését. Ennek érdekében egyértelműsíteni kell a Varsói Szerződés irányából érkező fenyegetést, hatékonyabb információs politikát kell folytatni, és ki kell hangsúlyozni, hogy a cél az egyensúly megteremtése a lehető legalacsonyabb szinten.⁴⁹ Ezzel egy időben Forlani kijelentette, hogy a török gazdasági problémák és a Varsói Szerződés erősödése miatt a Mediterráneumban fennáll a destabilizáció veszélye, ezért hatékonyabb együttműködést kell kialakítani a fegyvergyártásban. Ennek kapcsán Olaszország olyan javaslattal állt elő, ami szerint nem csak a katonai szükségletek kielégítésében, hanem ipari és technológiai téren is szorosabb kapcsolatokra lenne szükség a szövetségben belül.⁵⁰

A kedvezőtlenül alakuló nemzetközi helyzet miatt 1979-ben a NATO döntést hozott támadó és védelmi kapacitásának fokozásáról. Ennek értelmében az 1980-as évekre fegyverek új generációját igyekezett hadba állítani, mint például a Remotely Piloted Vehicles, amelyet Dél-Kelet-Európában és a Földközi-tenger medencéjében terveztek elhelyezni. Ez a lépés összhangban állt egy 1978-as olasz–amerikai egyezményvel, amely szorosabb közös szervezési munkálatokat irányzott elő a fegyverzet

⁴⁸ ÁBTL 3.2.3 Mt 867/14. 151-159. o. Információs jelentés, Budapest, 1978. június 28.

⁴⁹ ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'The autumn sessions of NATO Ministers of Defense meetings (Eurogroup: 4th December; DPC 5th-6th December 1978)', 1978. december 14. 1-3. o.

⁵⁰ ASILS AGA NATO series Memorandum by Ministry for Foreign Affairs, 'The 1978 Ministerial Atlantic Council', 1978. december 18. 1-4. o.

kialakításában. A Földközi-tenger térségében fellelhető problémák miatt 1978-ban a NATO két hadgyakorlatot tartott a zónában, amelyekkel felkészültségét és katonai erejét igyekezett bizonygatni.⁵¹ Mindeközben az NSZK-ban, Nagy-Britanniában és Olaszországban döntés született Pershing II cirkálórakéták és egyéb rakétarendszerek létrehozásáról, amely a résztvevő országok szerint közbeeső megoldás lehet egy önálló európai nukleáris erő irányába. Nyugat-Európa ugyanis az 1970-es évek végéhez közeledve olyan európai védelmi rendszer kialakítására törekedett, ami nem kötődik a kontinensen kívüli szövetségesekhez. Ebben pedig a WEU-nak⁵² nagy szerepet szántak. A rakétatelepítésről szóló döntés azonban – még úgy is, hogy a Pershing II csak 1983-tól lenne működésképes – nem váltott ki túl nagy lelkesedést Olaszországban, amelyet szorosabb kapcsolatok fűztek az Egyesült Államokhoz, mint a többi európai szövetségesét.⁵³ Néhány hónappal később a magyar hírszerzés úgy értesült, hogy 1979 decemberében a NATO-n belül döntés fog születni a Pershing II Nyugat-Európába történő telepítéséről, amelyet két lépcsőben terveztek végrehajtani: először szakértők egyeztetnek arról, hogy mikor és milyen formában lehet telepíteni, majd a tagállamok külügyminiszterei megegyeznének abban, hogy melyik országba hány rakétát telepítenének. „Von Schiller” információi alapján Andreotti már bele is egyezett a telepítésbe, amelyre három helyszínt jelöltek ki: Calabria, az Appenninek északi része és Szardínia. Ezekon kívül azonban további rakéták telepítése várható Camp Darby-be, illetve dél-olasz kikötőbe.⁵⁴

1979. november 15-17-én Velencében értekezletet tartottak a NATO megalakításának 30. évfordulója alkalmából. Itt kinyilvánították, hogy a szövetség ereje szabad népek konszenzusán alapul, az idők során a katonai szövetségből komplex biztonsági szervezet lett, és létjogosultsága megkérdőjelezhetetlen, hiszen visszatartja a szovjet katonai potenciált, amivel fenntartja az európai békét. Az értekezleten azonban vita alakult ki a NATO céljairól, fejlődéséről, és leginkább Európa és az Egyesült Államok biztonságáról a Nyugat–Kelet stratégiai egyensúly tükrében. A jelenlévők megállapodtak abban, hogy a katonai biztonság többé már nem választható el a politikai biztonságtól, illetve, hogy a szövetség legsürgősebb kérdése a NATO-ra nehezedő fenyegetés, amelyet a stratégiai egyensúly eróziója okoz a szovjet fegyverkezés miatt, hiszen az SS20-asok kihívást jelentenek a NATO-nak, és azon belül elsősorban Nyugat-Európának.

⁵¹ ÁBTL 3.2.3 Mt 867/14. 208. o. Információs jelentés, Budapest, 1979. május 28.

⁵² A Nyugat-Európai Uniót (Western European Union-WEU) 1954. október 23-án Párizsban Nagy-Britannia, az NSZK, Hollandia, Belgium, Luxemburg, Franciaország és Olaszország képviselői hozták létre. A szervezet katonailag ugyan a NATO alá volt rendelve, az első 20 évében mégis aktív szerepet játszott Európa történelmében. Már csak azért is, mert ez volt az egyetlen olyan európai fórum, amelyen a „hatok” és Nagy-Britannia találkozhattak egymással. Lásd: LÁNG Péter: Egy szervezet négy évtizede. A WEU rövid története (1954-1993). In: DUNAY Pál – GAZDAG Ferenc (szerk.): *Nyugat-Európai Unió. A megalakulástól a megvalósulásig*. SVKI, Budapest, 1994. 63-66. o.

⁵³ ÁBTL 3.2.3 Mt 867/14. 246-247. o. Információs jelentés, Budapest, 1979. augusztus 29.

⁵⁴ ÁBTL 3.2.3 Mt 867/14. 254. o. Információs jelentés, Budapest, 1979. október 24.

A NATO 1979. decemberi csúcstalálkozásán döntés született a nukleáris újrafegyverkezésről. Ennek értelmében a következő években Nyugat-Európában minimum 572 Pershing II-t vagy Tomahawkot fognak elhelyezni. A kilövőbázisokon amerikai személyzet szolgál majd. Olaszország vállalta 132 cirkálórakéta és 28 Pershing II telepítését, előbbieket valószínűleg Szardíniára, utóbbiakat pedig az ország északi részén. A jelenlévők kinyilvánították, hogy reményeik szerint a rakétakilövések telepítése 1980 után megkezdődik. Ráadásul az európai tagok a csúcstalálkozáson nem ragaszkodtak a kettős kulcs ellenőrzési rendszeréhez, vagyis nem kell majd a helyi kormány beleegyezése a rakéták kilövéséhez. A találkozó döntés született továbbá egy multinacionális tengeri és légiereő létrehozásáról, amelyhez ausztrál, japán és kínai egységek is csatlakoznának.⁵⁵

Ezzel nagyjából egy időben, 1979. december 18-19-én Nápolyban az Egyesült Államok, Nagy-Britannia, az NSZK és Olaszország képviselői is tanácskozást tartottak az AFSOUTH terveinek megvalósításáról. Ennek értelmében a NATO déli szárnyán agresszívebb külpolitikába kezdenek, amely magába foglalja a gazdasági nyomásgyakorlást és a stratégiai intézkedések bevezetését. A tervek szerint 1982-re sikerül végrehajtani a terveket, aminek következtében a NATO szerepét kiterjesztik a Közel-Keleten túlra és Afrikába, szorosabb együttműködést alakítanak ki az Egyesült Államokkal a perzsa-öbölbeli ellenőrzés visszaszerzése érdekében, a stratégiai ellenőrzést kiterjesztik a „szürke zónákra”, vagyis a Perzsa-öböllel határos országokra, támaszpontokat létesítenek Kelet-Afrikában és Szaud-Arábiában, illetve titkos ellenintézkedéseket foganatosítanak Közép-Európában a Közös Piac segítségével.⁵⁶

A NATO 1979. december 10. és 14. közötti brüsszeli tanácskozása értelmében a nyugati szövetség új típusú középhatótávú nukleáris rakéták gyártásába és rendszerbe állításába kezdett, amelyhez természetesen Olaszország is csatlakozott.⁵⁷

Az eurorakéták komoly vitát eredményeztek a NATO-n belül. Belgium és Hollandia például elutasította a rakétatelepítést, míg Olaszország támogatta, és egy Spadolini által aláírt titkos szerződés értelmében át is engedték a comisói repülőteret a telepítésre, az olasz képviselőház pedig 1983 novemberében meg is szavazta 16 darab cirkálórakéta telepítését az országba. Ez a rakétatelepítési terv a szovjet nukleáris fegyverzet modernizálási programjára, valamint az emiatt veszélybe került európai katonai egyensúlyra adott válasz volt, és jelezték az atlanti újrafegyverkezés első momentumát, melyet az amerikai elnökök, Nixon és Reagan szorgalmaztak. 1980-tól kezdve az Egyesült Államok a békeidőben bekövetkező valaha volt legnagyobb katonai növekedését produkálta. Míg 1980-ban Washington 134 milliárd dollárt költött védelmi kiadásokra, addig 1985-ben már ennek majdnem dupláját, 252 milliárd dollárt fektettek a célba. Ezzel az 1980-as évek közepén az amerikai katonai kiadások

⁵⁵ ÁBTL 3.2.3 Mt 867/14. 268-270. o. Információs jelentés, Budapest, 1979. december 27.

⁵⁶ ÁBTL 3.2.3 Mt 867/14. 287. o. Információs jelentés, Budapest, 1980. február 11.

⁵⁷ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1980/110. Jelentés, Róma, 1980. február 18. 7. o.

meghaladták mind a második világháború utolsó évének, mind a koreai háború utolsó évének a kiadásait.⁵⁸

Nem sokkal később a magyar hírszerzést arról tájékoztatták, hogy Olaszországban katonai szolgálatra hívták be azokat, akiket az azt megelőző tíz évben a Civitavecchiában lévő gerillaellenes kiképzőközpontban képeztek ki. Ennek oka a jelentés szerint az volt, hogy katonai egységeket képezzenek ki gerillaellenes hadviselésre, utcai harcokra, illetve baloldali elemek és pártvezetők elleni akciókra, és megalakítsanak egy olyan gerilla-hadviselésre alkalmas fegyveres erőt, amit képesek lehetnek hatékony felhasználni a Varsói Szerződés tagállamai ellen. A jelentés ezen kívül kitért arra, hogy Cossiga miniszterelnök és Colombo külügyminiszter 1980-ban az Egyesült Államokba látogatott. Az út során megállapodtak az amerikai katonai jelenlét megerősítésében, a NATO-n kívüli amerikai egységek olaszországi támaszpontokon való elhelyezéséről, illetve az olasz vezetők kinyilvánították támogatásukat az amerikai diplomáciai akciók felé, és hangsúlyozták, hogy egyetértenek az Egyesült Államok afganisztáni és iráni külpolitikájával.⁵⁹

A vezető szerep megőrzése

Az olasz miniszterelnök és a külügyminiszter amerikai útja is bizonyítja, hogy Olaszország majdnem mindenben támogatta az amerikai politikát, és különösen Carter elnök lépéseit. Így volt ez az amerikai nukleáris erők felülvizsgálatának tervével, új nukleáris opciók kialakításával, amelyről az NPG ülésén döntöttek, illetve Olaszország nagyobb részvételével az első csapásban, a kétlépcsős nukleáris hadviselésben, illetve a biológiai és vegyi hadviselés előkészítésében. Ez utóbbi érdekében a NATO vegyi anyagok felhalmozásába kezdett Camp Darbyn és Avianóban, illetve biológiai fegyverraktár létesítésébe kezdett Szardínián.⁶⁰

Az olasz kormánynek az imént említett lépései és az amerikai politika ilyen mértékű támogatása egyértelmű törekvés volt arra, hogy Olaszország megőrizze kiemelkedő szerepét a Földközi-tenger térségében, és valóban a NATO „fellegvárává” nője ki magát. Ezen cél elérése érdekében pedig Róma aktív külpolitikát folytatott a Mediterráneum országaival. 1980. szeptember 15-én megkötötték az olasz–máltai garanciaegyezményt, amely biztosította Málta semlegességét, és Olaszország ígéretet tett arra, hogy amennyiben szükség lenne rá, akár katonai eszközökkel is támogatja Málta függetlenségét.⁶¹ Ennek ellenére Dom Mintoff máltai miniszterelnök tárgyalásokat folytatott Líbiával és a Szovjetunióval, amiknek eredményeképpen szovjet hadihajókat engedett be Valletta kikötőjébe, míg Líbia helikopterbázist

⁵⁸ MINOLFI, Salvatore: Italia, Europa e Stati Uniti: La NATO dal 1969 al 1989. In MINOLFI, Salvatore (szerk): *L'Italia e la NATO. Una politica estera nelle maglie dell'alleanza*. CUEN, Nápoly, 1993. 120-129. o.

⁵⁹ ÁBTL 3.2.3 Mt 867/14. 310-318. o. Információs jelentés, Budapest, 1980. augusztus 5.

⁶⁰ ÁBTL 3.2.3 Mt 867/14. 349. o. Információs jelentés, Budapest, 1980. október 10.

⁶¹ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1980/110. Jelentés, Róma, 1980. szeptember 18. 1. o.

építhetett a szigeten.⁶² Néhány hónappal ezt követően Colombo Athénba utazott, hogy megpróbálja rávenni Görögországot a NATO-ba való visszatérésre.⁶³ Mindeközben 1979 ősztől rendszeressé váltak az olasz–jugoszláv egyeztetések a NATO keretein belül. A nyugati szövetség abban reménykedett, hogy Belgrádon keresztül sikerül híreket és információkat szereznie Kelet-Európáról, és esetleg katonai felszereléseket tud eladni Jugoszláviának. A délszláv országra a nyugati szövetségi rendszernek azért volt szüksége, hogy a délkeleti szárnyon vissza tudja szerezni egyeduralmát a Földközi-tengeren. Mivel az itteni ütőerő jelentős részét áthelyezték a Perzsa-öbölbe és az Indiai-óceánra, ezért a térségben az egyetlen számottevő tényező továbbra is az amerikai 6. flotta volt. Az amerikai flotta azonban nem lett volna képes megvédeni szövetségeseit, és angol, francia, olasz segítséggel sem tudott volna megállítani, feltartóztatni egy ellenséges támadást.⁶⁴ Mivel a NATO joggal tartott egy szovjet támadás veszélyétől, ezért természetesen az 1970-es és 1980-as években is igyekezett kijátszani a „kínai kártyát”. 1979-ben például Hua Kuo-feng kínai miniszterelnök európai körutazást tett, amelynek során ellátogatott Franciaországba, Nagy-Britanniába, az NSZK-ba és Olaszországba. Bár a körút nem járt nagy sikerrel, hiszen csak általános egyezmények születtek a gazdasági, technikai és kereskedelmi kapcsolatok bővítéséről, a távol-keleti ország kormányfője mégis ígéretet tett arra, hogy megnyitja a kínai kikötőket a multinacionális tengeri erőknek. Ami Olaszországot illeti, egyedül a FIAT tudott értékelhető egyezményt kötni Kínával, amelynek értelmében az olasz gyár engedélyt kapott egy mezőgazdasági gépeket gyártó üzem alapítására az ázsiai országban.⁶⁵

1980-ban a NATO tisztázta, hogy mit is vár el Olaszországtól. Eszerint Rómának elsősorban katonai kötelezettségeit kell teljesítenie, ami magába foglalta azt is, hogy négy olasz haditengerészeti egységet át kellett telepíteni az Indiai-óceánra, és az olasz légierő bázisainak egy részét át kellett engednie használatra a NATO szárazföldi és tengeri erőinek támogatására, amivel megvalósult az Egyesült Államok és Nagy-Britannia légihídja. Ezekon kívül egy esetleges afrikai válság esetén Rómának fontos politikai szerepet szántak, hiszen Olaszország jó kapcsolatokat ápolt Algériával, Líbiával és Szíriával. Mindemellett részt kellett vennie egy, a Földközi-tenger keleti részén kialakításra kerülő hatékonyabb tengeri flotta felállításában, és tengeri összeköttetést kellett biztosítani a NATO tagállamai között. Bár Róma igyekezett betölteni azt a szerepet, amit a NATO és az Egyesült Államok szánt neki, a magyar hírszerzés információi szerint azonban Reagan megválasztása mégis félelemmel töltötte el az olasz vezetést – akárcsak a többi európai szövetséges vezetését –, hogy elveszítheti a NATO-n belüli autonómiáját. Éppen ezért Olaszország az 1980-as években elkezdett két kártyával játszani. Egyrészt igyekezett továbbra is szoros kapcsolatot fenntartani Washingtonnal, másrészt viszont aktív szerepet játszott egy önállóbb Európa létrehozásában. Az új amerikai elnök megválasztása még aktuálisabbá

⁶² ROMANO, Sergio: *Guida alla politica estera italiana. Da Badoglio ai nostri giorni*. BUR Rizzoli, Milánó, 2019. 198-199. o.

⁶³ MNL OL XIX-J-1-j Olaszország KÜM TŰK 1980/110. Jelentés, Róma, 1980. november 21. 1-3. o.

⁶⁴ ÁBTL 3.2.3 Mt 867/14. 292-296. o. Információs jelentés, Budapest, 1980. június 10.

⁶⁵ ÁBTL 3.2.3 Mt 867/14. 274. o. Információs jelentés, Budapest, 1975. december 28.

tette az eurorakéták kérdését. A NATO úgy döntött, hogy amennyiben csúszik a rakéták telepítése, abban az esetben nyomást fognak gyakorolni Görögországra, hogy Athén is engedjen be rakétákat saját területére. Ezen kívül 1981 januárjára várták annak a határozatnak az elfogadását, amely döntött az eurorakéták telepítéséről. Az előzetes várakozások szerint az NSZK, Belgium és Hollandia csak akkor egyezik bele a rakételepítésbe, ha aláírják a SALT II-t,⁶⁶ míg Nagy-Britannia és Olaszország mindenképpen telepít, sőt, még azt is elképzelhetőnek tartották, hogy többet is, mint amennyi eredetileg vállalt.

A Földközi-tenger térségében betöltött vezető szerep érdekében Olaszország az 1980-as évek elején még szorosabbra fűzte kapcsolatát az Egyesült Államokkal. Folyamatosan növelte katonai fennhatóságú területeit, amelyeket elsősorban az amerikai és a NATO erői rendelkezésére bocsátott. A magyar hírszerzés értesülései alapján Olaszországban radarbázist létesítenek, rakétákat telepítenek, páncélos kiképzés és gyakorlótér működik majd, bővítik az amerikai bázisokat, és új amerikai tengeralattjáró támaszpont jön létre. Mindezek mellett az amerikai hadsereg további három bázist alakít ki Olaszország területén. Az új bázisok kialakítása és a már meglévők bővítése azonban rengeteg költséggel járt volna, amiket az olasz kormány nem tudott bevállalni, ezért a fejlesztési költségek 70%-át az Egyesült Államok magára vállalta, míg a NATO további 10%-os hozzájárulást ajánlott fel. A NATO külügyminiszterei 1980-as római tanácskozásán Olaszország az amerikai politika melletti teljes elköteleződésének adott hangot, és további új bázisokat ajánlott fel Washingtonnak, például Augustában, ahol atom-tengeralattjárók, AWACS-gépek és vadászgépek állomásozhattak, illetve egy kiegészítő megegyezésben ígéretet tettek arra, hogy a Szicíliaiba telepítendő cirkálórakéták számát megemelik. Ennek ellenére „Von Schiller” arról tájékoztatta a magyar hírszerzést, hogy a hivatalos bejelentéssel ellentétben Comisóban nem fognak 127 rakétát tárolni. Szerinte ennek legfeljebb az egyharmada várható a támaszpontra, míg a többit széttelepítik Olaszország egyéb részein. A tervek szerint egyébként a bázisnak három éven belül el kell készülnie, és összeköttetésben áll majd az AWACS-rendszerrel, öt éven belül pedig nukleáris fejekkel is felszerelik majd a rakéták egy részét.⁶⁷

Az imént említett események azt mutatják, hogy az 1970-es évek végén és az 1980-as évek elején Olaszország fokozott aktivitást fejtett ki a Földközi-tenger medencéjében. Ennek érdekében az olasz kormány szorgalmazta, hogy a madridi értekezleten központi kérdés legyen a földközi-tengeri biztonság és együttműködés. Madridban Colombo úgy fogalmazott, hogy *„Földközi-tengeri ország minőségünkben nagy jelentőséget tulajdonítunk annak a fejezetnek, amelyet a záróokmány szentel ennek a bizonytalan és kényes egyensúlyú térségnek, amely egyensúlynak a felbomlása súlyos és destabilizáló következményekkel járna a világ szélesebb értelemben vett*

⁶⁶ A SALT (Strategic Arms Limitation Talks) II. megállapodást 1979. június 18-án Bécsben írta alá Brezsnyev és Carter, az afganisztáni szovjet intervenció miatt azonban az amerikai elnök 1980. január 1-jén levette a szenátus napirendjéről annak ratifikálását.

Lásd: HORVÁTH – PARAGI – CSICSZMANN 2014, 257-263.

⁶⁷ ÁBTL 3.2.3 Mt 867/15. 5-47. o. Információs jelentés, Budapest, 1980.november 20.

egyensúlyára is...”. A kijelentéssel összhangban Olaszország felvetette egy 1982-es össz-földközi-tengeri értekezlet összehívását. A Mediterráneum egyensúlyának és biztonságának megteremtése érdekében Róma célja a bipolaritás helyett a konstruktív multipolaritás elérése volt, vagyis a két szuperhatalom mellé szeretne volna felzárkóztatni a világ többi részét, elsősorban természetesen Nyugat-Európát. De akármennyire is szeretett volna Olaszország a Földközi-tenger térségének kiemelkedő hatalma lenni, és meghatározó szerepet vállalni az itteni biztonság és egyensúly kialakításában, valójában nem volt meg sem gazdasági, sem katonai ereje ahhoz, hogy valószínű vezető szerepet töltsön be a térségben. Éppen ezért Róma az Egyesült Államok egyik leghűségesebb szövetségese maradt, és rendszeresen fellépett az amerikai érdekek képviselőjében.⁶⁸

Ezt az elképzelést megerősíti, hogy Colombo 1981. október 1-2-án a Képviselőházban tartott beszámolójában kijelentette, hogy az Egyesült Államoknak tetsző külpolitikai irányvonalon kíván maradni, és ennek érdekében megvédte az eurorakéták telepítésének tervét, a neutronbomba kérdésére pedig csak annyit mondott, hogy ez amerikai belügy, ami nem érinti Olaszországot.⁶⁹ Ez utóbbi megnyilatkozását úgy tűnik, hogy valóban komolyan gondolta, ugyanis amikor 1981 februárjában az Egyesült Államokban járt, akkor tárgyalásai során egyáltalán nem érintette a neutronbomba kérdését. Amerikai partnereivel inkább a védelmi képességek növeléséről és az olasz hadiflotta esetleges támadó feladatairól egyeztetett, illetve szóba került, hogy Olaszország katonai erőket küld a Sínai-félszigetre. Ezzel a második világháború vége óta először vetnének be olasz katonai egységeket a NATO körzetén kívül. Az amerikai út során természetesen szóba kerültek az eurorakéták is, amellyel kapcsolatban kijelentették, hogy az amerikai–szovjet tárgyalásoktól függetlenül bizonyos számú rakétát telepítenek Nagy-Britanniába, az NSZK-ba és Olaszországba, míg ideiglenes jelleggel a többi egyelőre tengeralattjárókon helyezik el. Az út alatt az amerikai sajtóban nem éppen felmagasztaló stílusban Olaszországot „önkorlátozott szuverenitású országnak”, illetve a „legamerikaibb európai országnak” bélyegezték, utalva arra, hogy Róma milyen mértékben szolgálja ki Washington érdekeit, és veti alá magát az amerikai akaratnak.⁷⁰

Az eurorakéták Olaszországba telepítése, a comisói bázis kijelölésének elsőként való bejelentése és a hadiköltség jelentős, közel 5%-os emelése, szemben a NATO által elvárt 3%-al azonban negatív változásokat eredményeztek a katonai enyhülésben. Ehhez hozzájárult az is, hogy bár Olaszország csatlakozott a zéró opcióhoz, vagyis a tömegpusztító fegyverek legalacsonyabb szintű korlátozásához, mégis fokozódó agresszivitást fejtett ki. Ezt az agresszivitást bizonyítja, hogy az olasz vezető körökben egyre több támogatója volt annak a francia javaslatnak, hogy Európában létre kéne hozni egy európai elrettentő nukleáris erőt. Ezzel párhuzamosan azonban folyamatosan megerősítették NATO-hűségüket. Lagorio hadügyminiszter például

⁶⁸ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1981/119. Jelentés, Róma, 1981. február 19. 1-4. o.

⁶⁹ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1981/120. Jelentés, Róma, 1981. október 14. 1-2. o.

⁷⁰ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1981/119. Jelentés, Róma, 1981. március 23. 1-6. o.

kijelentette, hogy a NATO a béke legfőbb biztosítója Európában, míg Luns főtitkár Olaszországot a NATO legszilárdabb szövetségének titulálta.⁷¹

Olasz haderőfejlesztés

A NATO-főtitkár szavainak természetesen volt alapja. Olaszország aktívan kivette részét az újrafegyverkezésben, amit bizonyít, hogy 1978–1985 között Róma 1777 milliárd lírát költött védelmi kiadásokra, többet, mint a hidegháború kezdete óta bármikor. Az országban az 1970-es évek végén és az 1980-as években megfigyelhető katonapolitikai dinamizmus annak is köszönhető volt, hogy a korszakban minden politikai erő elfogadta az atlanti blokkhoz tartozást. Az eurorakéták telepítése Olaszországot különleges helyzetbe hozta, hiszen bizonyította a belső kohéziót. Az, hogy 1980-ban Lagorio, egy szocialista politikus lett a védelmi miniszter, egyértelmű jele volt annak, hogy a PSI elfogadta az atlanti vonalhoz tartozást, ez pedig hozzájárult ahhoz, hogy az 1980-as években Olaszország megerősítette szerepét a NATO-n belül, míg korábban csak egy marginális országa volt a szövetségnek. 1981 és 1984 között például a falklandi háborúban érintett Nagy-Britannián kívül az egyetlen ország volt, ahol nőtték a katonai kiadások, méghozzá 12,5%-kal. A fegyveres erők átstrukturálásának köszönhetően az olasz hadsereg kompatibilisabb, jobban integrálható lett a NATO technológiai innovációjához, amit a cirkálórakéták, a Tornado repülőgépek mellett a Garibaldi 1984-es átadása is bizonyít. Az Atlanti Szövetség körülbelül 30 évig csak kontinentális érdekeltséggel rendelkezett, ám ebben az 1980-as években változás állt be, ami a Földközi-tengert is érintette. Ennek hatására az olasz kül-és katonapolitika is aktivizálódni kezdett. Rogers tábornok kijelentette, hogy *„A NATO-nak nagyobb érdeklődéssel kell Olaszországot figyelnie... [amely] a Mediterráneumban a Szövetség védelmi rendszerének kulcsa [lett]”*. Rogers kijelentése egyet jelentett Olaszország feladatának a növekedésével, ami igazi vezető szerepet eredményezett a Földközi-tengeren.⁷²

A vezető szerep miatt Rómának csak még erősebb lett a viszonya az Egyesült Államokkal. A rendkívül szoros kapcsolatok miatt írhatták azt egy 1981-es nagykövetségi jelentésben, hogy Olaszország az USA-val egyeztetett külpolitikát folytat, azonban nem önálló elképzelés nélküli NATO-ország, és törekszik egy önállóbb külpolitikára. Bár alapvető érdekei egybeesnek a NATO, vagy az Egyesült Államok érdekeivel, de kisebb ügyekben időnként ezekkel ellentétes álláspontra helyezkedik. Az olasz katonai vezetés pedig igyekszik nagyobb önállóságra szert tenni, hogy „első vonalban lévő NATO-országgá” tudjon emelkedni. Ehhez viszont támogatásra van szüksége, amely magába foglalta a hadiköltségek megemelését, a saját haderő korszerűsítését és a kiképzési szint növelését. Ezekkel, illetve az eurorakétákkal és a neutronbombával Olaszország hozzá tudna járulni a katonai erőegyensúly kialakításához. Amennyiben ez megvalósulna, abban az esetben Olaszország vezető szerepre tudna szert tenni a Földközi-tengeren, amely gazdasági érdekei mellett politikai ambíció is, ugyanis a nagy döntések meghozatalából Róma eddig rendre

⁷¹ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1981/119. Jelentés, Róma, 1981. november 13. 3-6. o.

⁷² MINOLFI 1993, 136-139.

kimaradt. Mivel az olasz vezetés szerint az európai nyugalmat leginkább a földközi-tengeri feszültség veszélyeztette, ezért is igyekezett az olasz kormány kezdeményező félként fellépni az itteni enyhülés és együttműködés felé. A vezető szerep megszerzése érdekében döntés született új amerikai bázisok koncessziójáról, a hadiipari termelés megnöveléséről és az olasz haderő arányosabb elosztásáról az országon belül – amelyre már csak az amerikai katonai jelenlét csökkentése miatt is szüksége volt –, míg Lagorio rendszeresen hangoztatta, hogy egy konfliktus esetén „Olaszország területe lenne a lőtér”, ezzel nem kis nyomást helyezve nyugati szövetségeseire.⁷³

Ennek a nyomásgyakorlásnak meg is lehetett a következménye, ugyanis a magyar hírszerzés információi szerint 1982-re nukleáris kutatólabort létesítenek országban. A látszólag polgári célokat szolgáló, de valójában katonai kutatásokat is végző labort 20 millió dollárból építik fel. Mindemellett a Lazióban található NATO-bázist és radarállomást kiterjesztik, és Santa Luciában vegyifegyver-raktárat építenek, ahol elsősorban amerikai vegyifegyvereket fognak tárolni. „Von Schiller” azzal a hírrel szolgált, hogy a földközi-tengeri stabilitás miatt a 6. flotta tengerészeti gyakorlatokat fog rendezni Ciprus partjainál, míg Comisóban már jól haladnak a bázis kialakításával. A római rezidentúra jelentése azonban kihangsúlyozza, hogy ez a bázis valójában csak a NATO és az Egyesült Államok félrevezető hadművelete az ellenzéki csoportok azonosítására, az itt elhelyezett rakéták közel fele egyszerű utárat, és az igazán fontos támaszpontok az ország más részein lesznek elhelyezve.⁷⁴

Annak ellenére, hogy a magyar hírszerzés rendszeresen kapott olyan jelentéseket, amelyek az olaszországi bázisok és katonai létesítmények bővítéséről szóltak, 1982-ben egy római magyar nagykövetségi jelentés szerint az országnak mégis az enyhülés az érdeke, hiszen csak így alakulhat ki politikai és katonai egyensúly a két szemben álló tömb között, és türelmet, illetve önkormányzott eredményezhetne mindkét oldalon. Közben azonban Rómának figyelemmel kell lennie a katonai helyzet változására a Földközi-tengeren, a görög–török kapcsolatok alakulására, Málta helyzetére, a Közel-Keletre és a Maghreb-térségre, illetve a katonai egyensúly fenntartására a lehető legalacsonyabb szinten. Mivel Olaszország elhelyezkedéséből és geopolitikai helyzetéből adódóan a nyugati világ része, a nyugati világ őre a NATO délkeleti szektorában, ezért mind a Kelet-Nyugat, mind az Észak-Dél problémákban érintett. Ebből kifolyólag az olasz külpolitikai három legfőbb pillére az Egyesült Államok, az Atlanti Szövetség és az Európai Közösség.⁷⁵

A nyugati világ őreként azonban Olaszországnak szembesülnie kellett azzal a falklandi háború kapcsán levont tapasztalattal, hogy a NATO egy erős flottával sem lenne képes kivédeni egy általános támadást a Földközi-tengeren. Mivel a nyugati szövetségi rendszerben ekkor Görögországra nem számíthattak, ezért döntés született szárazföldi bázisú légierő kiépítéséről, és hogy a hagyományos tengeri erőket

⁷³ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1981/121. Jelentés, Róma, 1981. április 24. 1-6. o.

⁷⁴ ÁBTL 3.2.3 Mt 867/15. 51-87. o. Feljegyzés, Budapest, 1981. október 26.

⁷⁵ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1982/112. Jelentés, Róma, 1982. január 16. 10-12. o.

felcserélik tengeralattjáró és rakétahordozó hajók kombinációjával. Olyanokkal, amilyeneket „Von Schiller” szerint Olaszországban már építenek. Mivel a Földközi-tenger instabilnak számított, ezért a NATO-ban egyetértettek abban, hogy emelni kell a hadiköltségeket, végre kell hajtani a fegyverzetstandardizálást és fejleszteni kell a szövetség erőinek utánpótlását. A falklandi háború ugyanis megmutatta, hogy mi történik abban az esetben, ha kombinált légi és rakétatámadások érnek egy nem kellően felkészült tengeri erőt. Ezt adaptálták a 6. flottára és a vegyes tengeri erőkre, hiszen, bár a 6. flotta tüzereje és légierője nagyobb, mint a vele szemben álló flottáé, de egy masszív rakétatámadás komoly veszélyt jelentene a NATO tengeri erőire és a nukleáris létesítményekre. Olaszországban attól féltek, hogy az Egyesült Államokban és a NATO-ban alábecsülik a támadó rakétarendszerek ütőerejét, és figyelmen kívül hagyják az elektronikus elhárítórendszerek jelentőségét, így egy konfliktus esetén a földközi-tengeri erők tétlenségre lennének ítélve. A tervek szerint, amennyiben a Dardanellák és a Szezi-csatorna elesne, abban az esetben aktivizálják a tengeralatti aknarendszert, hogy az ellenséges hajókat megállítsák Afrika és az Adriai-tenger között, ám ha ez nem sikerülne, akkor az anyahajó-flottát és a felszíni tengeri erőket átcsoportosítanák a Földközi-tenger nyugati medencéjébe, így a keleti medence szabadabbá válna a rakéták számára.

Európa, mint „harmadik erő”

A nyugati szövetségi rendszeren belül viszont komoly gondokat okozott Reagan kormányzása, ami a politikai légkör állandó torzulását eredményezte. Ebből kifolyólag a nyugat-európai szövetségesek úgy döntöttek, hogy amennyiben nem valósul meg a NATO revíziója, abban az esetben egy összeurópai fegyveres erőt alakítanak ki. Bár a tervet Nagy-Britannia ellenezte, az Egyesült Államok pedig pénzügyi és gazdasági nyomást gyakorolt a tagállamokra ennek halogatására, Franciaország és az NSZK mégis előkészített egy katonai együttműködésről szóló szerződést, amihez Olaszország is szívesen csatlakozott volna. Ezt azzal indokolták, hogy ha Reagan nem korrigál, az azt eredményezheti, hogy a NATO elavulttá válik, így fel kell készülni arra, hogy Európát „harmadik erővé” kell alakítani. A magyar hírszerzés azonban Olaszországot az Egyesült Államok “trójai falovának” tekintette, amely kettős játékot űz, és miközben elvileg támogatja Franciaországot egy független katonai erő létrehozásában, közben folyamatosan tájékoztatja Washingtont az európai lépésekről. Teszi mindezt újabb amerikai kölcsönök reményében.⁷⁶

Lagorio honvédelmi miniszter 1982 novemberében felszólalt a Képviselőház Védelmi Bizottságának ülésén. Felszólalásában hangsúlyozta, hogy „*az Atlanti Szövetség földrajzilag körülhatárolt védelmi szövetség, amely szuverén, saját önállóságukra és függetlenségükre kényes államok szövetsége*”. Ennek értelmében szerinte szükség van a tagállamok közötti további szilárdításra, hiszen a NATO az európai béke biztosítója, de Olaszország szuverén állam, amelynek politikája nagyrészt megegyezik a NATO politikájával, viszont nem ért egyet a szövetség minden lépésével.

⁷⁶ ÁBTL 3.2.3 Mt 867/15. 109-128. o. Információs jelentés, h. n., d. n.

Ez a szövetség az 1970-es évek közepéig teljes védelmi garanciát nyújtott az országnak, ez azonban a nemzetközi helyzet változása miatt megszűnt Olaszország vonatkozásában. Az 1970-es évek második felétől nukleáris vonatkozásban a Varsói Szerződés 3:1-hez arányban áll a NATO-hoz képest, a bécsi tárgyalások holtpontra jutottak, a genfi tárgyalások pedig lassan haladnak. Róma mégis bízik a „nulla alternatíva” elérésében, és akkor nem telepítenek majd cirkálórakétákat és Pershing II-t az országba. Olaszország európai és mediterrán ország, ebben a kettős minőségében pedig mindent megtesz a stabilitás és az enyhülés érdekében, négy problémával azonban mindenképpen szembe kell néznie: a Varsói Szerződés fegyverrendszerének fejlődésével, a mediterrán térség növekvő instabilitásával, a csökkenő amerikai légi és tengeri jelenléttel, és azzal, hogy Olaszország minden irányból ki van téve támadás veszélyének. Éppen ezért Olaszországnak szüksége lenne modern védelmi rendszerre, ám nincs anyagi forrása ennek megteremtésére. Példaként Nagy-Britanniát, Franciaországot és az NSZK-t hozta fel, amelyeknek védelmi kiadásai szerinte háromszor nagyobbak az olasz védelmi kiadásoknál. Az anyagi, pénzügyi gondok miatt nem sikerült végrehajtani a fegyveres erők átszervezését, modernizációját, és fejlesztési folyamatát, amelyről még az 1970-es évek közepén született döntés, és amit 1985-ig le kellene zárni. Ezek a gazdasági problémák azt okozzák, hogy a Legfőbb Védelmi Tanács 1981 januárjában elfogadott programját 1990-re kell halasztani, az 1983-as védelmi költségvetésből 950 milliárd lírát le kell faragni, és a NATO felé vállalt 3%-os katonai költségemelését még sosem sikerült teljesíteni.⁷⁷

1983 elején a NATO-ban jelenést írtak az atlanti védelem kilátásairól az 1980-as évekre vonatkozóan. A jelentés szerint az elrettentés politikája eddig kettő fejlődési szakaszon ment keresztül, és most jár a harmadikban: az 1950-es években még létezett az atomfegyver amerikai monopóliuma, az 1970-es évek közepéig még megvolt az amerikai nukleáris arzenál fölénye, jelenleg azonban már egyenlőség alakult ki, így a Nyugat többé nem számíthat előnyre. Az SS20-asok váratlan fenyegetést jelentenek, ami miatt megszűnt Európa felett az amerikai nukleáris ernyő, a hagyományos erők fejlesztése pedig lassú és költséges, így a NATO stratégiai struktúrájában csak az eurorakéták okozhatnak revíziót és változást. Ez viszont azt jelenti, hogy szükség van a stratégiai direktívák újragondolására, hiszen a hatékony védelmi elrettentés nem csak katonai, hanem politikai természetű szükséglet is. Ennek eléréséhez elégséges katonai szerkezet és politikai egyetértés kell. A NATO elrettentési stratégiájának lényege, hogy az eszközök és a következmények ismertek az ellenséges erőknek, ezzel megelőzik a kalandor kezdeményezéseket. A Szövetség elrettentési politikájában azonban két szükséglet van: az egyik az Európa és az Egyesült Államok védelmének kapcsolata, ami az eurorakétákkal megvalósult, a másik az európai nukleáris konfliktus elkerülése, ami viszont még nem teljesen valósult meg. Ennek érdekében Sam Nunn amerikai szenátor, az amerikai Védelmi Bizottság tagja elutazik az európai fővárosokba, hogy a tagállamokat meggyőzze a NATO katonai stratégiája iránti elköteleződésről, és

⁷⁷ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1982/112. Jelentés, Róma, 1982. november 16. 1-5. o.

megértesse a nyugat-európai kormányokkal, hogy a hagyományos struktúrák modernizálásán túl szükség van a nukleáris védelem kialakítására is.⁷⁸

A védelem kialakítása azonban igencsak akadozott, ugyanis az irányítóberendezésekkel kapcsolatos problémák miatt a cirkálórakéták olaszországi telepítése elhúzódott. A magyar hírszerzés szerint az első rakéták augusztusban érkeznek majd, méghozzá két ütemben, először Camp Darby-re, ahonnan továbbítják majd a többi bázisra. Ezt követően szeptemberben újabb szállítmányok várhatók. A magyar hírszerzést arról is értesítették, hogy 1984-re elkészül az augustai támaszpont, ami a 6. flotta gaetai és nápolyi bázisainak felváltására épült. Itt lesz a NATO mozgó tengeri erőinek legfontosabb támaszpontja, és az Olasz Legfelsőbb Tengerészeti Parancsnokságának alternatív bázisa, ahonnan nem csak Comisót lehet fedezni, de visszavonulás esetén is használható az ellenséges erőkkel szemben. Mindeközben Nagy-Britanniában, az NSZK-ban és Olaszországban a vegyipari kutatóintézetek egy új japán festékkal kísérleteznek, ami képes elnyelni a radarsugarakat, így az ellenség nem tudja érzékelni és szemmel tartani a légielő gépeit. A hírek alapján a festéket már átadták kipróbálásra az amerikai légielőnek, és amint beválik, az európai NATO haderő is megkapja felhasználásra. Eközben pedig Washington folyamatosan bővíti rakétakilövő eszközeit, légifigyelő berendezéseit, és rakétairányítási rendszereit a Közép-Mediterráneumban, amelyek közvetlenül az amerikai légi és tengeri parancsnokságainak felügyelete alatt állnak, így függetlenek a NATO-tól, és szorosan kapcsolódnak a cirkálórakéták Comisóba és Közép-Olaszországba, illetve a Pershing II-k Közép- és Észak-Olaszországba való telepítésével. Ezeknek az irányítóberendezéseit Comisóban, Pantellerián és Lampedusán lesznek elhelyezve, utóbbi helysín pedig a technikai ellenőrzés és irányítás központja lesz, sőt, az itt létrejövő új bázis képes lesz Észak-Afrika és a Közel-Kelet ellenőrzésére is.⁷⁹

A comisói bázis

1983. március 8-9-én Colombo az Egyesült Államokban járt, hogy egy egységesített nyugat-európai álláspontot képviseljen eurorakéták és a Kelet-Nyugat kapcsolatok ügyében. A találkozón az olasz miniszterelnök arra kérte az amerikai elnököt, hogy a tárgyalások folytatása érdekében tegyen új javaslatot Genfben, hiszen annak ellenére, hogy a végcél a nulla megoldás lenne, Nyugat-Európa elképzelhetőnek tartott közbülső megoldásokat, mint például a cirkálórakéták és a Pershing II részleges telepítése, ha cserében a Szovjetunió visszavonja az SS20-as, az SS4-es, és az SS5-ös rakétáinak egy részét. Az olasz kormányfő ugyanakkor kilátásba helyezte, hogy amennyiben a genfi tárgyalások holtpontra jutnak, abban az esetben 1983 decemberétől megkezdik a rakéták telepítését Olaszországba. Colombo útja azonban sikertelen volt, hiszen Reagan elnök nem volt hajlandó megváltoztatni az amerikai álláspontot a genfi

⁷⁸ ASILS AGA NATO series Report by Permanent Representative to NATO Torretta to Minister of Foreign Affairs Colombo, 'Perspectives about Atlantic defense for the 1980s', 1983. február 15. 1-10. o.

⁷⁹ ÁBTL 3.2.3 Mt 867/16. 11-45. o. Információs jelentés, h. n., d. n.

tárgyalásokon. Azt viszont az olasz miniszterelnöknek sikerült elérnie, hogy újabb amerikai gazdasági segítséget kapjon az ország, ezzel fokozva a pénzügyi együttműködést. Ezért cserében viszont ígéretet kellett tennie arra, hogy a libanoni–izraeli határ garantálása érdekében Olaszország és a többi európai szövetséges csapatokat küld a térségbe, ezzel tulajdonképpen egyfajta csendőrszerepet betöltve a Közel-Keleten.⁸⁰ A washingtoni tárgyalásokon elhangzottakat megerősíti egy későbbi nagykövetségi jelentés, ami szerint Olaszország legfontosabb lépése az eurorakéták telepítése, és ha Genfben nem sikerül előrehaladást elérni, akkor az Európában elsőként bejelentett comisói bázis határidőre elkészül, ugyanis a munkálatokkal a tervek szerint haladnak. A comisói építkezés második szakaszára Reagan 200 millió dollárt ajánlott fel Olaszországnak, amely összeg 60%-a a NATO költségvetését terhelte.

Ezzel párhuzamosan Spadolini kijelentette, hogy Olaszország új katonai alakulatok felállításába kezdett, míg Észak-Olaszország túlzásúfoltága miatt a régebbi alakulatokat elkezdték áthelyezni. Beszédében azt is kihangsúlyozta, hogy meg kell teremteni a hadsereg és a polgári lakosság jobb együttműködését, ugyanis az olasz közvélemény egy jelentős része ellenezte a rakétatelepítéseket, és békemozgalmakat szerveztek a comisói támaszpont ellen. Bár ezeket a mozgalmakat a kormány igyekezett figyelmen kívül hagyni,⁸¹ 1983 nyarán már nemzetközi találkozót szerveztek a fegyverkezés ellen Olaszországban, és folyamatossá váltak az üléssztrájkok, a torlaszépítések és a kerítésrongálások. Az események odáig fajultak, hogy 1983 júliusa és szeptembere között több összecsapás is volt a tüntetők és a rendőrök között. Az olasz és az amerikai vezetést azonban nem igazán hatották meg ezek az események. Weinberger amerikai védelmi miniszter a békemozgalmakra meglehetősen cinikusan csak annyit reagált, hogy *„a rakétákat telepítik, a többit meg majd meglátjuk”*.⁸² De hogy a rakétákat valóban telepítették-e, és milyen tempóban, arról már megoszlottak a vélemények. 1983. október 4-én Hágában a NATO őszi ülésén angol képviselők előadtak egy jelentést az atomfegyverek telepítéséről, aminek során a comisói bázis állapotát is felmérték. A jelentésben azt közölték, hogy az építésben pár hónapos csúszás figyelhető meg, így a várható átadás csak 1984 márciusában következik be. Ezzel szemben Spadolini azt mondta Weinbergernek, hogy a rakétákat időben telepítik, hacsak Genfben nem sikerül megegyeznie a két szuperhatalom képviselőinek.⁸³ Nem sokkal később „Von Schiller” azt jelentette a magyar hírszerzésnek, hogy az első 12 cirkálórakéta már Olaszországban, a comisói bázison van, igaz, még nincsenek összeszerelve. Értesülései szerint két éven belül az összes rakéta megérkezhet Olaszországba, sőt, úgy tudja, hogy végül az eredetileg tervezett rakétáknak a kétszeresét fogják Olaszországba telepíteni.⁸⁴ „Von Schiller” értesüléseit megerősítik a korabeli újságírói információk, amelyek arról szóltak, hogy a rakétatelepítést még az év vége előtt megkezdik, bár a csúszás miatt elképzelhető, hogy egyelőre a

⁸⁰ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1983/101. Jelentés, Róma, 1983. március 12. 1-7. o.

⁸¹ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1983/102. Jelentés, Róma, 1983. szeptember 4. 1-3. o.

⁸² MNL OL XIX-J-1-j Olaszország KÜM TÜK 1983/102. Jelentés, Róma, 1983. október 14. p. 1.

⁸³ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1983/102. Jelentés, Róma, 1983. október 14. 1-2. o.

⁸⁴ ÁBTL 3.2.3 Mt 867/16. 53. o. Információs jelentés, 1983. november 14.

tervezetnél kevesebb rakéta lesz Olaszországban. Ezek az információk is alátámasztják, hogy Rómának fontos volt a rakétatelepítés, mert az ország rá volt szorulva az amerikai rakétákra, és ezzel akarták a NATO ernyőjét megerősíteni Olaszország felett.⁸⁵

Spadolini egy parlamenti felszólalásában arról beszélt, hogy Olaszország a NATO-n belül a katonai hozzájárulás terén a legkevesebbet fizetők között van, ezért arra szólította fel képviselőtársait, hogy szavazzák meg az anyagi áldozatvállalás megemelését. Indoklasként azt hozta fel, hogy Olaszország nem tudja magát megvédeni egy nagyhatalmi támadástól, ezért a NATO szempontjainak figyelembevételével fejleszteni kell az olasz haderőt, és legkésőbb 1991-re végre kell hajtani az olasz véderő átszervezését. A római magyar nagykövetség szerint Spadolini azért is akarta fejleszteni az olasz haderőt, mert az olasz kormányban az volt a célja, hogy negyedik európai nagyhatalommá nője ki magát, ez azonban mind gazdasági, mind katonai súlyát meghaladta az országnak.

Közben Genfben folytak a tárgyalások a leszerelésről, amelyek kapcsán a nyugat-európai szövetségesek szorgalmazták egy egységes európai álláspont megfogalmazását annak érdekében, hogy ezáltal elérjék az európai csatlakozást a tárgyalásokhoz, és abban bíztak, hogy a Pershing II-esek okozta fenyegetés miatt a Szovjetunió hajlandó lesz újrainyitni az érdemi tárgyalások felé. Moszkva azonban nem akarta elfogadni azt az amerikai javaslatot, hogy a START-ba számítsák bele az eurorakétákat, és az SS20-asokat, illetve az SS5-ösöket is.⁸⁶ A fegyverzetkorlátozási, illetve -leszerelési tárgyalásokat viszont akadályozta a rendkívül feszült nemzetközi helyzet, amit a dél-koreai repülőgép-szerencsétlenség⁸⁷ és a grenadai amerikai beavatkozás idézett elő.⁸⁸

⁸⁵ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1983/102. Jelentés, Róma, 1983. október 28. 1. o.

⁸⁶ ASILS AGA NATO series Telegram by Ambassador Rinaldo Petrignani, 'Prospects of resuming the FNI negotiations', 1983. december 5. 6-7. o.

⁸⁷ 1983. szeptember 1-én egy dél-koreai Boeing 747-es utasszállító berepült a Szovjetunió légterébe. Mivel a leszállásra vonatkozó felszólításokra nem reagált, ezért szovjet vadászgépek lelőtték. A gép mind a 269 utasa és a teljes személyzet életét veszítette. Az ENSZ BT 9 tagja elítélte az esetet, és vizsgálatot követelt, ezt azonban a Szovjetunió megvétőzte. Pár nappal a szerencsétlenség után Reagan szankciókat hídett meg a Szovjetunió ellen. A Közös Piac tagjai, köztük Olaszország részvételét nyilvánította ki az áldozatok hozzátartozóinak, de nem ítélte el az akciót. Lásd: Pók Attila: A nemzetközi élet krónikája 1945-1997. *História*, Budapest, 1998. 207-208. o.

⁸⁸ Grenada 1974-es függetlenségének kikiáltása után az 1976-os választásokon a baloldali pártok győztek. A választás után Maurice Bishop puccsot hajtott végre, és kubai segítséggel új kormányt alakított, majd felfüggesztette az alkotmányt és diktatúrát vezetett be. Néhány évvel később Bishop megintcsak Kuba támogatásával egy „nemzetközi repülőter” felépítését jelentette be, és kereskedelmi szerződést kötött a Szovjetunióval. 1983-ban azonban hatalmi harc kezdődött az országban, amelynek során Bernard Coard átvette a hatalmat, és 1983. október 19-én kivégeztette Bishopot. Két nappal ezt követően a Kelet-karibi Államok Szervezete felhatalmazta az Egyesült Államokat a beavatkozásra, amely október 24-én meg is kezdődött, és amelynek során az amerikai hadsereg hat nap alatt az egész szigetre kiterjesztette befolyását. Lásd: MAGYARICS Tamás: *Az Egyesült Államok külpolitikájának története. Mítosz és valóság: érdekek és értékek*. Antall József Tudásközpont, Budapest, 2014. 494-495. o.

A WEU feltámasztásának terve

A növekvő nemzetközi feszültség és Kissinger állítólagos meglehetősen negatív véleménye a közvéleményről és a nyugat-európai kormányokról⁸⁹ önálló cselekvésre ösztönözték a nyugat-európai szövetségeket, ezért 1984. január 31-én Franciaország javaslatot tett a WEU feltámasztásáról. A felélesztett szervezet létrehozhatja az európai együttműködést a biztonsági kérdésekben, és új katonai dimenziókat nyithat. Olaszország támogatóan viszonyult a WEU újjáélesztéséhez, amíg a szervezet hatékonyan együtt tud működni a NATO-val, sőt, az amerikai kormány is kijelentette nyitottságát a WEU felé. Ezek következtében 1984. június 12-én Párizsban megrendezték a WEU miniszteri szintű tanácskozását, ahol megszabták az általános irányvonalakat, és megvizsgálták két szervezet, a CPA (Fegyverkezés Állandó Tanácsa), és az ACA (Fegyverzet-ellenőrzési Szervezet) feladatait. Mivel a WEU célja egy integrált hadsereg felállítása volt, ezért egyrészt ezt a helyzetet tisztázni kellett a NATO-val, másrészt a CPA-n keresztül nagyobb együttműködést igyekeztek kialakítani a fegyverzetgyártásban, főleg a hagyományos fegyverek területén.⁹⁰

Időközben Thatcher miniszterelnök befagyasztotta a nukleáris fegyverek elhelyezésének folyamatát, ezért Olaszországban attól tartottak, hogy kialakulóban van egy Nagy-Britanniából, Franciaországból és az NSZK-ból álló atomvédelmi trojka, ami az ország elszigetelődéséhez vezethet. Amennyiben ez megvalósulna, a hírek szerint az olasz kormány előtt három alternatíva kínálkozott: lemond a WEU-tagságáról, és kétoldalú szövetséget alakít ki az Egyesült Államokkal, vagy atomfegyverek gyártásába kezd, így hozva létre az Európai Négyeket, esetleg tárgyalásokat kezdeményez a Varsói Szerződés tagállamaival a Mediterráneum denuklearizálásáról. A magyar hírszerzéshez eljutott információk arról szóltak, hogy a WEU következő ülésén Olaszország arra készül, hogy Nagy-Britanniával, Franciaországgal és az NSZK-val szemben szavazzon az Európai Biztonsági Tanács létrehozásának tervéről. Craxinak ugyanis az volt a véleménye, hogy egy ilyen szervezet a NATO megsemmisítéséhez vezetne.⁹¹

1984 márciusában Spadolini újra tájékoztatta az olasz parlamenti képviselőket a rakétatelepítésről. Azt ígérte, hogy március végére operatívvá teszik a comisói cirkálórakéták egy részét, és bár számokat nem közölt, információk szerint egyelőre 16 rakétáról volt szó. Ezt követően kitért arra, hogy további időre van szükség ahhoz, hogy a kiegészítő struktúrákat kiépítsék, és végrehajtsák a személyzet kiképzését.⁹² A már telepített 16 rakétáról elmondta, hogy ezek gyakorlatilag már hadrafoghatók, de csak az olasz kormány beleegyezésével lehet kilőni. Majd hozzátette, hogy a

⁸⁹ ASILS AGA NATO series Telegram by the Ambassador to the United States Petrigiani to Ministry of Foreign Affairs, 'Prospects of resuming the FNI negotiations', 1984. március 1. 1. o.

⁹⁰ ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'UEO -Updated positions of the Seven about the relaunch of the Organization-Preparatory works of the Ministerial Council in June', 1984. május 26. 1-4. o. Elérhető:

⁹¹ ÁBTL 3.2.3 Mt 867/16. 104-106. o. Infirmációs jelentés, Budapest, 1984. február 20.

⁹² MNL OL XIX-J-1-j Olaszország KÜM TÜK 1984/117. Jelentés, Róma, 1984. április 11. 1-2. o.

telepítést amerikaiak végzik, és a támaszpont amerikai parancsnokság alatt áll.⁹³ Néhány hónappal később, 1984 májusában a NATO védelmi minisztereinek brüsszeli tanácskozásán Spadolini hozzájárult az amerikai cirkálórakéták számának növeléséhez 1985-től kezdve. A rakétákat továbbra is elsősorban Comisóba, másodsorban Észak-Olaszországba telepítik majd, és a tervek szerint új Tomahawkok, illetve 12-18 Pershing rakéta állomásoztatására tett ígéretet.⁹⁴

Bár a korszakban természetesen a rakétatelepítés volt a legfontosabb kérdés a NATO-n belül, de az Egyesült Államok sérelmezte, hogy emiatt néhány fontos téma háttérbe szorult, mint például a nagyobb európai részvétel a közös védelemben, vagy a hagyományos haderő megerősítése.⁹⁵ Az amerikaiak által meghirdetett célok összefüggésben állhattak azzal, hogy az Egyesült Államok nyomást gyakorolt Olaszországra, aminek következtében Róma egy új fegyverkezési programot hirdetett. Ennek értelmében belekezdtek egy 38 ezer tonnás anyahajó építésébe, amely alkalmas Harrierek szállítására is, illetve a Tengerészeti Minisztérium terve szerint 5 éven belül elkészül egy 80 ezer tonnás hajó.⁹⁶ Az egyre nagyobb amerikai elvárásokat és az USA olaszországi térnyerését egyes olasz lapok már nem nézték jó szemmel. Több újságcikk is megjelent arról, hogy a 6. flotta beosztottainak Washington házakat, telkeket bérel évi 10 millió dollár értékben az olasz tengerparton, és az amerikai politikai és gazdasági ellenőrzés fenntartása érdekében az amerikai kormány még akár a Cosa Nostrát is felhasználja.⁹⁷

Az új hajók építése része volt annak a Spadolini által meghirdetett célnak, ami növelni akarta az olasz haderő ütőképességét. Ennek érdekében a védelmi miniszter azt javasolta, hogy Olaszország alakítson ki gyors reagálású erőket és két új hadihajókötéléket. A javaslat tartalmazta továbbá egy új típusú védelmi modell kialakítását, aminek a keretein belül átalakították a felső katonai vezetést. Az átalakítás következtében innentől az olasz haderőt két tábornok irányította, egyikük operatív-technikai feladatokat látott el, míg a másik az adminisztrációban tevékenykedett. Ettől Rómában azt várták, hogy felszámolja a katonai vezetés megosztottságát, és integrálni fogja a szárazföldi, a haditengerészeti és a légierő nézeteit. Spadolini azt is kijelentette, hogy mivel a NATO-n belül az olasz katonai kiadások a legalacsonyabbak között vannak, ezért 1985-re 13%-kal többet kell fordítani a védelmi kiadásokra, szemben a szövetség által elvárt 3%-kal. A megemelt védelmi kiadások összefüggésben állhattak a Rogers-tervvel, amely szerint a cirkálórakéták és a Pershing telepítése mellett a NATO-nak a hagyományos fegyvereit is erősítenie kell. Az olasz védelmi miniszter ugyanakkor azért is akarhatott ilyen nagy mértékű emelést, mert az olasz nagytőke szerint a gazdasági nehézségekből a hadiipari termékek kivitelének fokozása jelentheti a kiutat, amihez újabb beruházások kellenek.⁹⁸

⁹³ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1984/117. Jelentés, Róma, 1984. május 7. 1-2. o.

⁹⁴ ÁBTL 3.2.3 Mt 867/16. 123. o. Feljegyzés, Budapest, 1984. július 20.

⁹⁵ ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'Situation of the Atlantic Alliance', 1984. május 29. 1-5. o.

⁹⁶ ÁBTL 3.2.3 Mt 867/16. 128. o. Információs jelentés, Budapest, 1984. július 6.

⁹⁷ ÁBTL 3.2.3 Mt 867/16. I. számú melléklet 51. o. Információs jelentés, Budapest, 1984. május 3.

⁹⁸ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1984/117. Jelentés, Róma, 1984. november 16. 1-5. o.

A hagyományos fegyverzet megerősítése miatt Rogers NATO főparancsnok javaslatot tett a védelmi kiadások 7%-os megemelésére, ami komoly problémákat okozott volna Olaszországnak, hiszen hiába a Spadolini által belengetett 13%, valójában Róma arra sem volt képes, hogy a NATO által elvárt 3%-ot tartani tudja. Közben egyre erőteljesebb lett az az amerikai tendencia, amiről egyébként Rogers is beszélt, hogy az Egyesült Államok a három nagy európai ipari országgal, nevezetesen Nagy-Britanniával, Franciaországgal és az NSZK-val fegyverkezési együttműködést alakítson ki. Az elképzelés sértette volna az olasz érdekeket, hiszen Olaszország kimaradt volna ebből az együttműködésből, ami különösen fájhatott az olasz kormányban. Ráadásul időközben született egy francia–német szerződés tankelhárító helikopterek megalkotásáról, aminek eredetileg olasz–német együttműködésben kellett volna megvalósulnia.⁹⁹

Ezek a lépések már egyértelműen abba az irányba mutattak, hogy az 1980-as évek elején felvetődött egy önálló európai integrált védelem létrehozásának a gondolata. Az amerikai érdekeket is megvalósító tervet Olaszország támogatta, és legfőbb szervezeteként a WEU jött szóba, hiszen a WEU képes lehetett volna arra, hogy az európai országokat koordinálja egy közös hadiipar és fegyverzet kialakításában, hogy önálló európai hangot fogalmazzon meg a szuperhatalmak felé, és ezzel kiegyensúlyozza az amerikai–európai kapcsolatokat. A tervet Andreotti kifejezetten támogatta, aki szerint mindenképpen szükséges az európai védelem megerősítése, hiszen az amerikai hadsereg egy jelentős része más területeken, például a Távol-Keleten van lekötve.¹⁰⁰ Olaszország amúgy is nagy jelentőséget tulajdonított a nyugat-európai szervezetnek, amely az azt megelőző 30 évben fontos funkciókat láthatott volna el, de potenciálja kiaknázatlan maradt. Róma azt várta a WEU-tól, hogy egyrészt ellensúlyozza az amerikai katonai jelenlét csökkentését a kontinensen, másrészt nagyobb gazdasági, kereskedelmi, politikai és stratégiai megjelenést biztosít Nyugat-Európának a kontinensen kívüli térségekben, elsősorban a Csendes-óceánon. Ennek megfelelően 1984. október 26-27-én az olasz fővárosban speciális ülést tartottak a Nyugat-európai Unió külügyminiszterei és védelmi miniszterei, amelyen politikai kiáltványt fogalmaztak meg, és elfogadták a szervezet operatív-szervezeti dokumentumát. Ennek értelmében a WEU célja Európa egységesítése, az Atlanti Szövetség erősítése, az egyensúlyi helyzet megteremtése az Egyesült Államok és Európa között, illetve a kelet-európai államokkal való párbeszéd fejlesztése. Emellett döntés született a technikai szervek, mint például a Fegyverzetellenőrzési Ügynökség (ACA) és a Fegyverzet Állandó Tanácsa (CPA) újrastrukturálásáról, reformjáról.¹⁰¹

⁹⁹ ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'European cooperation in the field of armaments', 1984. november 15. 6-7. o.

¹⁰⁰ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1984/116. Jelentés, Róma, 1984. november 22. 2-4. o.

¹⁰¹ ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'Ministerial session of the Atlantic Council (Bruxelles, 13th-14th December 1984). Security problems', 1984. december 13. 1-3. o.

Az SDI és az európai országok

Közben 1984. december 13-14-én Brüsszelben megrendezték az Atlanti Szövetség Miniszteri Szekciójának ülését. Az ülésen elhangzott, hogy a szövetségnek jelenleg két problémával kell szembenéznie. Az egyik a NATO hagyományos erőinek megerősítése és modernizálása – amire, mint láttuk, voltak már kísérletek –, valamint a politikai és katonai gondok az űrfegyverek kutatásában. Mivel azonban az európai országok nagy bizalommal vannak egymás és az Egyesült Államok felé, ezért a szövetség képes ezekre a problémákra koncentrálni, és megoldásukra adekvát válaszokat megfogalmazni. Ugyanakkor nem szabad megfeledkezni arról, hogy a szövetség államai politikai, katonai és gazdasági gondokkal küzdenek, ami jelentősen hátráltatja a védelmi kiadások 7%-os megemelését, illetve, hogy az űrfegyverkezés kérdésében eltérő álláspontot fogalmaz meg az Egyesült Államok és Franciaország.¹⁰²

Az űrfegyverkezés, vagyis az SDI,¹⁰³ illetve az ehhez való európai csatlakozás még jó ideig nyitott kérdés maradt. Egyrészt Európában tartottak az erre adandó szovjet reakcióktól, másrészt a program megkérdőjelezné a francia „force de frappe”¹⁰⁴ hihetőségét és az ország védelmének szuverenitását, hiszen a programmal Franciaország védelmének garantálása amerikai ellenőrzés alatt állna. Ezek miatt a kérdések miatt Franciaország úgy döntött, hogy távolmarad az SDI-től, és inkább a Heuréka-tervre koncentrál.¹⁰⁵ Mivel a többi NATO-tagállam még nem döntött a csatlakozásról, ezért 1985. április 22-23-án Bonnban összeült az Állandó Tanács, hogy közös választ, koordinált reakciót adjon az SDI-be szóló amerikai meghívásra. A jelen lévők úgy döntöttek, hogy abban az esetben csatlakoznak a kutatásokhoz, amennyiben megmarad a Szövetség stratégiai egysége, és a program nem annak érdekében valósul meg, hogy a NATO fölényt szerezzen a fegyverkezésben, hanem csak és kizárólag a katonai kapacitások kiegyensúlyozása lesz a cél. Néhány hónappal később, 1985. június 28-29-én az Európai Tanács milánói ülésén a jelenlévők kijelentették, hogy

¹⁰² ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'Ministerial session of the Atlantic Council (Bruxelles, 13th-14th December, 1984). Security problems', 1984. december 13. 1-9. o.

¹⁰³ A Stratégiai Védelmi Kezdeményezést (Strategic Defense Initiative-SDI) 1983 márciusában hirdette meg Reagan amerikai elnök, amelynek az volt a lényege, hogy egy bonyolult, főleg a lézertechnológiára alapuló védelmi pajzsot hoznak létre, amelynek egyes elemeit a világűrben helyeznék el. Lásd: MAGYARICS Tamás: *Az Amerikai Egyesült Államok története 1914-1991. (A rövid XX. század)*. Kossuth Kiadó, Budapest, 2008. 173-174. o.

¹⁰⁴ A „force de frappe” a francia nukleáris ütőerő, amelyet De Gaulle azért hozott létre, mert ellenezte azt a tervet, ami a brit-francia nukleáris erőt egyesítette volna az amerikai nukleáris erővel a NATO-parancsnoksága alatt (Multilateral Forces-MLF). A tábornok már 1965 januárjában kijelentette, hogy véget kell vetni a francia haderők integrációjának, és valamennyi külföldi katonát el kell távolítani Franciaországból. Lásd: SHENNAN, Andrew: *De Gaulle*. Akadémiai Kiadó, Budapest, 1997. 140-142. o.

¹⁰⁵ ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'European participation to the Strategic Defense Initiative. Political implications', 1985. január 1. 1-3. o.

a Heuréka nem kompatibilis az SDI-vel, vagyis egyértelműen letették voksukat az amerikai program mellett.¹⁰⁶

1983. március 4-7-én Craxi és Andreotti az Egyesült Államokban tartózkodott annak érdekében, hogy Olaszország Nagy-Britanniához, Franciaországhoz, illetve az NSZK-hoz hasonlóan fel tudjon zárkózni az amerikai űrfegyverkezési tervhez. Az egyeztetésen az olasz miniszterelnök leszögezte, hogy országa támogatja az amerikai programot, és az olasz kormány részét kell vennie a kutatásokban, ugyanakkor kihangsúlyozta, hogy az SDI nem vezethet az erőegyensúly megbomlásához és a fegyverkezési verseny felgyorsulásához. Válaszában Reagan elnök garanciát vállalt arra, hogy az űrterv nem változtatja meg az Egyesült Államok addigi békés és védelmi jellegű céljait. Az olasz politikusok megnyugtatóként azt hozta fel, hogy az űrfegyverkezés nem mond ellent az 1972-es megállapodásoknak,¹⁰⁷ hiszen azok a kutatást engedélyezik, csak a gyártáshoz és rendszerbe állításhoz kellene nemzetközi tárgyalások. Az egyeztetések végén az olasz küldöttség kijelentette, hogy örömmel csatlakozik az SDI-hez, de Olaszország csak részprogramokban vesz részt. A csatlakozás természetesen tovább erősítette a két ország viszonyát, amely az amerikai tőke beáramlása és a központi bankok közötti együttműködés miatt már amúgy sem volt gyenge. Ugyanakkor az olasz kormány ragaszkodott önállóbb diplomáciai tevékenységek folytatásához, ennek jeleként pedig elleneztek az Egyesült Államok esetleges nicaraguai beavatkozását.¹⁰⁸

Craxiék útja bizonyítja, hogy az olasz külpolitikai koncepció alapvetően nem változott az 1980-as években. Ez azt jelentette, hogy a cél továbbra is az önállóbb európai politika elérése, a Nagy-Britanniához, Franciaországhoz, és az NSZK-hoz való felzárkózás, és a NATO-hoz, illetve az Egyesült Államokhoz fűződő kapcsolatok erősítése volt. Ez utóbbinak részét képezte az olasz csatlakozás az amerikai űrállomás létesítésében, amelyet a tervek szerint 1990-re fejeznek be, miközben az 1980-as években egyre szélesedő kapcsolati kör alakult ki Washingtonnal, amely politikai, gazdasági, katonai és kulturális befolyást eredményezett. A két ország között ellentét legfeljebb csak akkor alakult ki, ha az Egyesült Államok stratégiai elképzelései ütköztek az olasz érdekekkel, de Róma még ebben az esetben sem tett önálló lépéseket. A NATO pedig továbbra is az olasz külpolitika és katonapolitika alaptétele volt, és Róma mindenképpen szeretett volna tevékenyen hozzájárulni a déli szárny megerősítéséhez, aminek jeleként az 1977-ben elfogadott 15 éves fegyverkezési programot aktívan hajtotta végre az ország.¹⁰⁹ Az Egyesült Államokhoz fűződő kapcsolatok bizonyítéka,

¹⁰⁶ ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'UEO -Coordination of the reactions of member countries to the US invitation to take part in the SDI (and attached: Interim Report of the SDI Working Group)', 1985. 9-12. o.

¹⁰⁷ A SALT I. (Strategic Arms Limitation Talks) szerződést 1972. május 26-án írták alá Moszkvában. A szerződés rögzítette a szárazföldről indítható ICBM (Intercontinental Ballistic Missiles) és a tengeralattjáróról indítható SLBM (Submarine Launched Ballistic Missiles) felső számát, ezen kívül tiltotta szárazföldi rakétaindító állomások építését, és szabályozta a támadórakéták korszerűsítésének módozatait. Lásd: HORVÁTH – PARÁGI – CSICSMANN 2013, 213.

¹⁰⁸ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1985/118. Jelentés, Róma, 1985. március 19. 1-5. o.

¹⁰⁹ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1984/116. Jelentés, Róma, 1985. január 16. 1-4. o.

hogy Libanonban Olaszország az amerikai nyomás ellenére sem volt hajlandó katonai akciókban szerepet vállalni, csak békemisszióban és közvetítésben vett részt, sőt, még vissza is vonta csapatait Libanonból. Igaz, ez utóbbit már amerikai engedéllyel tette.¹¹⁰

Olaszországnak a NATO-ban növekvő súlyát jelezte, hogy Lord Carrington, az új NATO-főtitkár első útja 1985 februárjában az olasz fővárosba vezetett, ahol találkozott a miniszterelnökkel, a külügyminiszterrel és a védelmi miniszterrel, hogy meghallgassa az olasz álláspontot a nemzetközi eseményekről. Az egyeztetéseken megállapodtak abban, hogy az eurorakéták telepítése után bekövetkezhet a közös védelem adekvát elosztása, ugyanakkor az európai országoknak nagyobb és aktívabb részvételt kell vállalniuk az amerikai kezdeményezésekben, főleg a technológiafejlesztésben, és a védelmi rendszer megerősítésében. Ez utóbbi kapcsán leszögezték, hogy a NATO a jövőben is 3%-os növekedést vár el a tagállamoktól a védelmi kiadásokban. Ettől Olaszország, ha minimálisan is, de elmaradt a maga átlagos 2,8%-ával. A védelmi rendszer megerősítésére többek között azért volt szükség, mert az Egyesült Államokban Nunn javaslatot tett 80 ezer amerikai katona Európából történő kivonására a 330 ezerből.

Az olasz fővárosban tett látogatása során a NATO-főtitkár kihangsúlyozta, hogy bár az európai országoknak korlátozott gazdasági lehetőségek állnak rendelkezésükre, mégis megmutatták akarukat a közös védelem megerősítésére, és ebből a szempontból Olaszország szintén bizonyított, amikor vállalta a katonai jelenlétet a Szinai-félszigeten, a Vörös-tenger térségében és Libanonban, amivel egyaránt hozzájárult a nemzeti és nyugati érdekek védelméhez. A védelmi miniszterek előző év decemberében megtartott ülésén felhatalmazták a főtitkárt arra, hogy kidolgozza a NATO védelmi formuláit, ami magába foglalta a prioritásokat, a nemzeti politikák koordinálását, a szövetséges tervezést és az erőforrások hatékonyabb elosztását. A felhatalmazással a zsebében Lord Carrington tervbe vette az infrastrukturális műveletek kiegészítését és a hagyományos erők modernizálását. Craxiék mindkettőben nagyobb olasz részvételt ígértek, és biztosították a főtitkárt arról, hogy a kívánalmakat már elkezdték megvalósítani, és a szövetséges elvárásokat beépítik a nemzeti katonai programba, fegyvergyártásba is.¹¹¹

Nem sokkal később Spadolini Weinbergerrel találkozott, hogy két témáról, nevezetesen az SDI-ről és az olasz–amerikai fegyverzetcseréről egyeztessenek. Az első kapcsán Spadolini leginkább afelől érdeklődött, hogy az olasz ipar miben tud az Egyesült Államok segítségére lenni, amerikai kollégája pedig ígéretet tett arra, hogy felülvizsgálja a védelmi termékek cseréjét, hiszen az Egyesült Államoknak szüksége volt az olasz szállítmányokra, főleg az Európában állomásozó amerikai csapatok miatt.¹¹²

¹¹⁰ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1985/118. Jelentés, Budapest, 1985. január 16. Melléklet 2-3. o.

¹¹¹ ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'Visit of NATO's Secretary General, Lord Carrington (Rome, 11th February 1985)', 1985. január 25. 1-7. o.

¹¹² ASILS AGA NATO series Letter by Permanent Representative to NATO Sergio Romano to the Secretary General of the Ministry of Foreign Affairs Ruggiero, 1985.május 23. 1-2. o.

Ezzel nagyjából egyidőben az amerikai olasz nagykövet a Pentagonban egyeztetett Abrahamson tábornokkal, az SDI szervezet vezetőjével, amelyen az amerikai tábornok leszögezte, hogy az SDI végcélja az elrettentés és a stabilitás, amely egyelőre még a támadó fegyvereken nyugszik, ezzel szemben azonban az SDI egy védelmi komponens.¹¹³ Még ez év augusztusában Abrahamson hivatalosan is meghívta Rómát az amerikai technológiai misszióba, amelynek értelmében olasz vállalatok és kutatóközpontok vehettek részt a kisebb kutatási tervek kidolgozásában, ugyanakkor az amerikai tábornok nem zárta ki annak a lehetőségét sem, hogy az olasz kormány a későbbiekben megkapja a rendszer megépítéséről készült tanulmányokat. Az ígéretek ellenére azonban az olasz kormány egyelőre még nem nyilvánított véleményt a csatlakozásról.¹¹⁴

Olaszországban ugyanis vita folyt arról, hogy SDI-hez, vagy a francia Heurékához csatlakozzanak. Míg az SDI-t egyértelműen katonai célokra tervezték, addig a Heuréka polgári célokat szolgálta, ráadásul nem amerikai, hanem európai kézben lenne, ami az olasz kormány számára vonzóbbá tette. Ugyanakkor az SDI egy már létező valóság volt a maga 1200 oldalas kutatási tervével és az amerikai kormány által garantált 26 milliárd dolláros anyagi alapjával, míg a Heuréka csak egy elképzelés volt, amelyben 12 kormány vett volna részt, ami rendkívül bizonytalanná tette a programot. Bár Olaszország mind az SDI-ben, mind a Heurékában közreműködött, de 1984 júniusában a külügyminiszter, a honvédelmi miniszter és az iparügyi miniszter jelenlétével megrendezett minisztériumközi bizottsági ülésen arról döntöttek, hogy megkezdik a gyártás koordinálását az Egyesült Államokkal, ami egyértelmű utalás volt arra, hogy Rómához közelebb áll az amerikai terv. Ráadásul hónapokkal korábban Weinberger írásos felajánlást tett az SDI-ben való részvételre, amivel kapcsolatban ugyan állami döntés még nem született, de az olasz magánipar gyártáskapacitásának jelentős részét ezzel Washington már lekötötte, és ellátta megrendelésekkel. Ezeknek köszönhetően Spadolini kijelentette, hogy Olaszország a tervek szerint csatlakozik az SDI megvalósításához, és bekapcsolja az állami ipart is a kutatási programba. Ennek következtében 1985. szeptember 4-én egy amerikai küldöttség járt Rómában, hogy az olasz ipar képviselőivel tárgyaljon a műszaki kérdésekről, majd ezt követően októberben olasz gyáriparosok látogattak az Egyesült Államokba, hogy egyeztessék a részleteket. A tárgyalásoknak köszönhetően 1985 folyamán több olasz vállalat is csatlakozott az SDI-hez, mint például az Agusta, az Oto Melara, az Aeritalia, a Selenia, az Italtel, vagy a magáncégek közül a FIAT. Ezek a vállalatok elsősorban a lézerkutatásban, az infravörös érzékelők fejlesztéséhez, számítógépek, laborberendezések és műholdalkatrészek modernizációjához járultak hozzá. Közben pedig az olasz kormány rendszeresen hangsúlyozta, hogy Olaszország csak a kutatásokban vesz részt.¹¹⁵

¹¹³ ASILS AGA NATO series Report by Ambassador Pettrignani to the Minister of Foreign Affairs Andreotti, 1985. május 24. 1-8. o.

¹¹⁴ ASILS AGA NATO series Memorandum by the Ministry of Foreign Affairs to Minister Andreotti, 'Meeting at the Ministry of Defense with General Abrahamson', 1985. augusztus 27. 1. o.

¹¹⁵ MNL OL XIX-J-1-j Olaszország KÜM TÜK 1985/120. Jelentés, Róma, 1985. szeptember 27. 1-11. o.

Befejezés

A feszült nemzetközi helyzet arra ösztönözte az Egyesült Államokat és a NATO-t, hogy megerősítse pozícióit a Földközi-tenger térségében. Mivel az itt található országok közül mind belpolitikailag, mind Washingtonhoz és Brüsszelhez való hűség szempontjából Olaszország volt a legstabilabb, ezért az országnak egyfajta „fellegvár” szerepet szántak. Ezt a helyzetet Róma jól használta ki arra, hogy egyre meghatározóbb helyzetbe kerüljön, és felemelkedjen az európai nagyhatalmak sorába. Ennek érdekében nem csak az elsők között vállalta a Pershing II-k és a cirkálórakéták telepítését és csatlakozott az SDI programjához, hanem hosszú tervezést és előkészítést követően belekezdett hadseregének fejlesztésébe is.

A haderőfejlesztés elsősorban az olasz légierőt érintette. Róma első lépésként továbbfejlesztette az F104 Starfighter típusú vadászpülőt. Az eredetileg az 1950-es években a Lockheed által kifejlesztett vadászgépből az Egyesült Államokon kívül 14 ország vásárolt, köztük Kanada, Japán, Hollandia, Németország és Olaszország, és az évtizedek során számos változata készült el. Ezek közül a korszakban az egyik legfejlettebb az Európában rendszeresített F104G volt. Ezt a típust az 1970-es évek végén, az 1980-as évek elején a FIAT korszerűsítette, így született meg az F104S, amely új, nagyobb teljesítményű hajtóművet kapott, sikerült jobb repülési stabilitást elérni, és alkalmas lett Sparrow rakéták kilövésére. Ennek egy még továbbfejlesztett változata lett az 1984 decemberében megszületett F104S/ASA (Aggiornamento Sistema d'Arma), amely az előző verzióknak a fegyverrendszerét modernizálta.¹¹⁶

Az olasz légierő azonban nem csak az F104 Starfighterek módosításait hajtotta végre. Az 1960-as évek végén, az 1970-es évek elején megszületett az MRCA (Multi Role Combat Aircraft) egyezmény, amelynek célja egy új, modernebb vadászgép kifejlesztése volt. A program három ország, Nagy-Britannia, az NSZK és Olaszország összefogásával született meg. Ez a három ország megalapította a brit székhelyű Trinational Tornado Training Establishmentet (TTTE), és az 1970-es években belekezdett a Tornado rülőgépek prototípusainak gyártásába és tesztelésébe.¹¹⁷ Végül az 1980-as években elkészült a vadászpülő, amelyből összesen 644-et gyártottak, ebből Olaszország 100 darabot kapott, az első 1982. augusztus 27-én landolt a Ghedi katonai repülőtéren. Ennek köszönhetően az Aeronautica Militare (AM) támadó ereje jelentősebb javult, ami az F104 Starfighterekkel már nem volt lehetséges.¹¹⁸ A Tornado sikerét jelzi, hogy az 1990-es években többek között Irakban, és Jugoszláviában, majd a 2000-es esztendőkből Afganisztánban is bevetésre kerültek, miközben polgári védelmi akciókban is alkalmazták a vadászgépeket.¹¹⁹

¹¹⁶ Sz.n.: F104 Starfighter, International F-104 Society. é.n.

¹¹⁷ NICOLI, Riccardo: Il Tornado in Aeronautica Militare. *Rivista Aeronautica*, 2022/4. 18-23. o.

¹¹⁸ COSCI, Stefano: La storia del programma MRCA/Tornado. *Rivista Aeronautica*, 2022/4. 12-17. o.

¹¹⁹ NACCA, Francesco: 40 anniversario del velivolo „Tornado”. Ministero Della Difesa, Aeronautica Militare é.n.

Olaszország nem csak légierejét, hanem hadiflottáját is modernizálta. Ennek ékes példája a Garibaldi repülőgép-hordozó cirkálóhajó, amely 1985-ös hadrendbe állításától egészen 2012-ig az olasz haditengerészet zászlóshajója volt. A Garibaldi a hagyományos repülőgép-hordozó külső vonalaival rendelkezett, de légvédelmi, hajó-és tengeralattjáró-elhárító tengeri egységként is bevethető volt, illetve parancsnoki, koordinációs és irányítóközponti feladatokat is ellátott. A hadihajót a legmodernebb elektronikus rendszerekkel szerelték fel, amelyek minden cselekvési területet lefednek, legyen szó légi és tengeri megfigyelőrendszerekről, víz alatti környezetről, elektronikus hadviselési műveletekről vagy kommunikációról.¹²⁰

A haderőfejlesztés mellett Olaszország szövetségen belüli súlyát és szerepét növelte, hogy kihasználva földrajzi helyzetét, hidat képezett Afrika és a Közel-Kelet irányába, és részt vett a libanoni békemisszióban. Ez utóbbi azért is volt kiemelkedő, mert a második világháború óta Olaszország először vett részt olyan akcióban, amely saját területén kívülre esett. Mindeközben nem szabad megfeledkeznünk a NATO főtitkárainak, Luns-nak és Carringtonnak a látogatásairól, Brown ex-védelmi miniszter és az amerikai elnökök kijelentéseiről, és arról sem, hogy mind az Egyesült Államok, mind az NSZK fejlesztette és megerősítette olaszországi támaszpontjait. Ezek alapján kijelenthető, hogy az 1980-as évekre Olaszország valóban a NATO „déli fellegvéra” lett.

Felhasznált irodalom:

ANDERLE Ádám: Latin-Amerika története. Pannonica Kiadó, 1998.

ANDREIDES Gábor: *Egy megbízható elvtárs. Száll József útja az MKP-től a P2-ig.* NEB Könyvtár, Budapest, 2019.

Archivio Storico Istituto Luigi Sturzo Archivio Giulio Andreotti (ASILS AGA) NATO series Memorandum by Minister of Defense ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'The autumn sessions of NATO Ministers of Defense meetings (Eurogroup: 4th December; DPC 5th-6th December 1978)', 1978. december 14. Elérhető: <https://digitalarchive.wilsoncenter.org/document/memorandum-ministry-foreign-affairs-autumn-sessions-nato-ministers-defense-meetings> (Letöltés ideje: 2024. 04. 04.)

ASILS AGA NATO series Letter by Permanent Representative to NATO Sergio Romano to the Secretary General of the Ministry of Foreign Affairs Ruggiero, 1985.május 23. Elérhető: <https://digitalarchive.wilsoncenter.org/document/letter-permanent-representative-nato-sergio-romano-secretary-general-ministry-foreign> (Letöltés ideje: 2024. 04. 04.)

ASILS AGA NATO series Memorandum by Ministry for Foreign Affairs, 'The 1978 Ministerial Atlantic Council', 1978. december 18. 1-4. o. Elérhető: <https://digitalarchive.wilsoncenter.org/document/memorandum-ministry-foreign-affairs-1978-ministerial-atlantic-council> (Letöltés ideje: 2024. 04. 04.)

¹²⁰ Sz.n.: Portaeromobili (LHA). Classe Garibaldi. Ministero Della Difesa, Marina Militare, é.n.

ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'UEO -Updated positions of the Seven about the relaunch of the Organization-Preparatory works of the Ministerial Council in June', 1984. május 26. Elérhető:

<https://digitalarchive.wilsoncenter.org/document/memorandum-ministry-foreign-affairs-ueo-updated-positions-seven-about-relaunch> (Letöltés ideje: 2024. 04. 04.)

ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'Situation of the Atlantic Alliance', 1984. május 29. Elérhető:

<https://digitalarchive.wilsoncenter.org/document/memorandum-ministry-foreign-affairs-situation-atlantic-alliance> (Letöltés ideje: 2024. 04. 04.)

ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'European cooperation in the field of armaments', 1984. november 15. Elérhető:

<https://digitalarchive.wilsoncenter.org/document/memorandum-ministry-foreign-affairs-european-cooperation-field-armaments> (Letöltés ideje: 2024. 04. 04.)

ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'Ministerial session of the Atlantic Council (Bruxelles, 13th-14th December, 1984). Security problems', 1984. december 13. Elérhető:

<https://digitalarchive.wilsoncenter.org/document/memorandum-ministry-foreign-affairs-ministerial-session-atlantic-council-bruxelles-13th> (Letöltés ideje: 2024. 04. 04.)

ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'Ministerial session of the Atlantic Council (Bruxelles, 13th-14th December, 1984). Security problems', 1984. december 13.

Elérhető: <https://digitalarchive.wilsoncenter.org/document/memorandum-ministry-foreign-affairs-ministerial-session-atlantic-council-bruxelles-13th> (Letöltés ideje: 2024. 04. 04.)

ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'European participation to the Strategic Defense Initiative. Political implications', 1985. január 1. Elérhető:

<https://digitalarchive.wilsoncenter.org/document/memorandum-ministry-foreign-affairs-european-participation-strategic-defense-initiative> (Letöltés ideje: 2024. 04. 04.)

ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'UEO - Coordination of the reactions of member countries to the US invitation to take part in the SDI (and attached: Interim Report of the SDI Working Group)', 1985. Elérhető:

<https://digitalarchive.wilsoncenter.org/document/memorandum-ministry-foreign-affairs-ueo-coordination-reactions-member-countries-us> (Letöltés ideje: 2024. 04. 04.)

ASILS AGA NATO series Memorandum by Ministry of Foreign Affairs, 'Visit of NATO's Secretary General, Lord Carrington (Rome, 11th February 1985)', 1985. január 25. Elérhető:

<https://digitalarchive.wilsoncenter.org/document/memorandum-ministry-foreign-affairs-visit-natos-secretary-general-lord-carrington-rome> (Letöltés ideje: 2024. 04. 04.)

ASILS AGA NATO series Memorandum by the Ministry of Foreign Affairs to Minister Andreotti, 'Meeting at the Ministry of Defense with General Abrahamson', 1985. augusztus 27. Elérhető:

<https://digitalarchive.wilsoncenter.org/document/memorandum-ministry-foreign-affairs-minister-andreotti-meeting-ministry-defense-general> (Letöltés ideje: 2024. 04. 04.)

ASILS AGA NATO series Report by Ambassador Petrignani to the Minister of Foreign Affairs Andreotti, 1985. május 24. Elérhető:

<https://digitalarchive.wilsoncenter.org/document/report-ambassador-petrignani-minister-foreign-affairs-andreotti-0> (Letöltés ideje: 2024. 04. 04.)

ASILS AGA NATO series Report by Permanent Representative to NATO Torretta to Minister of Foreign Affairs Colombo, 'Perspectives about Atlantic defense for the 1980s', 1983. február 15. Elérhető:

<https://digitalarchive.wilsoncenter.org/document/report-permanent-representative-nato-torretta-minister-foreign-affairs-colombo-perspectives> (Letöltés ideje: 2024. 04. 04.)

ASILS AGA NATO series Telegram by the Ambassador to the United States Petrignani to Ministry of Foreign Affairs, 'Prospects of resuming the FNI negotiations', 1984. március 1. Elérhető: <https://digitalarchive.wilsoncenter.org/document/telegram-ambassador-united-states-petrignani-ministry-foreign-affairs-prospects-resuming> (Letöltés ideje: 2024. 04. 04.)

Attilio Ruffini for the Prime Minister Andreotti, 'Washington Summit -NATO's program for long-term defense (LTDP)' 1978. május. 30. Elérhető:

<https://digitalarchive.wilsoncenter.org/document/memorandum-minister-defense-attilio-ruffini-prime-minister-andreotti-washington-summit> (Letöltés ideje: 2024. 04. 04.)

BOTTONI, Stefano: „Mozart” és „Fekete”. Egy hírszerzési dosszié különös története I. rész. *Betekintő*, 2014/4.

BURAKOWSKI, Adam – GUBRYNOWICZ, Aleksander – UKIELSKI, Pawel: 1989. *A kommunista diktatúra végnapjai Közép-és Kelet-Európában*. Rézbong Kiadó, Budapest, 2014.

CHIARINI, Roberto: A Movimento Sociale Italiano-történeti áttekintés. In: FEITL István (szerk.): *Jobboldali radikalizmusok tegnap és ma*. Napvilág Kiadó, Budapest, 1998.

COSCI, Stefano: La storia del programma MRCA/Tornado. *Rivista Aeronautica*, 2022/4. 12-17. o. Elérhető: <https://www.calameo.com/read/00710489831aeb32ec9cb> (Letöltés ideje: 2024. 03. 05.)

DR. TÁLAS Péter (szerk.): *NATO kézikönyv*. HM Stratégiai Védelmi Kutató Hivatal, Budapest, 2001.

GHEBALI, Victor-Yves: Az EBEÉ fejlődése Helsinkitől Párizsig (1975-1990.) In: DUNAY Pál – GAZDAG Ferenc (szerk.): *A helsinki folyamat: az első húsz év. Tanulmányok és dokumentumok*. Zrínyi Kiadó, Budapest, 1995.

HORVÁTH Jenő – PARAGI Beáta – CSICSIMANN László: *Nemzetközi kapcsolatok története 1941-1991*. Antall József Tudásközpont, Budapest, 2014.

- KERESZTY András: *Tények könyve: NATO*. Greger-Delacroix, Budapest, 1997.
- LÁNG Péter: Egy szervezet négy évtizede. A WEU rövid története (1954-1993). In: DUNAY Pál – GAZDAG Ferenc (szerk.): *Nyugat-Európai Unió. A megalakulástól a megvalósulásig*. SVKI, Budapest, 1994.
- MAGYARICS Tamás: *Az Amerikai Egyesült Államok története 1914-1991. (A rövid XX. század)*. Kossuth Kiadó, Budapest, 2008.
- MAGYARICS Tamás: *Az Egyesült Államok külpolitikájának története. Mítosz és valóság: érdekek és értékek*. Antall József Tudásközpont, Budapest, 2014.
- MAMMARELLA, Giuseppe – CACACE, Paolo: *La politica estera dell'Italia. Dallo stato unitario ai gorni nostri*. Editori Laterza, Róma, 2010.
- MAMMARELLA, Giuseppe: *L'Italia contemporanea (1943-2011)*. Società editrice il Mulino, Bologna, 2012.
- MINOLFI, Salvatore: Italia, Europa e Stati Uniti: La NATO dal 1969 al 1989. In MINOLFI, Salvatore (szerk): *L'Italia e la NATO. Una politica estera nelle maglie dell'alleanza*. CUEN, Nápoly, 1993.
- NACCA, Francesco: 40 anniversario del velivolo „Tornado”. é.n. Elérhető: <https://www.aeronautica.difesa.it/2022/09/08/40-anniversario-del-velivolo-tornado/> (Letöltés ideje: 2024. 04. 08.)
- NEUSPILLER Ferenc: A római rezidentúra malacperselye. Miért támogattott a magyar hírszerzés egy olasz disznóhizlaldát? *Betekintő*, 2019/1.
- NICOLI, Riccardo: Il Tornado in Aeronautica Militare. *Rivista Aeronautica*, 2022/4. Elérhető: <https://www.calameo.com/read/00710489831aeb32ec9cb> (Letöltés ideje: 2024. 03. 05.)
- PÁL István: A madridi rezidentúra – A magyar hírszerzés Spanyolországban a detente csúcspontjától a kishidegháború végéig 1976-1984. *Nemzet és Biztonság*, 2020/3.
- PÓK Attila: A nemzetközi élet krónikája 1945-1997. *História*, Budapest, 1998.
- ROMANO, Sergio: *Guida alla politica estera italiana. Da Badoglio ai nostri giorni*. BUR Rizzoli, Milánó, 2019.
- SHENNAN, Andrew: *De Gaulle*. Akadémiai Kiadó, Budapest, 1997.
- SILVESTRI, Stefano: Il dibattito sulla non-proliferazione nucleare. In: MERLINI, Cesare (szerk): *La politica estera dell'Italia. Cinquant'anni dell'Istituto Affari Internazionali*. Società editrice il Mulino, Bologna, 2016.
- SOARDI, Mario: *Manuale di polizia municipale*. Casa Editrice F. Apollonio&C, Brescia, 1962.
- STEPHEN, Michael: *The Cyprus question. A concise to the history, politics, and law of the Cyprus Question*. Meto Print, London, 2001.
- Sz.n.: Allied Naval Forces Souther Europe (NAVSOUTH). GlobalSecurity.org, é.n. Elérhető: <https://www.globalsecurity.org/military/agency/navy/navsouth.htm> (Letöltés ideje: 2024. 04.04.)

Sz.n.: F104 Starfighter, International F-104 Society. é.n.
Elérhető: <https://www.i-f-s.nl/f-104-types/> (Letöltés ideje: 2024. 03. 05.)

Sz.n.: Portaeromobili (LHA). Classe Garibaldi. é.n. Elérhető:
<https://www.marina.difesa.it/noi-siamo-la-marina/mezzi/forze-navali/Pagine/Garibaldi.aspx> (Letöltés ideje: 2024. 04. 08.)

Sz.n.: Reparti mobili. Polizia di Stato – olasz nemzeti rendőrség hivatalos honlapja, é.n.
Elérhető: <https://www.poliziadistato.it/articolo/i-reparti-mobili> (Letöltés ideje: 2024. 04. 04.)

TRANFAGLIA, Nicola: *Anatomia dell'Italia repubblicana 1943-2009*. Passigli Editori, Firenze, 2010.

VARGA Csaba Béla: *Afganisztán a legyőzhetetlen*. Kelet Kiadó Kft., Budapest, 2010. 190-198. o.

GRIFFITHS DÁNIEL¹

A KOGNITÍV SZÁMÍTÁSTECHNIKA-ALAPÚ AUTOMATIZÁCIÓ SZÜKSÉGESSÉGE A BIZTONSÁGI MŰVELETI KÖZPONTOKBAN

A biztonsági műveleti központok kulcsfontosságú elemei a szervezetek védelmi stratégiáinak, ugyanakkor számos operatív kihívással szembesülnek. Az ezen környezetekben alkalmazott hagyományos automatizálási megközelítések ugyan enyhítettek bizonyos hatékonysági hiányosságokon, de továbbra is korlátozott hatáskörűek. A kognitív számítástechnika ígéretes lehetőségeket kínál a SOC-ok működésének hatékonyabbá tételére, különösen a riasztások kivizsgálásának automatizálása terén. A technikai fejlesztések ellenére továbbra is fennállnak kihívások, például a gépi tanulási modellek elleni támadások, a klasszifikációk időbeli romlása és a számítási komplexitás. Az átláthatatlan rendszerek az elemzők bizalmát is csökkentik, amely szükségessé teszi a megmagyarázható mesterségesintelligencia-megközelítések alkalmazását. A hatékonyabb működés érdekében kulcsfontosságú a szabványos keretrendszerek kialakítása, a minőségi adatkészletek gyűjtése, illetve a tudományos kutatások és piaci fejlesztések közötti szorosabb együttműködés.

Kulcsszavak: kiberbiztonság, biztonsági műveleti központ, mesterséges intelligencia, gépi tanulás, kognitív számítástechnika

THE NEED FOR AUTOMATION THROUGH COGNITIVE COMPUTING IN SECURITY OPERATIONS CENTRES

Security Operations Centres (SOCs) are key elements of organisations' defence strategies; however, they also face a number of operational challenges. While traditional automation approaches have mitigated some inefficiencies, these approaches remain limited in scope. Cognitive computing offers promising opportunities to improve the operational efficiency of SOC, particularly in the area of automating the investigation of alerts. Despite technical advances, many challenges remain, such as adversarial machine learning, concept drift and computational complexity. Opaque cognitive computing systems also reduce the confidence of analysts, which necessitates the use of explainable artificial intelligence approaches. The development of standardised frameworks, the collection of high-quality datasets and closer collaboration between academic and industrial research are key to further efficiency gains.

Keywords: cyber security, security operations centre, artificial intelligence, machine learning, cognitive computing

¹ ORCID-azonosító: 0009-0005-6206-7598

Háttér

A SOC² egy olyan létesítmény, amely a kiberbiztonsági támadások észleléséért, elemzéséért és az azokra való reagálásért felelős. Tekintettel arra, hogy a SOC-ok folyamatos megfigyelést biztosítanak, ezért alapvető fontosságú az emberi erőforrások hatékony felhasználása. A szervezetek különböző módon strukturálják a SOC-csapatukat. Egyesek többszintű modellt alkalmaznak, míg mások a laposabb struktúrát részesítik előnyben.³ Ez a változatosság az operatív igények, az erőforrások rendelkezésre állása és a stratégiai prioritások közötti különbségekből adódik. Ugyan az elterjedt keretrendszerek jellemzően elkerülik az explicit struktúrák előírását, a többszintű modell továbbra is az uralkodó megközelítés maradt. Ezt a vezető kiberbiztonsági szervezetek,⁴ kutatók⁵ és szakértők⁶ egyaránt jól dokumentálják.

A többszintű struktúrák jellemzően három vagy négy fokozatot alkalmaznak.⁷ Az első szintű elemzők intézik a riasztások kezdeti osztályozását, miszerint előre meghatározott forgatókönyvek alapján határozzák meg, hogy a riasztások tévesek-e, vagy további vizsgálatot igényelnek. Ezek az elemzők nem határozzák meg az incidensek kiváltó okait, és nem kommunikálnak az érintett felekkel. Az elsődleges szerepük az észlelőrendszerek által generált zaj kiszűrése, hogy csak a releváns riasztások kerüljenek továbbításra a magasabb beosztású elemzők számára. Ennek következményeképp, ezek az elemzők kezelik a legtöbb riasztást, miközben jellemzően nem rendelkeznek mélyreható műszaki ismeretekkel. A második szintű elemzők jelentősebb szakértelemmel rendelkeznek, ezért ők veszik át az incidensgyanús riasztások kivizsgálását. Jellemzően szintén a feladatkörükbe tartozik a riasztásokat kiváltó okok elemzése és a támadásra utaló viselkedések megállítása. A harmadik szintű elemzők a proaktív fenyegetésvadászatra, a fejlett fenyegetések feltárására és a második szintű elemzők számára túl bonyolultnak bizonyult vizsgálatok elvégzésére összpontosítanak. Hozzájuk tartozik az észlelési képességek naprakészen tartása és stratégiák kidolgozása a védelmi rendszerek további fokozására. A negyedik, ritkán emlegetett szint, a SOC-vezetőség. Ezek a menedzserek felügyelik a csapat működését, meghatározzák a csapat prioritásait és optimalizálják az erőforrások kihasználását. Továbbá ők biztosítják a szervezet biztonsági céljaihoz való igazodást, valamint stratégiai felügyeletet biztosítanak a kritikus események során.

² SOC – Security Operations Center – biztonsági műveleti központ

³ KNERLER Kathryn et al.: *11 Strategies of a World-Class Cybersecurity Operations Center*. The MITRE Corporation, Bedford, 2022. 65-67. o.

Sz.n.: How to Become a SOC Analyst. SANS, 2024. 07. 16.; PAWAR Shekar: Role Of Authentication, Role Management & Access Control as Integral Part Of SOC Capabilities. EC-Council, 2023. 08. 16.

⁵ BERZSENYI Dániel et al.: *Incidensmenedzsment*. Dialóg Campus Kiadó, Budapest, 2017. 119-120. o.; VIELBERTH Manfred et al.: *Security Operations Center: A Systematic Study and Open Challenges*. IEEE Access, 2020/8. 18. o.

⁶ BASTA Alfred et al.: *Open-Source Security Operations Center (SOC): A Complete Guide to Establishing, Managing, and Maintaining a Modern SOC*. John Wiley & Sons, New Jersey, 2024. 46. o.

⁷ Uo.

A SOC szerepe a szervezetek fejlődő fenyegetésekkel szembeni védelmében kulcsfontosságú, azonban számos tartós és néhány újonnan megjelenő kihívásokkal kell szembenézniük. Míg a SOC-ok számos eszközre támaszkodnak a rosszindulatú tevékenységek észlelésére, ezek az észlelési források gyakran nem elég felhasználóbarátak és emellett jelentős zajt produkálnak. A felügyelt rendszerek köre folyamatosan növekszik, ahogy a szervezetek egyre összetettebb infrastruktúrákat vezetnek be, ami további terhelést jelent az elemzők helyzetismeretére.⁸ Ezeket a kihívásokat a munkaerőbeli hiányosságok is tetézik, mivel a 24 órás felügyelet erőforrás-igényes, és folyamatos hiány van magasan képzett kiberbiztonsági szakemberekből. Noha egyes kihívások régóta fennállnak, sok SOC közeledik a hagyományos megoldások által nyújtott optimalizálás határaihoz. Viszont a mesterséges intelligencia és a gépi tanulás fejlődése olyan kifinomult automatizálásokat tesz lehetővé, amelyek képesek segíteni a fenyegetések észlelésében és kivizsgálásában. Bár ezek az AI-⁹ és ML-alapú¹⁰ rendszerek nagy potenciállal bírnak, új kihívásokat is hoznak magukkal, amelyek csak bonyolultabb és kevésbé átlátható problémákkal helyettesítik a meglévő kihívásokat.

Ez a szakirodalmi áttekintés a SOC-okkal kapcsolatos kihívásokat és lehetőségeket tárja fel a modern kiberbiztonság kontextusában. Az alapvető problémák elemzésével kezdődik, beleértve a működési és technológiai limitációkat. Az áttekintés ezután az automatizálást vizsgálja, a hagyományos módszerekre, valamint a mesterséges intelligencia és a gépi tanulás növekvő használatára összpontosítva, miközben feltárja e technológiák kockázatait és összetettségeit. Végül mérlegeli a jövőbeli kutatási irányokat, trendeket és innovatív megközelítéseket azonosít a fenntarthatóbb SOC-gyakorlatokhoz. A „kognitív számítástechnika” kifejezés gyűjtőfogalomként használt e szakirodalmi áttekintésben, amely magába foglalja az emberi intelligencia reprodukálására irányuló technológiákat, mint például a mesterséges intelligenciát és annak közismert részhalmozát, a gépi tanulást.

Hatékonyság a Biztonsági Műveleti Központokban

A kognitív számítástechnika használhatóságának elemzéséhez először fel kell tárni, hogy ezek a technológiák milyen hatékonysági problémák megoldására törekednek. A SOC-okat érintő kihívások sokrétűek, és jelentős hatással vannak a kiberbiztonsági fenyegetések mérséklésének hatékonyságára. A SOC-ok hiányosságaival kapcsolatos szakirodalom átfogó vizsgálata öt kulcsfontosságú, egymással szorosan összefüggő területet azonosított.

⁸ VIELBERTH 2020, 16.

⁹ AI – Artificial Intelligence – mesterséges intelligencia

¹⁰ ML – Machine Learning – gépi tanulás

Az Alert Fatigue¹¹

A SOC-ok alkalmazottjait egyre jobban megterheli a különféle eszközök által generált biztonsági riasztások elsöprő mennyisége. Egy SOC naponta akár több ezer riasztással is szembesülhet, amelyek jelentős része üzemszerű eseményekből ered, és nem utal valódi rosszindulatú tevékenységre.¹² Az észlelések beáramlása egy „alert fatigue”-ként ismert jelenséghez vezethet, ami egy olyan állapot, amelyben az elemzők érzéketlenné válnak a riasztások iránt, és kevesebb odafigyeléssel kezdik kivizsgálni őket. Ez növeli annak valószínűségét, hogy figyelmen kívül hagyják a valódi fenyegetéseket.¹³ A riasztások manuális kivizsgálása ismétlődő és időigényes feladat lehet, ami súlyosbítja ezt a problémát és további megterhelést jelent a már amúgy is korlátozott erőforrásokkal működő SOC-csapatokra. Ez különösen igaz az első szintű elemzőkre, akik gyakran csak most kezdték pályafutásukat a kibertudomány terén, és ezért tapasztalatlanok. Ennek következtében csökken a fenyegetésészlelés és a válaszadás hatékonysága, ami növeli a sikeres kibertámadások kockázatát.¹⁴

Iparági kutatások is alátámasztják az „alert fatigue” negatív hatásait. Egy 2020-as tanulmány például megállapította, hogy a SOC csapatok által kezelt riasztások közel egyharmada téves, és a riasztások 28%-át teljesen figyelmen kívül hagyják, mivel az elemzők így is nehezen tudnak megbirkózni a napi feladataikkal.¹⁵ Egy újabb, 2023-as tanulmány eredményei is megerősítik ezt a jelenséget, ami arra következtet, hogy nincs jelentős javulási tendencia.¹⁶ A tanulmány szerint az elemzők által megvizsgált riasztások 63%-a alacsony prioritású vagy hamis pozitív besorolású, és az incidensek csak 49%-át vizsgálják felül egy átlagos munkanapon, így jelentős elmaradás marad a megoldatlan riasztásokból.¹⁷

A riasztások vizsgálatának monoton és nagy volumenű természete gyakran vezet unalomhoz, kiegészítéshez és az elemzők teljesítményének csökkenéséhez. A SOC-környezetek a természetükből eredően nagy nyomásúak és nagy tétellel bírnak, mivel a helytelen döntések súlyos következményekkel járhatnak.¹⁸ A riasztások özönével szembesülő elemzők kognitív képességei csökkennek, amely rontja az információk hatékony feldolgozását és a megalapozott döntések meghozatalát. Ez növeli a kritikus támadások sikerességének kockázatát, mivel a zaj közepette a támadók el tudják kerülni a biztonsági csapatok figyelmét. Továbbá az „alert fatigue”

¹¹ alert fatigue – magas riasztás mennyiség által okozott figyelmetlenség

¹² BASTA 2024, 84.

¹³ AGYEPONG Enoch et al.: Challenges and performance metrics for security operations center analysts: a systematic review. *Journal of Cyber Security Technology*, 2020/4, 11-12. o.

¹⁴ KEARNEY Paul et al.: Combating Alert Fatigue in the Security Operations Centre. *SSRN Electronic Journal*, 2023, 29. o.

¹⁵ Sz.n.: The 2020 State Of Security Operations. Forrester, 2020.

¹⁶ Sz.n.: Global Security Operations Center Study Results. IBM, 2023.

¹⁷ Uo.

¹⁸ VIELBERTH 2020, 16.

által kiváltott stressz gyakoribb hibákhoz vezethet a felügyeletben, ami a SOC teljes biztonsági állapotának rovására megy.¹⁹

Az „alert fatigue” következményei túlmutatnak az emberi teljesítményen. Például a rosszul hangolt riasztási szabályokból eredő túlzott zaj következményeképp túlterhelt SOC-csapatok sokszor egyszerűen kikapcsolják ezeket a szabályokat, ahelyett, hogy finomítanák őket.²⁰ Az ilyen gyakorlatok veszélyeztetik a SOC-észlelő képességeit a valódi fenyegetésekkel szemben, és a kezelhetetlen munkaterhelés miatt hozott átgondolatlan intézkedéseket tükrözik.

Meghosszabbított Dwell Time²¹

A döntéshozatali idő (dwell time) a kezdeti kompromittálás és a fenyegetés észlelése vagy megfékezése közötti időszak. A meghosszabbított döntéshozatali idő lehetővé teszi a támadók számára, hogy mélyebbre jussanak az érintett rendszerekben, ellophassanak érzékeny adatokat, kiterjesszék a jogosultságaikat vagy egyszerűen nagyobb kárt okozzanak. Egy korábban említett iparági kutatás alátámasztja a probléma súlyosságát, kiemelve, hogy a riasztások mindössze 49%-a kerül lekezelésre egy munkanapon belül.²² Ez a késedelem azt jelenti, hogy egyes riasztások legalább 24 órán keresztül vizsgálatlanok maradhatnak. Ez kritikus lehetőséget kínál a támadóknak, hogy mélyebbre áshassák magukat a feltört rendszerekben. Továbbá ez a kutatás arra is rámutat, hogy a riasztásokra való reagálás átlagos ideje növekvő tendenciát mutat.²³ A TTD²⁴ és TTR²⁵ mérőszámok nyomon követése szintén hozzájárulhat az elemzők elégedetlenségéhez, ha negatív visszacsatolásként használják az elemzői teljesítményre vonatkozóan, mivel nem veszik figyelembe az elvégzendő elemzés esetleges összetettségét.²⁶

A hosszabb döntéshozatali idő kiváltó okai messze túlmutatnak egyszerű operatív problémákon. Olyan mögöttes hiányosságokat tükrözhetnek, mint a felügyelt infrastruktúra elégtelen átláthatósága, valamint a riasztásokban rejlő komplex fenyegetések azonosításának képtelensége.²⁷ Ezek a késedelmek nemcsak a támadók munkáját egyszerűsíti, hanem növelik a kiberincidensekkel kapcsolatos költségeket is.

¹⁹ HÁMORNIK Balázs Péter – KRASZNAY Csaba: A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers. Előadás: *International Conference on Applied Human Factors and Ergonomics*. Los Angeles, 2017. július 20.

²⁰ KEARNEY 2023, 29.

²¹ dwell time – az az időintervallum, ameddig egy fenyegetés észrevétlenül jelen van egy kompromittált rendszeren

²² Sz.n.: Global Security Operations Center Study Results. IBM, 2023.

²³ Uo.

²⁴ TTD – Time To Detect – egy kártékony tevékenység és a hozzá tartozó riasztás kiváltása közötti idő

²⁵ TTR – Time To Respond – egy incidens azonosítása és a válaszlépés végrehajtása közötti idő

²⁶ AGYEPONG, Enoch et al.: Challenges and performance metrics for security operations center analysts: a systematic review. *Journal of Cyber Security Technology*, 2020/4, 15-21. o.

²⁷ BASTA 2024, 84.

Az extrém várakozási időkkel jellemezhető támadások nagyobb zavart okoznak az üzleti folyamatokban, ami gyakran jelentősen magasabb pénzügyi következményeket jelent a szervezetek számára.²⁸

Elégtelen képzettség és szakértelem

A kiberbiztonsági készségek terén fennálló tartós hiányosság továbbra is jelentős kihívások elé állítja a SOC-okat, elsősorban az elemzők elégtelen képzettsége és szakértelme miatt. A modern SOC-ok összetett eszközökre és platformokra támaszkodnak, amelyek kezelése speciális szakértést igényel. Azonban sok szervezet küzd a szükséges tapasztalattal és képesítéssel rendelkező személyzet felvételével és megtartásával. Ez a probléma tovább súlyosbodik a nagy nyomású környezetekben, ahol elengedhetetlen a hatékony csapatstruktúra.²⁹ Azonban a SOC-okban előforduló munkaerőbeli hiányosságok ellehetetlenítik az ehhez szükséges kollaborációt.

Az emberi erőforrások elégtelen kihasználása és a rossz menedzsment tovább bonyolítja a problémát. Ezek a szervezeti hiányosságok meghosszabbítják a döntéshozatali időt vagy akár egy incidens téves lezárásához vezethet, mivel az elemzők nincsenek felkészülve a fejlett fenyegetésekkel szemben. A támadók folyamatosan módosítják technikáikat, de sok biztonsági szakember nem rendelkezik megfelelő képzési lehetőségekkel ahhoz, hogy lépést tudjon tartani. A kiberfenyegetésekre adott hatékony válasz nem csak technikai szakértelmet igényel, hanem erős csapatmunkát és egyértelmű szerepmeghatározást is. Ezeknek a kritikus elemeknek a hiánya a SOC-okon belül tovább akadályozza a fenyegetések időben történő és hatékony mérséklését.³⁰

A magasan képzett és tapasztalt kiberbiztonsági szakemberek hiányának mértéke jelentős aggodalomra ad indokot. Egy 2024-es tanulmány 4,7 millió kiberbiztonsági szakemberre becsüli a globális hiányt,³¹ illetve egy másik jelentése szerint a szervezetek 71%-ának van betöltetlen kiberbiztonsági pozíciója.³² Az előrejelzések szerint 2025-re a jelentős kiberbiztonsági incidensek több mint feléért a tehetség hiánya vagy az emberi hiba lesz a felelős.³³ Ez rávilágít arra a paradoxonra, amely az észlelési képességek terén tett előrelépések és a biztonsági csapatok által tapasztalt hiányosságok között van. Egyrészt javul a rosszindulatú tevékenységek észlelésének képessége, de az ezen észlelések vizsgálatára való képességek nem tartottak lépést.

²⁸ RAHMAN Abdul: *A Qualitative Study on The Reduction of Dwell Time Exceeding 200 Days*. PhD-disszertáció. Capella University School of Business, Technology and Health Care Administration, 2024. 13-39. o.

²⁹ HÁMORNIK 2017.

³⁰ AL-HAJJA Qasem Abu: Human factors in cyber defense. *The Art of Cyber Defense: From Risk Assessment to Threat Intelligence*. CRC Press, Boca Raton, 2024. 396-401. o.

³¹ Sz.n.: *Cybersecurity Workforce Study*. ISC2, 2024.

³² Sz.n.: *State of Cybersecurity 2023*. ISACA, 2023.

³³ GOPAL Deepti et al.: *Predicts 2023: Cybersecurity Industry Focuses on the Human Deal*. Gartner, 2023.

A hiány részben a megfelelő képzési lehetőségek hiányából adódik, hiszen a képzések sokszor előnyben részesítik az elméletet a gyakorlati készségekkel szemben. Ezen túlmenően számos, technikai személyzet által létrehozott programból hiányoznak a hatékony oktatási módszerek, amely következképp csökkenti a szükséges szakértelem megszerzésének lehetőségét.³⁴ A szervezeteknek és egyéneknek is nehézséget okoz, hogy megbízható tanúsítványokat találjanak meghatározott szerepkörökhöz. Ezt a kihívást megnehezíti, hogy sok magas színvonalú tanúsítványhoz több éves igazolt tapasztalat szükséges.³⁵

A kiégés

Ahogy korábban is említésre került, a SOC személyzetének gyakran nagy nyomású körülmények között kell dolgoznia, egyensúlyban tartva a kritikus eseményekre való reagálást és a megfigyelés rutinfeladatait. Ez az állandó sürgősségi állapot és stressz olyan környezetet teremt, ahol a kiégés jelentős veszélyt jelent. A kiégés nemcsak az elemzők mentális egészségére és jólétére van hatással, hanem a SOC működési hatékonyságát is jelentősen károsítja. A kiégés lassabb válaszidőben, az elemzések pontosságának csökkenésében és megnövekedett munkaerő-fluktuációban nyilvánulhat meg, amelyek mind súlyosbítják a képzett kiberbiztonsági szakemberek hiányát.³⁶

A kiégés egyik elsődleges tényezője a feladatok ismétlődő és monoton jellege. Az elemzők gyakran rengeteg hamis jelzést vizsgálnak, ami fárasztó és kihívástalan feladattá válhat. A kihívások hiánya, valamint az előre meghatározott eljárások kötöttsége korlátozza az elemzők azon képességét, hogy kreatív gondolkodásmódot fejlesszenek ki a komplex fenyegetésekre való reagáláshoz. Az ebből eredő elégedetlenség növelheti a munkaerő-fluktuációt, ami munkáltatóknak sem előnyös, hiszen jelentős erőforrásokat kell fordítaniuk az új személyzet toborzására és képzésére. A SOC-elemzők gyakran jelzik, hogy elégedetlenek a szerepükkel, a hétköznapi feladatokból eredő túlterheltséget és a nem megfelelő automatizáltságot említve legfőbb tényezőkként.³⁷

A kiégés tágabb következményei az egyes elemzőkön túl a kiberbiztonsági csapatok általános teljesítményére is kiterjednek. A fáradtság, a stressz és a kiégés csökkenti az alkalmazottak kognitív képességeit, ami csökkenti az egész csapat gyors és pontos reagálási képességét. Ezt a veszélyeztetett állapotot kihasználhatják a támadók, akik az éberség hiányát megragadva megkerülhetik az észlelést. A munkavállalók mentális és fizikai egészségére gyakorolt káros hatások is jelentősek. Sok szakember számolt be

³⁴ HATZIVASILIS George et al.: Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Applied Sciences*, 2020/10. 2. o.

³⁵ FURNELL Steven: The cybersecurity workforce and skills. *Computers & Security*, 2021/100. 2-6. o.

³⁶ HÁMORNIK 2017.

³⁷ VIELBERTH 2020, 8.

rendkívüli fáradtságról, munkahelyi stresszről és a munkakörnyezet feletti kontroll elvesztéséről.³⁸

Az eszközök és folyamatok közötti integráció hiánya

A modern SOC-ok jelentős kihívásokkal szembesülnek, amelyek a működésüket megalapozó eszközök és folyamatok integrációjának hiányosságaiából fakadnak. A fenyegetések életciklusának különböző szakaszainak kezeléséhez számos biztonsági eszközre támaszkodnak, de az ezen eszközök közötti zökkenőmentes interoperabilitás hiánya gyakran adatsilókat hoz létre és bonyolítja a munkafolyamatokat. Az eltérő rendszerekből érkező riasztások korrelálása gyakran manuális munkát igényel, ami késedelmet okoz a folyamatban lévő támadások azonosításában.³⁹ Ez a széttagoltság nem csak a SOC szakemberek közötti együttműködést akadályozza, hanem a fenyegetésekre való reagálás és a kockázatcsökkentési erőfeszítések összetettségét is fokozza, mivel az elemzők kénytelenek töredezett és szétszórt információkat összerakni, hogy egységes képet alkossanak a kockázatokról.

Az empirikus adatok rávilágítanak a kihívások mértékére. Egy iparági kérdőív szerint például a szervezetek gyakran több mint 45 biztonsági eszközt használnak, valamint az incidensekre való választétezkedéshez egyszerre 19 eszköz koordinációjára van szükség.⁴⁰ Paradox módon a védelmi eszközök túlságos sokasága akadályozhatja a fenyegetések hatékony észlelését és az azokra való reagálást. Az 50-nél több eszközt használó szervezetek 8%-kal rosszabbnak ítélték magukat a felderítési képességek és 7%-kal a válaszadási képességek terén.⁴¹ Ez azt jelzi, hogy a több eszköz alkalmazása nem feltétlenül javítja a biztonsági helyzetet, sőt, sok esetben rontja azt. Ezzel szemben az interoperabilis platformokat és automatizálási technológiákat alkalmazó szervezetek jelentős javulásokról számoltak be. A jól teljesítő válaszadók 63%-a állította, hogy az ilyen megközelítések javították a kibertámadásokra való reagálási képességüket.⁴²

A problémák egy része a robusztus integráció hiánya, amely az elemzők szerint jelentős akadálya a fenyegetésekre való időben történő reagálásnak. Egy felmérés szerint a biztonsági elemzők 76%-a úgy érezte, hogy a jól integrált eszközök hiánya lassítja a válaszadási idejüket.⁴³ A rossz eszközeintegráció a SOC hatékonyságát akadályozó egyik legfontosabb technológiai kihívás, valamint az eszközök használatához kapcsolódó meredek tanulási görbék is nehezítik a munkát. Átlagosan a biztonsági riasztásoknak csupán 17%-át kezelik automatizálással, így az elemzőknek manuálisan kell kezelniük a maradékot számos eszköz segítségével.⁴⁴ Továbbá egy felmérésben részt vevő

³⁸ NOBLES Calvin: Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *HOLISTICA – Journal of Business and Public Administration*, 2022/13., 6-15. o.

³⁹ VIELBERTH 2020, 18.

⁴⁰ Sz. n.: Cyber Resilient Organization Report 2020. IBM, 2020.

⁴¹ Uo.

⁴² Uo.

⁴³ Sz.n.: Global Security Operations Center Study Results. IBM, 2023.

⁴⁴ Uo.

szervezetek mindössze 49%-a ért egyet azzal, hogy a biztonsági eszközeikből származó adatok jól integrálhatók. Ezen felül több, mint egyharmaduk arról számolt be, hogy munkatársaik emiatt rendszeresen jelentős időt pazarolnak a téves nyomok üldözésére.⁴⁵

Az integrációs kihívások mellett a használhatóság és a funkcionalitás kérdései tovább akadályozzák a SOC hatékonyságát. Sok eszközt inkább megfelelési vagy költségvetési okokból választanak, mintsem a praktikusságuk miatt, ami szintén hatékonyságbeli csökkenéséhez vezet. A rossz használhatóság és a gyakori meghibásodások további terheket rónak az elemzőkre, negatívan befolyásolva a fenyegetésekre való hatékony reagálási képességüket. A különböző infrastrukturális forrásokból gyűjtött adatok heterogenitása megnehezíti az információfeldolgozást, az elemzést és a korrelációt, amely akadályozza annak megállapítását, hogy egy esemény elszigetelt incidens vagy egy szélesebb körű támadás része.⁴⁶

A hagyományos automatizálási megközelítések és a kognitív számítástechnika megjelenése

A hagyományos automatizálási megközelítések célja a korábban megállapított problémák mérséklése. A SOC-okon belüli incidenskezelés automatizálására irányuló megközelítések túlnyomórészt a Security Orchestration, Automation and Response (SOAR) rendszerekre és más biztonsági megoldásokkal való integrációkra támaszkodtak. A SOAR⁴⁷ rendszerek olyan egységesítő keretrendszerként szolgálnak, amely a biztonsági infrastruktúra különböző összetevőit összehangolja. Ez az integráció egyszerűsített munkafolyamatokat tesz lehetővé, és csökkenti a biztonsági elemzők manuális munkaterhét. Mindez az ismétlődő feladatok automatizálásával érhető el, ami összehangoltabb incidenskezelési képességeket tesz lehetővé.

A SOAR-rendszerek egyik központi jellemzője az előre meghatározott „playbook”-ok⁴⁸ használata, amelyek riasztások által indított konfigurálható, automatizált munkafolyamatok. Például egy ismert fenyegetés észlelésekor a SOAR-rendszer a tűzfalszabályok módosításával automatikusan elszigetelheti a kompromittált gépet. Ezek az azonnali válaszlépések hagyományosan kézi beavatkozást igényeltek, de automatizálásuk lehetővé teszi az elemzők számára, hogy az incidenskezelés összetettebb aspektusaira, például a kiváltó okok elemzésére és a helyreállításra összpontosítsanak.⁴⁹ Az ilyen munkafolyamatokat gyakran felhasználóbarát,

⁴⁵ Sz.n.: The 2020 State Of Security Operations. Forrester, 2020.

⁴⁶ VIELBERTH 2020, 18.

⁴⁷ SOAR – Security Orchestration, Automation, and Response – biztonsági eszközök integrálása és a válaszlépések automatizálására szolgáló platform

⁴⁸ playbook – egy incidenskezelési lépések előre meghatározott forgatókönyve

⁴⁹ BASTA 2024, 381-383.

„low code”⁵⁰ vagy „no code”⁵¹ interfészekon keresztül határozzák meg, lehetővé téve a biztonsági személyzet számára, hogy automatizált lépéssorozatokat tervezzenek nagyfokú programozási szakértelem nélkül. Ezek a lépések magukban foglalhatják a riasztások kontextuális információkkal való gazdagítását vagy az automatizált válaszhelyettesítések elindítását.⁵² Az ilyen munkafolyamatokhoz szükséges integrációkat jellemzően API-kon⁵³ keresztül valósítják meg, lehetővé téve a biztonsági megoldások közötti interoperabilitást.

Bár a SOAR-rendszerek a hagyományos automatizálás egyik alappillérei, a tapasztalt biztonsági személyzettel rendelkező szervezetek gyakran áthidalják ezeket a rendszereket az egyedi fejlesztésű automatizálást preferálva. A képzett fejlesztők a különböző biztonsági termékek API-jait kihasználva hasonló automatizálási eredményeket érhetnek el anélkül, hogy dedikált SOAR-eszközöket használnának.

A piackutatások azt mutatják, hogy a SOAR-rendszereket elsősorban a nagyobb és fejlettebb kiberbiztonsági képességekkel rendelkező szervezetek vagy a kiberbiztonsági szolgáltató cégek alkalmazzák.⁵⁴ Ezen túlmenően más biztonsági technológiák, például a SIEM⁵⁵ és a XDR⁵⁶ rendszerek fejlődése csökkentette a SOAR-rendszerek egyedi vonzerejét bizonyos felhasználási esetekben.⁵⁷

Bár a SOAR-rendszerek egyszerűsítik a munkafolyamatokat és automatizálják a rutinfeladatokat, használhatóságuk és teljesítményük nagymértékben függ a megfelelő konfigurációtól. A SOAR-rendszerek bevezetéséről szóló átfogó tanulmány kimutatta, hogy a rosszul konfigurált eszközök csökkentett funkcionalitáshoz és operatív hiányosságokhoz vezethetnek.⁵⁸ Míg a SOAR-rendszerek általában csökkentették a vizsgálati időt és minimalizálták a kontextusváltásokat, az automatizmusok túlzott használata néha kevésbé pontos vagy akár hiányos incidensjegyeket eredményezett az automatizált űrlapok kitöltésében mutatkozó hiányosságok miatt.⁵⁹ Az elemzők aggodalmukat fejezték ki a túlzott automatizálással kapcsolatban, figyelmeztetve arra, hogy az a vizsgálatok során elmulasztott lépésekhez

⁵⁰ low code – egy programfejlesztési megközelítés, ahol minimális programozási ismeret szükséges

⁵¹ no code – egy programfejlesztési megközelítés, ahol programnyelvek használata nem szükséges

⁵² MUGHAL Arif Ali: Building and Securing the Modern Security Operations Center (SOC). *International Journal of Business Intelligence and Big Data Analytics*, 2022/5. 10-11. o.

⁵³ API – Application Programming Interface – szoftverek közötti kommunikációt lehetővé tevő interfész

⁵⁴ LAWSON Craig – SHOARD Pete: *Market Guide for Security Orchestration, Automation and Response Solutions*. Gartner, 2023.

⁵⁵ SIEM – Security Information and Event Management – biztonsági események gyűjtése, elemzése és kezelése szolgáló rendszer

⁵⁶ XDR – Extended Detection and Response – egy biztonsági termék/platform, amely többféle rendszerből gyűjt adatokat a fenyegetések észlelésére és kezelésére

⁵⁷ Uo.

⁵⁸ BRIDGES Robert et al.: Testing SOAR tools in use. *Computers Security*, 2023/129. 15-16. o.

⁵⁹ Uo.

vagy hibákhoz vezethet.⁶⁰ Emellett a SOAR-eszközök integrálása a meglévő munkafolyamatokba erőforrás-igényesnek bizonyult, és gyakran magasan képzett fejlesztőket vagy elemzőket igényelt a zökkenőmentes működés biztosításához.⁶¹

Ugyan a SOAR-rendszerek továbbra is értéket képviselnek, piaci jelentőségük a korábban említett korlátok⁶² miatt egyre inkább csökken. Továbbá a generatív mesterségesintelligencia-technológiák és a nagy nyelvi modellek elterjedése a hagyományos SOAR-funkciókat meghaladó automatizálási lehetőségeket teremtett.⁶³ A kognitív számítástechnika fejlődésével az automatizálás fókusza a SOAR-rendszerekről és a hagyományos automatizálásról az összetettebb megoldások felé mozdult el.

A kognitív számítástechnika előretörése az automatizálásban összhangban van a mesterséges intelligencia átalakító hatásával, amelyet hatalmas beruházások, innováció és integráció jellemez. A generatív mesterséges intelligencia gazdasági potenciálja óriási, becslések szerint évente 6,1 és 7,9 billió dollár közötti összeget tudna hozzátenni a termelékenység növekedéséhez a különböző iparágakban.⁶⁴ Ez a gazdasági növekedés a nagyobb országok GDP-jéhez⁶⁵ viszonyítható.

A kognitív számítástechnika célja a kiberbiztonsági csapatok hatékonyságának növelése a kiberfenyegetések összetettségének adaptív, hatékony és automatizált megoldásokkal való kezelése révén. A védelmi rendszerek ezáltal képessé válnak arra, hogy érveljenek, tanuljanak, és olyan döntéseket hozzanak, amelyekhez általában emberi intelligenciára van szükség. Ez potenciálisan átalakíthatja a kiberbiztonsági gyakorlatokat, és enyhítheti a SOC-okat sújtó tartós problémákat. A kognitív számítástechnika arra is készítheti a SOC-okat, hogy újragondolják a munkaerő képzését. Egy iparági kutatócsoport előrejelzése szerint 2028-ra a generatív technológiák a belépőszintű kiberbiztonsági szerepkörök 50%-ában megszüntethetik a speciális képzés szükségességét.⁶⁶

Aktuális kognitív számítástechnikai megközelítések

A SOC-ok optimalizálására szolgáló kognitív számítástechnikai megközelítések változatosak és többdimenziósak. A szakirodalmi áttekintés során végzett kutatás alapján a kognitív számítástechnikán alapuló optimalizálás a SOC-okban nagyjából két területbe sorolható.

⁶⁰ Uo.

⁶¹ Uo.

⁶² A funkcionalitásukat más technológiák átveszik, illetve a tapasztalt felhasználók preferálják az egyedi integrálásokat.

⁶³ LAWSON 2023.

⁶⁴ CHUI Michael et al.: *The economic potential of generative AI: The next productivity frontier*. McKinsey & Company, 2023.

⁶⁵ GDP – Gross Domestic Product – egy ország gazdasági teljesítményének mérőszáma, az előállított termékek és szolgáltatások összértéke

⁶⁶ Sz. n.: *AI in Cybersecurity: Define Your Direction*. Gartner, 2024.

Az első kategória az észlelési képességek javítása, amely a kognitív számítástechnikát alkalmazza a kártékony tevékenységek azonosítására. Ez a terület jól kidolgozott alapokra épül, és több évre visszanyúló, kiterjedt szakirodalom áll mögötte. A hagyományos gépi tanulás alkalmazása nagymértékben az észlelési fázisra összpontosít, és olyan területeket foglal magába, mint az e-mailben terjedő fenyegetések, a felhasználói anomáliák, a hálózati behatolások és a rosszindulatú programok felismerése.⁶⁷ A kognitív számítástechnika ezen alkalmazása kibővítette a hagyományos szignatúra-alapú észlelési módszereket azáltal, hogy lehetővé tette a hatalmas mennyiségű strukturálatlan adat feldolgozását emberszerű kognitív értelmezéssel.

A felderítési képességek javítására irányuló kutatások gyakran különböző neurális hálózati architektúrák alkalmazásával foglalkoznak, különösen újabb figyelem mechanizmusokkal és optimalizációs algoritmusokkal kombinálva. Az élvonalbeli kutatásokban újonnan megjelenő „self-attention”⁶⁸ mechanizmusok lehetővé teszik, hogy a rendszerek hatékonyan és nagyfokú kontextustudatossággal dolgozzanak fel olyan adatszekvenciákat, mint a naplófájlok vagy a hálózati adatfolyamok. Ez új lendületet adott a rosszindulatú tevékenységek viselkedésalapú felismerésével kapcsolatos kutatásoknak. A legtöbb erőfeszítés azonban kismértékű pontosságnövelést céloz meg, hiszen sok esetben a precizitás már most is meghaladja a 95%-ot. Ezáltal az észlelési képességek javítása egy kiforrott, csökkenő megtérüléssel járó területnek mondható.⁶⁹

A második, úttörőjellegű kutatási terület a triázs folyamat különböző szakaszainak automatizálása. Ez a terület a kognitív számítástechnika technológiáinak felhasználására összpontosít a biztonsági elemzők döntéshozatali folyamatainak utánzására vagy kiegészítésére. A korábban részletezett észlelési képességek javításával ellentétben a triázs folyamat automatizálása viszonylag új terület a kiberbiztonsági kutatásokban. Ez az új technológia a SOC-ok előtt álló kritikus kihívások többségére megoldást jelenthet. Ez annak köszönhető, hogy ez a fajta automatizálás a SOC-észlelést követő tevékenységeire összpontosít, amelyek korábban jellemzően az emberi elemzők hatáskörébe tartoztak, mivel mélyreható betekintést és kézi vizsgálatot igényeltek. A neurális hálózati architektúrák, a figyelemmechanizmusok és az optimalizációs algoritmusok terén elért előrelépések itt is kulcsfontosságúak, lehetővé téve a klasszifikációs modellek számára a kontextuális információk megőrzését és a nagy mennyiségű adat elemzését.⁷⁰

⁶⁷ NTALAMPIRAS, Stavros et al.: *Artificial intelligence and cybersecurity research – ENISA research and innovation Brief*. European Union Agency for Cybersecurity, Athens, 2023. 06. 07.

⁶⁸ self-attention – egy mesterséges intelligencia mechanizmus, amely a bemenet egyes elemei közötti kapcsolatokat értékeli ki a szöveg vagy adatstruktúra kontextusának pontos megértése érdekében

⁶⁹ SALEM Aya et al.: Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, 2024/11., 1-34. o.

⁷⁰ BAKKER Pascal: Automating the Cybersecurity Triage Process. Előadás: *Twente Student Conference on IT*. University of Twente, Twente, 2024. Július 5.

Tekintettel a detekciót javító kutatások érettségére és széles körű elterjedtségére, ez a szakirodalmi áttekintés kizárólag a triázsfolyamat automatizálására összpontosít, amely a kognitív számítástechnikai alkalmazások izgalmasabb és kevésbé feltárt területét képviseli. Míg a felderítési képességekkel kapcsolatos kutatások a módszerek kifinomítására összpontosítanak, a triázs automatizálása lehetőséget kínál a SOC-műveletek alapvető átalakítására. A következő fejezetek ezt a feltörekvő területet vizsgálják, kiemelve, hogy a kognitív számítástechnika hogyan alakíthatja át a SOC-munkafolyamatokat az emberi elemzők támogatásával a triázs folyamat során.

A triázs automatizálása

A kognitív számítástechnika szerepe a kiberbiztonságban a szerény kezdetekhez képest jelentős fejlődésen ment keresztül. Az IBM úttörője volt egy ilyen kognitív számítástechnikai rendszernek, amelyet még a 2020-as évek eleji mesterségesintelligencia-felhajtás előtt vezettek be. Ez a megoldás az NLP-t,⁷¹ a gépi tanulást és a tudásreprezentációt kombinálta a strukturálatlan adatok elemzésére és a biztonsági elemzők támogatására a triázspan.⁷² Ez a termék kiegészítette az IBM SIEM rendszerét, segítve a SOC-elemzőket azáltal, hogy a belső hálózati adatok és a gépi tanulóval feldolgozott külső fenyegetéselemzés (TI) korrelációjával csökkentette a döntéshozatali időt. A feldolgozott TI⁷³-adatok egy tudásgráfba strukturálódnak, amely aztán kontextuális információt nyújthat a SIEM-ben kiváltott riasztásokhoz. Az incidenshez kapcsolódó tudásgráf vizuálisan ábrázolja az entitásokat (pl. belső informatikai eszközök, felhasználók, külső IP-címek és rosszindulatú szoftverek) és a köztük lévő kapcsolatokat. Ennek az áttekintésnek a célja, hogy vizuálisan bemutassa, hogyan bontakozott ki az észlelt támadás. Emellett az NLP-vel feldolgozott fenyegetettségi információk alapján hasznos tudnivalókat szolgáltat arról, hogy a támadók milyen további entitásokat veszélyeztethetnek.

A SOC-elemzők számára ez a döntéstámogató mechanizmust biztosít azáltal, hogy automatizálja a különböző TI-források összegzését, és igyekszik hasznosítható következtetéseket bemutatni. Bár ez mai mércével mérve triviálisnak tekinthető, ez volt az egyik korai felhasználási eset, amely a triázsfolyamat kognitív számítástechnikával való kiegészítését jelentette. Az ilyen vizualizációnak a döntéshozatali idő csökkentésében mutatkozó előnyei megkérdőjelezhetőek, különösen összetettebb esetekben. Ezt a korlátozott hasznosságot tükrözi e megoldás csekély számú letöltöttsége is.⁷⁴

Természetesen a kognitív számítástechnika hozzáadott értéke az évek során jelentősen javult, köszönhetően a jelentős technológiai áttöréseknek. Napjainkban az

⁷¹ NLP – Natural Language Processing – egy tudományág, amely lehetővé teszi a számítógépek számára az emberi nyelv megértését és feldolgozását

⁷² ROGERS Liz: Bringing the Security Analyst into the Loop: From Human-Computer Interaction to Human-Computer Collaboration. Előadás: *Ethnographic Praxis in Industry Conference Proceedings*. EPIC, Providence, 2019. 11. 11.

⁷³ TI – Threat Intelligence – kiberfenyegetésekről szóló információk gyűjtése és elemzése

⁷⁴ Sz.n.: QRadar Advisor With Watson -v7.5.0+. IBM, 2023. 04. 26.

egyik legelterjedtebb vállalati eszköz, amely a triázs kiegészítésére rendelkezésre áll, a Microsoft Security Copilot.⁷⁵ Ez a megoldás az OpenAI LLM-jét⁷⁶ integrálja a Microsoft saját kiberhírszerzésével és biztonsági adataival. Generatív AI-asszisztensként működik a biztonsági elemzők számára, amely elemzi a telemetriai adatokat, összefoglalja az incidenseket, és KQL⁷⁷ lekérdezéseket generál a hatékonyabb elemzéshez. A Copilotnak azonban vannak olyan összetevői is, amelyek hagyományosabb gépi tanulási modelleket használnak a biztonságspecifikus klasszifikációs és predikciós problémákhoz. Ilyenek például a riasztások osztályozása, a vizsgálati lépések azonosítása és a helyreállítási javaslatok kialakítása.

A Microsoft Research Group⁷⁸ közzétett egy tanulmányt egy olyan keretrendszerrel, amely megoldást kínál ezekre a kihívásokra.⁷⁹ A Microsoft Defender XDR-be⁸⁰ integrált, skálázható gépi tanulási architektúrát vezettek be, amely a telemetriai adatok és más Microsoft-ügyfelek korábbi incidensbesorolásai alapján előre jelzi az újabb incidensek minőségét (igaz pozitív, hamis pozitív vagy ártalmatlan pozitív). A rendszer robusztus előfeldolgozó rendszert alkalmaz, amely biztosítja a számítási hatékonyságot a földrajzilag elosztott infrastruktúrájukban. Az osztályozási modellt egy gridsearch⁸¹ optimalizált random forest⁸² algoritmus segítségével valósítják meg. A cikk szerzői szerint a modell 87%-os átlagos macro-F1⁸³ értéket ér el.⁸⁴ A keretrendszer kontextuális ajánlásokat is ad a riasztások kivizsgálásához a historikusan hasonló incidensek azonosításával. Ez a korreláció hash⁸⁵ egyeztetés és az incidens beágyazási vektorjainak koszinusz hasonlóságának kombinációjával történik. Ezek a beágyazások 180 napnyi telemetriai adat folyamatos feldolgozásával jönnek létre, biztosítva, hogy az ajánlások relevánsak és átfogóak legyenek. A szerzők állítása szerint a vizsgálati ajánlások 94%-os relevanciaarányt tartanak fenn, kiemelve a beágyazáson alapuló

⁷⁵ Microsoft Security Copilot – Egy mesterséges intelligenciával támogatott biztonsági eszköz, amely segít a fenyegetések elemzésében, választintézkedésekben és a kiberbiztonsági műveletek automatizálásában.

⁷⁶ LLM – Large Language Model – nagyméretű, nyelvi mintákon alapuló mesterséges intelligencia modell

⁷⁷ KQL – Kusto Query Language – Microsoft által fejlesztett lekérdező nyelv nagy adattömegek elemzésére

⁷⁸ Microsoft Research Group – A Microsoft kutatási csoportja, amely innovatív megoldásokat fejleszt különböző tudományos és ipari területeken

⁷⁹ FREITAS Scott et al.: AI-Driven Guided Response for Security Operation Centers with Microsoft Copilot for Security. h.n., 2024, 1-10. o.

⁸⁰ Microsoft Defender XDR – A Microsoft kibervédelmi termékcsaládja, amely átfogó és integrált védelmet nyújt az informatikai infrastruktúra valamennyi eleméhez

⁸¹ gridsearch – egy módszer, amelyben különböző paraméterkombinációkat próbálnak ki gépi tanulási modellek teljesítményének optimalizálása érdekében

⁸² Random forest – egy gépi tanulási algoritmus, amely több döntési fát épít és azok előrejelzéseit egyesíti

⁸³ macro-F1 – az F1-mutató olyan átlaga, amely az osztályokat egyenlő súllyal kezeli, függetlenül az osztályok gyakoriságától

⁸⁴ FREITAS 2024, 1-10.

⁸⁵ hash – egy algoritmus, amely adatokat fix méretű, egyedi azonosítókká alakít át

megközelítések hatékonyságát az incidensminták azonosításában.⁸⁶ A rendszer a korábban említett riasztási beágyazások alapján helyreállítási ajánlásokat is adhat, megpróbálva azonosítani az adott incidensre vonatkozó megfelelő válaszlépéseket (pl. egy felhasználó letiltása vagy egy gép elszigetelése). A cikk szerzői szerint a macro-F1 mutató 99%-os.⁸⁷ A vizsgálati és a helyreállítási modellek inferencia⁸⁸ mutatói elég magasnak tekinthetők ahhoz, hogy a valós SOC-környezetekben is használhatóak legyenek, azonban a triázs eredményei még mindig hagynak teret a fejlesztésre. Az eredmények közel sem elég pontosak ahhoz, hogy helyettesítsék az emberi elemzői triázt, azonban felhasználhatók a riasztási várólista előszűrésére vagy prioritizálására. Ezt a szerzők megállapításai is alátámasztják, miszerint az incidenseknek csak 41%-át lehet a gyakorlatban klasszifikálni, hiszen az éles működésben magasabb bizonyossági küszöbértékekkel kell dolgozni a téves klasszifikációk elkerülése végett.⁸⁹

A riasztások vizsgálata rendkívül nehéz osztályozási probléma, amely számos különböző forrásból származó adat elemzését igényli, az informatikai környezetre és a támadói taktikákra vonatkozó kontextuális ismeretekkel kombinálva. Ezen tényezők és a skálázhatósági problémák együttesen az okai annak, hogy még a piacvezető megoldások, mint például a Copilot, sem képesek teljesen automatizálni az emberi elemzői triázt. A kognitív számítástechnikában és az alapul szolgáló hardverekben⁹⁰ folyamatosan végbemenő hatalmas technikai fejlesztésekkel lehetséges, hogy hosszú távon az emberi elemzők helyettesíthetővé váljanak, különösen az alsóbb beosztásokban.

Addig is azonban számos kutató olyan keretrendszereket fejleszt ki, amelyek az emberi elemző triázs folyamatának támogatásával hatékonyabban használják a meglévő osztályozási képességeket. Az egyik ilyen keretrendszer automatizált, támogatott és kollaboratív döntéshozatali módokat integrál a SOC-ok hatékonyságának javítása érdekében.⁹¹ A keretrendszer a kognitív számítástechnikát javasolja a rutinszerű riasztások ellenőrzésére, az összetett esetekben az emberi elemzőkre történő szelektív átadást, valamint az újszerű és kétértelmű fenyegetések esetében a kollaboratív kivizsgálást. Ez a többretegű megközelítés a triázs folyamat optimalizálását szolgálja a kognitív számítástechnikai rendszerek és az emberi elemzők közötti döntéshozatali felelősség dinamikus egyensúlyozásával. Ez a megközelítés csökkenti az elemzők kognitív terhelését, ugyanakkor javítja a működési hatékonyságot. A rugalmas autonómia lehetővé teszi az automatizálás szintjének dinamikus módosítását a feladat összetettsége és a kontextuális követelmények alapján. Ebben a keretrendszerben az autonóm rendszerek öntudatossággal rendelkeznek, hogy felismerjék korlátjaikat, és szükség esetén az emberi elemzőkre bizzák a feladatukat, miközben ajánlásaikat az

⁸⁶ Uo.

⁸⁷ Uo.

⁸⁸ inference – mesterséges intelligencia modellek alkalmazása predikcióra

⁸⁹ FREITAS 2024, 1-10.

⁹⁰ REUTHER Albert et al.: AI and ML Accelerator Survey and Trends. Előadás: *IEEE High Performance Extreme Computing Conference (HPEC)*. IEEE, Waltham, 2022. 09. 21.

⁹¹ CHHETRI Mohan Baruwat et al.: Towards Human-AI Teaming to Mitigate Alert Fatigue in Security Operations Centres. *ACM Transactions on Internet Technology*, 2024/3. 1-22. o.

elemzők kognitív terheltsége és szaktudása alapján igazítják ki. A keretrendszer a Learning to Reject⁹² és a Learning to Defer⁹³ technikák alkalmazását javasolja a kognitív számítástechnikai modell azon képességének fokozására, hogy felismerje a bizonytalan helyzeteket, és a döntéshozatalt emberi szakértőkre delegálja. Ezen kívül az imitációs tanulás és a megerősítéses tanulás alkalmazásával a kognitív számítástechnikai rendszerek igazodhatnak az emberi elemzők elemzési szokásaihoz.

Bár a keretrendszer szerzői nem szolgáltatottak technikai megvalósítást, elméletük lehetővé tenné, hogy a kognitív számítástechnikai rendszerek az adatintenzív feladatokra összpontosítsanak, míg az emberi elemzők az árnyalt ítélőképességet igénylő feladatokkal foglalkoznak. Ez a többrétegű riasztáskezelési keretrendszer a jelenleg rendelkezésre álló riasztási triázsmodellekkel kombinálva elősegítheti a riasztások sokkal magasabb fokú automatikus triázsát anélkül, hogy az automatizált rendszer téves megítéléseket hozhatna. Bár pontos technikai implementáció hiányában nehéz megítélni a vázolt keretrendszer hatékonyságát. Ezért tehát további kutatásokra van szükség egy ilyen megoldás technikai megvalósíthatóságának vizsgálatához.

Egy másik hasonló megközelítés egy újszerű elképzelésre összpontosít, amelyet Continuous Human-in-the-Loop Learning (CHILL)⁹⁴ elnevezéssel illetnek. Ez egy olyan módszertant jelent, amelyben az emberi elemzők és a kognitív számítástechnikai rendszerek iteratív módon együttműködnek, és a tudás idővel átkerül az elemzőtől az automatizált rendszerekhez. Ez az együttműködés lehetővé teszi a rendszer számára, hogy folyamatosan finomítsa a riasztások és azok kiváltó okainak megértését, valamint a pusztán osztályozáson túl magyarázó és előrejelző képességeket érjen el. A CHILL alkalmazásával a kognitív számítástechnikai rendszer azáltal fejlődik, hogy döntéseit az elemző visszajelzéseivel validálja, és modelljét a döntéshozatal pontosságának javítása érdekében finomítja. Cserébe az elemzők egyre inkább támaszkodhatnak a modell osztályozási pontosságára, hogy újra prioritizálhassák a riasztásokat, és a mélyebb vizsgálatokra összpontosítsanak.

A rendszer pontos technikai megvalósítását a szerzők nem részletezték, azonban tanulmányukban felvetették az ML korlátait ebben a kontextusban, és azt javasolták, hogy alternatív Machine Reasoning⁹⁵ (MR) megközelítések alkalmasabbak lehetnek a célra. A szerzők egy Bayes-hálózat alapú illusztrációt is adtak az MR döntéshozatalhoz. Technikai részletek nélkül a tanulmány megállapításait nehéz igazolni. Azonban a szerzők bemutattak egy korai prototípust egy SOC-környezetben. Az előzetes eredményeik szerint bebizonyosodott, hogy az elemzői munkaterhelés jelentős

⁹² Learning to Reject – egy gépi tanulási technika, amely bizonytalan helyzetekben a döntést elutasítja

⁹³ Learning to Defer – egy gépi tanulási technika, amely bizonytalan helyzetekben emberi döntésre hagyatkozik

⁹⁴ KEARNEY 2023, 1-34.

⁹⁵ Machine Reasoning – egy kutatási terület, amely algoritmusokkal végez logikai következtetést és problémamegoldást (pl. szabályalapú rendszerek, formális logikai eszközök)

csökkentésére képes a rendszer. A Windows-rendszerek⁹⁶ bejelentkezéseivel kapcsolatos riasztások mélyreható elemzése (amelyek a SOC-hoz beérkezett esetek jelentős részét tették ki) kimutatta, hogy a rendszer nagy megbízhatósággal képes azonosítani az ártalmatlan riasztásokat, mint például a lejárt jelszavakat vagy a konfigurációs hibákat. Ennek eredményeként a kézi feldolgozást igénylő Windows bejelentkezési riasztások száma közel 90%-kal csökkent.⁹⁷

A megmagyarázható mesterséges intelligencia (XAI) ígéretes alternatívája lehet az MR-alapú megközelítéseknek. A "fekete dobozos" mesterségesintelligencia-modellekkel ellentétben az XAI⁹⁸ értelmezhetőséget és átláthatóságot biztosít, lehetővé téve az elemzők számára a döntéshozatali folyamatok megértését és validálását. Ez a megközelítés áthidalja a szakadékot a gépi ajánlások és a teljes triázsautomatizálás között, biztosítva az elszámoltathatóságot és az adaptivitást.⁹⁹ Az XAI ösztönzi az együttműködést azáltal, hogy az emberi elemzők számára lehetővé teszi az elemzés finomítását bemeneti módosítások, információfrissítések vagy „mi lenne, ha” forgatókönyvek segítségével.¹⁰⁰ Ezek a rendszerek intrinsíc¹⁰¹ vagy post-hoc¹⁰² módszerek alkalmazásával generálnak magyarázatokat. Az intrinsíc módszerek olyan, természetükből adódóan értelmezhető modelleket tartalmaznak, mint a lineáris regresszió vagy a döntési fák, ahol a predikciók mögötti logika teljesen átlátható. A post-hoc módszerek a modellsúlyok megváltoztatása nélkül magyarázzák a modell viselkedését, többnyire annak kiszámításával, hogy mely bemeneti tulajdonságok járultak hozzá leginkább egy adott döntéshez.

A magyarázó kimenetek különböző formában jelennek meg, de többnyire szöveges, vizuális vagy szabályalapúak. Az XAI-nak a döntések mögött meghúzódó logika magyarázatára vonatkozó kutatásai széleskörűek, számos technikai megvalósítással.¹⁰³ Az XAI-modellek magyarázatainak értékelése azonban nehézkes, mivel nem léteznek szabványosított mérési és összehasonlítási módszerek. Ezért a legtöbb tanulmány a felhasználói elégedettségi felmérésekhez fordul, amelyeket szintén nehéz szélesebb kontextusban értelmezni, és még nehezebb más modellekkel való összehasonlításra használni.

⁹⁶ Windows – Egy Microsoft által fejlesztett operációs rendszer

⁹⁷ KEARNEY 2023, 1-34.

⁹⁸ XAI – Explainable Artificial Intelligence – egy olyan típusú mesterséges intelligencia, amelynek kimenetelei (és a hozzájuk tartozó döntési folyamatok) átláthatóak

⁹⁹ SARKER Iqbal: AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability. *Springer Nature Switzerland, Cham*, 2024. 28-29. o.

¹⁰⁰ HOLDER Eric – WANG Ning: Explainable artificial intelligence (XAI) interactively working with humans as a junior cyber analyst. *Human-Intelligent Systems Integration*, 2021/3. 5-7. o.

¹⁰¹ intrinsic – egy modell belső jellemzőin alapuló elemzés

¹⁰² post-hoc – egy modell működésének utólagos elemzése

¹⁰³ ZHANG Zhibo et al.: Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access*, 2022. 1-36. o.

Az XAI triázs kontextusban történő felhasználását övező kutatások korlátozottabbak, azonban egy tanulmány javaslatot tett egy olyan architektúrára, amely kifejezetten a riasztási triázshoz szükséges magyarázatok létrehozására szolgál.¹⁰⁴ A javasolt megoldás egy adott riasztáshoz kapcsolódó eseménysorozatokból generál részgráfokat. Ezek a részgráfok lényegében egy lehetséges lépéssorozatot jelentenek, amely potenciálisan megmagyarázza a támadás lefolyását. A részgráfok fontosságát a kooperatív játékelméletből származó megközelítéssel (Shapley értékek¹⁰⁵) rangsorolják. A magasabb rangú részgráfok nagyobb mértékben járulnak hozzá a modell döntéséhez, és ezért valószínűleg tartalmaznak kritikussá válnak kapcsolatos eseményeket. A szerzők által végzett korlátozott tesztelés azt sugallja, hogy az elemzők a riasztások osztályozása során lényegesen jobb döntéseket hoztak, mint amikor más, nem kiberbiztonság-specifikus XAI-architektúrákat használtak a magyarázatok generálásához. A szerzők állításai szerint az elemzők 6-9 perccel gyorsabban hoztak döntést, és 33% és 58% közötti mértékben pontosabbak voltak.¹⁰⁶

A kognitív számítástechnikai rendszerek értelmezhetőségének biztosítása nem az egyetlen olyan megközelítés, amely szavatolja, hogy az osztályozási hibákat az emberi elemzők felismerjék. Ilyen például egy cikk, amely a SOAR-rendszerekben használt hagyományos, playbook-alapú automatizálásból merít ihletet egy olyan triázsfolyamat létrehozására, amely magában foglalja mind a kognitív számítástechnikát, mind az előre meghatározott munkafolyamatokat.¹⁰⁷ A szerzők egy strukturált módszertant javasolnak, amely három kulcsfontosságú szakaszból, az adatkinyerésből, a feldolgozásból és a playbook végrehajtásából áll. Az adatkinyerési fázisban egy mesterséges intelligencia a különböző formátumú (pl. XML,¹⁰⁸ JSON,¹⁰⁹ Syslog¹¹⁰) biztonsági riasztásokat egy közös sémába normalizálja. NLP-technikák segítségével a modell azonosítja a kontextuális entitásokat (pl. IP-címek, hosztnévek, fájlnevek stb.), amelyek kulcsfontosságúak a riasztások elemzéséhez. Ezt követően a feldolgozási fázis külső forrásokat, például konfigurációkezelő adatbázisokat, fenyegetéselemző platformokat és sebezhetőségi szkennerek eredményeit integrálja a kontextusba helyezés és a kinyert adatok validálása érdekében. Az utolsó szakaszban a gazdagított adatok felhasználása előre meghatározott forgatókönyveken keresztül történik. Ezek a forgatókönyvek szisztematikusan értékelik a riasztásokat az elemzők által előre meghatározott triázslépések elvégzésével. A szerzők a javasolt rendszert az

¹⁰⁴ MALACH Alon et al.: CyberShapley: Explanation, prioritization, and triage of cybersecurity alerts using informative graph representation. *Computers & Security*, 2024, 1-14. o.

¹⁰⁵ Shapley értékek – Egy kooperatív játékelméleti fogalom, amely meghatározza, hogy egy játékos milyen mértékben járul hozzá a közös eredményhez

¹⁰⁶ Uo.

¹⁰⁷ RAFIEY Pasha – NAMADCHIAN Amin: Using LLMs as AI Agents to Identify False Positive Alerts in Security Operation Center. *International Journal of Information Security*, é.n., 1-15. o.

¹⁰⁸ XML – Extensible Markup Language – strukturált adatok ábrázolására használt jelölőnyelv

¹⁰⁹ JSON – JavaScript Object Notation – strukturált adatok könnyen olvasható formátuma

¹¹⁰ Syslog – egy logformátum és protokoll rendszerek eseményeinek naplózására

NGIDS-DS¹¹¹ adathalmaz segítségével értékelték, és azt állítják, hogy a mesterséges intelligencia 93,1%-os F1¹¹² metrikával azonosította a téves pozitív jelenségeket, ami felülmúlja a kézi módszereket (91,3%), miközben az elemzési időt 325 percről 40 percre csökkentette 1000 tesztriesztás esetén.¹¹³ Ez a javasolt megközelítés néhány korábban ismertetett megközelítéshez képest egyszerűbb, mivel a tényleges döntéshozatalt átlátható, ember által tervezett munkafolyamatok végzik. A kognitív számítástechnikai folyamatok csupán kiegészítik az előfeldolgozási képességeket, amelyek segíthetik az emberi elemzőket a kifinomultabb és pontosabb munkafolyamatok létrehozásában.

Az eddig vizsgált kutatások nagy része speciális kognitív számítástechnikai megközelítéseket alkalmaznak a SOC-ok triázshatékonyságának növelésére. Ugyanakkor a közhasznált nagy nyelvi modellek alkalmazásával kapcsolatban is folytak kutatások.¹¹⁴ Az egyik ilyen cikk olyan modellek mélyreható tesztelését tartalmazza, mint a GPT-4,¹¹⁵ GPT-3.5, LLaMA-3,¹¹⁶ többek között az első szintű elemzői munkafolyamatok hatékonyságának és megbízhatóságának növelésére. A szerzők által javasolt módszertan szerint a riasztásokat a SIEM-rendszerből és a TI-forrásokból származó kontextuális információkkal gazdagítják, amelyeket aztán elemzés céljából a tesztelt nagy nyelvi modellekbe táplálnak. Az LLM a keretrendszer elemző központjaként szolgál, amely a riasztásokat „akcióképes” vagy „nem akcióképes” kategóriába sorolja. Ez a besorolás a riasztások kontextuális megértésén alapul, amely a riasztásokból kinyert tulajdonságokból származik. A rendszer a hallucinációk enyhítésére szolgáló mechanizmusokat is tartalmaz, amely a modell kimeneteinek a riasztás ismert adataival való összevetésével valósul meg. A nagy nyelvi modellek osztályozásai ezután olyan jelentésekké strukturálódnak, amelyek a SOC-elemzők számára érthetőek és felhasználhatók. Ezek a jelentések tartalmazzák a riasztás legfontosabb részleteit, a mesterséges intelligencia elemzését és a következő lépésekre vonatkozó ajánlásokat.

A keretrendszer kialakítása hangsúlyozza az automatizálás és az emberi felügyelet egyensúlyának fontosságát, és olyan hibrid megközelítést javasol, amelyben a nagy nyelvi modellek másodpilótaként működnek. A rendszer biztosítja a kezdeti osztályozásokat és ajánlásokat, míg az emberi elemzők megtartják a végső döntési hatáskört. A szerzők azt állítják, hogy az LLM-ek integrálása a triázsfolyamatba

¹¹¹ NGIDS-DS – Next-Generation Intrusion Detection System-Dataset – egy címkézett adathalmaz, amely hálózati és hoszt alapú naplókat tartalmaz, valós hálózatok normál és támadó forgalmi dinamikáját tükrözve.

¹¹² F1 – egy osztályozási modell teljesítményének mérőszáma, a pontosság és a visszahívás harmonikus átlaga

¹¹³ RAFIEY – NAMADCHIAN é.n. 1-15.

¹¹⁴ SINGH Yuvraj et al.: Enhancing Security Operations Center Efficiency through Multi-Model Integration of Large Language Models and SIEM Systems. *International Journal of Information Security*, é.n., 1-26. o.

¹¹⁵ GPT – Generative Pre-trained Transformer – szöveggorpusszal tanított neurális hálózat amely képes szövegek létrehozására és feldolgozására

¹¹⁶ LLaMA – Large Language Model Meta AI – Meta által fejlesztett nagyméretű nyelvi modell

jelentősen csökkentette az elemzők kognitív terhelését, és elmondásuk szerint 60%-kal csökkent a kézi felülvizsgálatot igénylő riasztások száma.¹¹⁷ A kezdeti riasztási kategorizálás és az alapvető fenyegetéselemzés automatizálása a kritikus incidensek eszkalációjához szükséges időt állítólag 40%-kal csökkentette.¹¹⁸ A legjobban teljesítő nagy nyelvi modell 94%-os pontosságot és 93%-os F1-értéket ért el.¹¹⁹ Ezek az eredmények ígéretesek, különösen, ha figyelembe vesszük, hogy a keretrendszer által javasoltak szerint a tényleges döntéshozatali hatáskör továbbra is az emberi elemzőnél marad. Mindazonáltal a hallucinációkkal, a modellek öregedésével járó „concept drift”¹²⁰ és a kevésbé ismert támadások osztályozásakor mutatózó teljesítmény továbbra is aggodalomra ad okot.

A triázs-munkafolyamat javításának másik érintőleges megközelítése nem az elemzők döntéshozatalának automatizálással való helyettesítése, hanem inkább az emberi elemzők képzettségének növelése. Ez könnyen megvalósítható a szituációs tanulás alkalmazásával, amely a biztonsági elemzőket valós forgatókönyvek alapján gyakorlati feladatokkal látja el. A nagy nyelvi modellek alkalmazásával az oktatók változatos szituációs feladatokat hozhatnak létre pillanatok alatt, amelyeket konkrét kompetenciabeli hiányosságokhoz és a szervezeti követelményekhez igazítanak. Egy tanulmány megállapította, hogy a feladatok generálásával az oktatók nemcsak jelentős időmegtakarítást értek el, hanem azok a hallgatók, akik nagyobb számú LLM által generált forgatókönyvvel dolgoztak, jobb tanulási eredményeket értek el, mint azok a hallgatók, akik csak egy kézzel létrehozott szcenárió alapján tettek.¹²¹ Ez az oktatási módszer segíthet abban is, hogy a kezdő elemzők a felvételt követően gyorsan beilleszkedjenek a munkába.¹²² Hasonló módon a mesterséges intelligencia NLP képességei felhasználhatók egy olyan belső tudásbázis létrehozására is, amely konkrét információkat tartalmaz a szervezet infrastruktúrájáról, és az azon belül ismert viselkedésformákról. Ezt a nagy nyelvi modell alapú tudásbázist az elemzők használhatják a riasztással kapcsolatos kontextuális információk lekérdezésére. Ez is különösen hasznos lenne az újonnan belépők számára, akiknek nincs sok ismeretük a szervezet infrastruktúrájáról, és jelentősen csökkenthetné az elemzők információkereséssel és más elemzőkkel való kapcsolatfelvétellel töltött idejét.¹²³

¹¹⁷ SINGH Yuvraj et al.: Enhancing Security Operations Center Efficiency through Multi-Model Integration of Large Language Models and SIEM Systems. *International Journal of Information Security*, é.n., 1-26. o.

¹¹⁸ Uo.

¹¹⁹ Uo.

¹²⁰ concept drift – amikor a prediktív modellek alapjául szolgáló adatok statisztikai tulajdonságai idővel megváltoznak, ami ronthatja a modell pontosságát

¹²¹ SHCHAVINSKY Yurii et al.: Application of Artificial Intelligence for Improving Situational Training of Cybersecurity Specialists. *Information Technologies and Learning Tools*, 2023/97. 1-10. o.

¹²² GUPTA Maanak et al.: From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access*, 2023/11, 17. o.

¹²³ CHUI 2023.

Potenciális problémák

Az áttekintés korábbi szakaszaiban számos olyan jelenlegi kutatási került feltárássra, amelyek célja a modern SOC-ok problémáinak megoldása. Ezen irányok közül sok rendkívül ígéretes a potenciális hatékonyságnövekedés szempontjából. Ugyanakkor számos lehetséges probléma is felmerülhet e technológia alkalmazásával kapcsolatban. Az egyik ilyen probléma az, hogy még a legjobb kognitív számítástechnikai megközelítések is hajlamosak hibázni. Minden mesterségesintelligencia-alapú megközelítésben léteznek osztályozási elfogultságok, a nagy nyelvi modellek hallucinációi pedig különösen látványosak és veszélyesek. Az osztályozási hibák elkövetésének vagy az elemzők egyéb módon történő félrevezetésének költségei jelentősek, mivel olyan sikeres kibertámadásokhoz vezethetnek, amelyek megkerülik a SOC felügyeletét. Eközben a hamis pozitív eredményeket eredményező osztályozási hibák az elemzők bizalmát is csökkentik, és újra előidéznek az „alert fatigue” problémáját.

Egy másik jól ismert jelenség, hogy az elemzők hajlamosak túlzottan az automatizált rendszerekre hagyatkozni, és gyakran nem keresnek megerősítő vagy ellentmondó bizonyítékokat a rendszer kimenetein túl.¹²⁴ Ezt a jelenséget súlyosítja az automatizált folyamatok gyorsasága és vélt hatékonysága, ami arra késztetheti az elemzőket, hogy a gyors válaszokat előnyben részesítsék az eredmények alapos validálásával szemben. Ehhez szorosan kapcsolódik az automatizálási elbizakodottság, amikor az automatizálásba vetett bizalom csökkenti az emberi éberséget és az automatizált rendszerek kritikus felügyeletét. Ez a teljesítmény csökkenéséhez vezethet, amikor az elemzők valamilyen technikai probléma miatt már nem támaszkodhatnak az automatizálásra. Ezek a viselkedésbeli változások különösen problematikusak, mivel a kognitív számítástechnikai eszközök szenvedhetnek a korábban említett osztályozási elfogultságok és hallucinációk korlátaitól.

Ezt a problémát tovább súlyosítja a legtöbb jelenlegi kognitív számítástechnikai megközelítés átláthatatlan jellege. Más szavakkal, az elemzők nem látják át azokat a döntéshozatali folyamatokat, amelyek egy adott osztályozáshoz vezetnek. Ezáltal korlátozva az elemzők képességét, hogy a megállapítások alapján hatékonyan cselekedjenek.¹²⁵ Ha az „alert fatigue” és a döntéshozatali idő csökkentésére törekedve olyan rendszert vezetünk be, amely érthetetlen döntéseket hoz, akkor csak egy jól ismert problémát cserélnénk le egy még összetettebb, átláthatatlanabb problémára. A szakirodalmi áttekintésben részletezett egyik megoldási javaslat erre a problémára az XAI alkalmazása volt. Ez a technológia azonban saját járulékos problémákkal is jár, ha nem megfelelően alkalmazzák.

¹²⁴ TILBURY Jack – FLOWERDAY Stephen: Automation Bias and Complacency in Security Operation Centers. *Computers*, 2024/13., 2. o.

¹²⁵ FAHEEM Muhammad Ashraf et al.: The Role of Explainable AI in Cybersecurity: Improving Analyst Trust in Automated Threat Assessment Systems. *Iconic Research And Engineering Journals*, 2022/4., 2. o.

Egy kutatási projekt, amelynek célja a megmagyarázható mesterséges intelligencia hatékonyságának tesztelése volt egy valós környezetben, jelentős problémákat talált a használhatóságával kapcsolatban. Az elemzők ritkán foglalkoztak az XAI-eszközzel, még az ismeretszerzést elősegítő tréningek után is. Ez a korlátozott elkötelezettség elsősorban annak tudható be, hogy az eszköz nem integrálódott az elsődleges eseménykezelő rendszereikbe, ami arra kényszerítette az elemzőket, hogy a platformok között ingázzanak, megzavarva ezzel a munkafolyamatokat. Ezen kívül az eszköz nem egészítette ki a meglévő eszközök által nyújtott kontextuális jelzéseket, amelyekben az elemzők jobban bíztak a döntéshozatal során. A legrosszabb problémát az XAI-eszköz által nyújtott magyarázatok jelentették. A rendszer a bemeneti attribútumok fontosságának vizualizációját használta annak bemutatására, hogy mely bemenetek járultak hozzá leginkább a döntéshez (TreeSHAP¹²⁶). Ez nem felelt meg az elemzők kognitív követelményeinek, mivel nem tartalmazott olyan lényeges kontextuális részleteket, mint a döntések bizalmi szintjei vagy a döntésekhez hozzájáruló attribútumok egyértelmű (azaz ember által érhető) meghatározása.¹²⁷ A jelenlegi megmagyarázható mesterségesintelligencia-megközelítések alapvető problémája az osztályozás mögötti döntési folyamat intuitív közvetítése.

Az eddig ismertett problémák mindegyikét súlyosbítja a „concept drift”, azaz a döntések minőségének csökkenése, amelyet a szervezeteket célzó fenyegetések gyors változása idéz elő. Naponta jelennek meg új kritikus sebezhetőségek és támadási vektorok, ami nem fér össze azzal, ahogyan a legtöbb kognitív számítástechnikai rendszert létrehozzák és karbantartják. Ezért a kognitív számítástechnikai modellek folyamatos képzése és frissítése szükséges ahhoz, hogy azok hatékonyak maradjanak.¹²⁸ Az ehhez szükséges adatkészleteket azonban nem könnyű beszerezni. Ez részben annak köszönhető, hogy a biztonsági elemzők kognitív folyamatainak szimulálása különösen nagy kihívást jelent. Az összetett biztonsági incidensek pontos kezelése több éves tapasztalatot igényel, és nagy kognitív terhet jelent az emberi elemzők számára. Az ilyen összetett triázstevékenységekből származó adatkészletek létrehozása további terhet jelent a meglévő elemzők munkaterhelésén felül.

A modellek tanításához használt triáz adatoknak az adott környezetre specifikusnak kell lenniük, vagy az osztályozási modellnek nagyon jól általánosíthatónak kell lennie.¹²⁹ Mindkét esetben ahhoz, hogy egy kognitív számítástechnikai rendszer a „concept drift”-et megelőzze, a modell karbantartóinak vagy az azt használó biztonsági csapatoknak folyamatosan új támadásokat kellene szimulálniuk a modell újratanítása érdekében. E kihívás megoldásának egyik alternatívája, hogy a nagy ügyfélkörrel rendelkező vállalati megoldások fenntartói aggregálják a triáz adatokat a különböző

¹²⁶ TreeSHAP – egy magyarázó módszer, amely a döntési fákból egyes bemeneti változók döntési eredményre gyakorolt hozzájárulását számszerűsíti

¹²⁷ NYRE-YU Megan et al.: Explainable AI in Cybersecurity Operations: Lessons Learned from xAI Tool Deployment. Előadás: *Usable Security and Privacy (USEC) Symposium*. USEC, San Diego, 2022. 04. 28.

¹²⁸ SARKER 2024, 196.

¹²⁹ SARKER Iqbal: Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. *Annals of Data Science*, 2023/10. 20. o.

ügyfélkörnyezetekből. Ezen adatkészletek összegyűjtésével a karbantartók újra taníthatják a modelleket, ezáltal az új modell jobban figyelembe fogja venni az új támadási vektorokat. Az ilyen adatvezérelt megoldásokban rejltő lehetőségek ellenére azonban továbbra is az emberek kreativitására és árnyalt ítélőképességére van szükség az új vagy kifinomult támadások felismeréséhez és osztályozásához, hogy azokat hozzá lehessen adni a tanítási adatkészletekhez.¹³⁰

Bármilyen fejlettek is lesznek a modellek, alapvetően az emberi szakértelemre támaszkodnak a támadási minták azonosításában, az incidensek kontextusba helyezésében és a kétértelmű riasztásokban való döntéshozatalban. Ez az emberi bemenetre való támaszkodás önfenntartó problémát okoz. Az emberi incidenskezelésből adódó munkaterhelés már így is túl nagy, ami az automatizálás szükségességét ösztönzi. A hatékony automatizáláshoz megbízható és reprezentatív képzési adatokra van szükség. E képzési adatok előállítására jelentős emberi felügyeletet igényel, ami növeli az elemzők terheit és állandósítja az eredeti munkaterhelési problémát.

Az ezen operatív kérdések kezelésére szolgáló fejlettebb modellek futtatása valószínűleg még számításigényesebb lesz, mint a jelenlegi megközelítések, amelyek már most is jelentősek.¹³¹ Ha a korábban említett elégtelen adatkészletekkel kapcsolatos problémák megoldhatók, a kellően összetett modellek képzése olyan hardver-és energiaköltségeket igényelhet, amelyek megfizethetetlenek lehetnek. Bár egy modell használata általában lényegesen kevésbé erőforrásigényes, mint a tanítása, egy összetett modell esetén a költségek elriaszthatják azokat a szervezeteket, amelyek egyébként nyitottak lennének az ilyen technológia bevezetésére. Más skálázhatósági problémák is felmerülhetnek, például az, hogy a bonyolultabb modellek több időt igényelnek a számítások elvégzéséhez, ami késleltetést eredményezhet olyan folyamatokban, ahol azonnali reakcióra és a riasztások megfelelő mennyiségű feldolgozására van szükség.

Végezetül van egy másik problémakör, mégpedig az ellenséges gépi tanulás. A támadók már régóta alkalmaznak taktikákat a biztonsági elemzők megtévesztésére az általuk kiváltott riasztásokban. Például amikor egy C2¹³² jeladó ütemezett feladatként történő telepítésével perzisztenciát hoz létre, azt egy jól ismert böngésző frissítési folyamatának nevezheti el. A rosszindulatú folyamat által kiváltott riasztásokat figyelmen kívül hagyhatják az elemzők, akik összetévesztik a legitim böngészőfrissítési folyamattal. Ilyen és sok más támadás létezik a kognitív számítástechnikai rendszerek ellen is.

¹³⁰ BASTA 2024, 219-220.

¹³¹ JADA Irshaad – MAYAYISE Thembekile: The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, 2024/8. 7. o.

¹³² C2 – Command and Control – támadók által használt kommunikációs infrastruktúra

A támadások a rendszer életciklusának betanítási és használati szakaszát egyaránt célba vehetik. A tanítás során mérgezési támadásokkal veszélyeztethető a modell integritása azáltal, hogy manipulálják a képzési adatokat, hátsó ajtókat vagy elfogultságokat létrehozva, amelyeket később ki lehet használni.¹³³ A kikerülő és injekciós támadások gondosan megtervezett rosszindulatú bemeneteket használnak, amelyek célja, hogy hibás predikciókat vagy téves klasszifikációt idézzenek elő.¹³⁴ A funkcionális extrakciós támadások lehetővé teszik a támadók számára a modellek replikálását kiterjedt lekérdezések segítségével, míg az inverziós támadások célja az érzékeny képzési adatok rekonstruálása és potenciálisan új lehetőségek azonosítása a súlyosabb injekciós vagy kikerülő támadásokhoz. Attól függően, hogy a támadók milyen típusú hozzáféréssel rendelkeznek, hardveralapú fenyegetéseket alkalmazhatnak. Ezek közé tartoznak az *side-channel*¹³⁵ és a hibainjekciós támadások, amelyek a kognitív számítástechnikai rendszerek fizikai infrastruktúrájának sebezhetőségeit használják ki.¹³⁶

Értékelés és kutatási irányok

Az áttekintett kutatások kiemelik a kognitív számítástechnikában rejlő átalakító potenciált a SOC-ok hatékonysági hiányosságainak kezelésében. Az észlelés utáni folyamatok automatizálása, beleértve a triázs és a döntéshozatali munkafolyamatokat, a kibbiztonság következő korszakát jelenti. A már elért eredmények ellenére számos megoldatlan kihívás rávilágít a további vizsgálatokat és innovációt igénylő területekre.

Az egyik legsürgetőbb kihívás a kognitív számítástechnikai rendszerek növekvő sebezhetősége az ellenséges támadásokkal szemben. Ahogy ezek a rendszerek egyre kifinomultabbá válnak, úgy nő a támadók lehetősége arra, hogy olyan nüanszokat fedezzenek fel, amelyek veszélyeztetik a működő rendszerek biztonságát. Ezek a támadások a gépi tanulási rendszerek betanítási és használati szakaszait is célba vehetik. Befolyásolhatják az automatikus incidencosztályozást, vagy a kognitív számítástechnikával támogatott elemzőket téves következtetések felé terelhetik. Számos gépi tanulási modellek átláthatatlan jellege súlyosbítja ezt a problémát, mivel az elemzők nem rendelkeznek megfelelő eszközökkel a mesterséges intelligencia által generált kimenetek vizsgálatához és validálásához. Nagyobb átláthatóság nélkül a támadók viszonylag könnyen kihasználhatják ezeket a rendszereket, ami megingatja az automatizálásba vetett bizalmat a SOC-környezetekben.

A megmagyarázható mesterséges intelligencia ígéretes megoldásként jelenik meg a kognitív számítástechnika átláthatatlanságának enyhítésére. Azáltal, hogy betekintést nyújt a döntések meghozatalának módjába, az XAI erősítheti az elemzők bizalmát a

¹³³ TADDEO Mariarosaria et al.: Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, 2019/1., 2-3. o.

¹³⁴ ANSARULLAH Syed Immamul et al.: AI-powered strategies for advanced malware detection and prevention. *The Art of Cyber Defense*, CRC Press, Boca Raton, 2024, 49. o.

¹³⁵ *side-channel* – egy olyan támadási módszer, amely a célrendszer viselkedéséből származó közvetett információk alapján dolgozik

¹³⁶ WONG Lily: AI Security 101. MITRE Corporation, 2024. November 1.

kognitív számítástechnikai ajánlásokban, és megkönnyítheti a kognitív rendszerek integrálását a SOC-munkafolyamatokba. A meglévő megmagyarázható mesterségesintelligencia-megoldások azonban továbbra sem megfelelőek. A legtöbb jelenlegi módszer csupán azokat a bemeneti jellemzőket emeli ki, amelyek a leginkább hozzájárultak a döntéshez. Ez olyan megközelítés, amely nem rendelkezik a gyakorlati alkalmazáshoz szükséges kontextuális gazdagsággal és mélységgel. Ahhoz, hogy az elemzők bizalmát elnyerjék, az XAI-rendszereknek fejlődniük kell, hogy részletes, használható érvelést nyújtsanak, amely összhangban van az elemzők kognitív munkafolyamatával és operatív igényeivel.

Amíg ilyen alapvető technikai fejlesztéseket nem hajtanak végre a megmagyarázható mesterséges intelligenciák esetében, a kognitív számítástechnika fejlődését elősegíthetné az LLM-ek relatív hatékonyságának vizsgálata a kiberbiztonság specifikus gépi tanulási modellekkel szemben SOC-környezetekben. A generatív mesterséges intelligencia, a nagy nyelvi modellek, illetve a legújabb neurális hálózati architektúrák és figyelmi mechanizmusok által hozott innováció még nem realizálódott teljes mértékben a kiberbiztonság kontextusában. Még a Microsoft Security Copilot (amely az egyik piacvezetőnek számít) sem használ nagy nyelvi modelleket számos biztonsági célú munkamenethez, ehelyett hagyományosabb gépi tanulási megközelítéseket alkalmaz. A generatív mesterséges intelligencia fellendülése megmutatta, hogy a neurális hálózatok milyen potenciállal rendelkeznek az emberi kognitív folyamatok szimulálásában, amikor kifürkészhetetlenül nagy adathalmazokból tanulnak. Ezek az adatkészletek azonban jelenleg nem állnak rendelkezésre a kiberbiztonságra jellemző kontextusokban. Így a közhasznált nagy nyelvi modellek előnye a hatalmas általános tudás és a rugalmasság, de hiányzik belőlük az árnyalt kiberbiztonsági feladatokhoz szükséges területspecifikusság. Ezzel szemben a specializált gépi tanulási modellek szűken meghatározott feladatokban jeleskednek, de a skálázhatósággal és az általánosíthatósággal küzdenek a valós SOC-kontextusokban. A jövőbeli kutatásoknak össze kell hasonlítaniuk ezeket a megközelítéseket, különösen az olyan feladatok esetében, mint az incidensek klasszifikációja és a triázs elősegítése.

Míg az általános nagy nyelvi modellek ígéretesnek tűnnek, a kognitív számítástechnika hosszú távú jövőképe a SOC-okban a területspecifikus LLM-szerű rendszerek kifejlesztésében rejlik. Ezek a modellek kiterjedt, jó minőségű kiberbiztonsági adathalmazok létrehozását igényelnék, amelyek jelenleg nem léteznek. A kutatásoknak fel kell tárniuk ezen adatkészletek és a megfelelő modellek létrehozásának megvalósíthatóságát, amelyeknek valószínűleg túl kell lépniük a generatív mesterséges intelligencia által használt szövegalapú megközelítéseken. Ehelyett a kiberbiztonsági incidensek adatainak és a kontextuális információkat tartalmazó beágyazásoknak a szerializálására szolgáló robusztus keretrendszer kell kidolgozni. Ennek a szabványnak egyszerre kell hatékonynak és bővíthetőnek lennie a különböző incidenstípusok befogadására. Még ez esetben is, egy ilyen kifinomult, szakterület-specifikus kognitív számítástechnikai modell inkább az emberi elemzők kiegészítésére szolgálhat, mintsem teljes helyettesítésére.

A kognitív számítástechnikai rendszerek fejlesztéséhez és karbantartásához szükséges adathalmazok gyűjtése egy önfenntartó kihívás. A SOC-oknak egyre inkább az automatizálásra kell támaszkodniuk az elemzői munkaterhelés enyhítése érdekében, ugyanakkor a „concept drift”-et ellenálló kognitív számítástechnikai rendszerek létrehozása és karbantartása jelentős emberi erőfeszítést igényel. Ez a paradox helyzet kiemeli az adatgyűjtés és a modelltanítás innovatív megközelítéseinek szükségességét. Olyan technikákat kell feltárni, amelyek a hagyományos felügyelt és transzfer tanulási módszereknél automatizáltabb megközelítéseket tesznek lehetővé, amelyek csökkenthetik a kézzel összeállított adathalmazoktól való függőséget, lehetővé téve a fenntarthatóbb rendszerfejlesztést.

Egy másik kritikus kérdés a tudományos kutatás és a gyakorlati üzleti megoldások közötti tartós megosztottság. A tudományos tanulmányok gyakran a magasan specializált gépi tanulási modelleket vagy koncepcionális keretrendszereket helyezik előtérbe. Bár értékesek, ezeket a tanulmányokat gyakran kontrollált környezetben, gondozott adathalmazok felhasználásával validálják, amelyek nem képesek reprodukálni az üzemelő SOC-ok kiszámíthatatlan és heterogén természetét. Emellett jelentősen korlátozott költségvetéssel és a kereskedelmi eszközök fejlesztői számára biztosított valós használati telemetriához való hozzáférés nélkül végzik őket. Ezzel szemben a piaci megoldások a skálázhatóságot, az integrációt és a működési hatékonyságot helyezik előtérbe, de gyakran feláldozzák az átláthatóságot, a részletességet és néha még a használhatóságot is. Egy tanulmány feltérképezte a technikai jellegű kiberbiztonsági személyzet és a kiberbiztonsággal foglalkozó vezetők által végzett ismétlődő feladatokat. Kimutatta, hogy a technikai személyzet által végzett összes feladatnak volt kapcsolódó kognitív számítástechnikai segédeszköze, míg a 17 vezetői feladtból 11-nek volt automatizálást lehetővé tevő terméke.¹³⁷ Figyelemre méltó, hogy e feladatok közül soknak több olyan eszköze is van, amelyek automatizálási lehetőséget ígérnek. Ezek az eszközök, bár potenciális előnyöket jelentenek, komoly kockázatokat is hordoznak, amelyeket harmadik felek vagy tudományos kutatások továbbra sem vizsgálnak kellőképpen. A kognitív számítástechnikát támogató termékek széles körű megjelenésével az iparági és a tudományos élet közötti különbségek áthidalása kulcsfontosságú a kognitív számítástechnika gyakorlati alkalmazásának előrelépéséhez. A jövőbeli kutatásoknak olyan standardizált keretrendszer kidolgozására kell koncentrálniuk, amely az üzleti megoldásokat tudományos keretek között alaposan értékeli, és biztosítja, hogy a gyakorlati eszközök empirikusan validáltak legyenek.

Ezekkel a kutatási irányokkal foglalkozva a kiberbiztonság területe közelebb kerülhet a kognitív számítástechnikában rejlő teljes potenciál kihasználásához a SOC-okban. Bár továbbra is jelentős kihívások állnak fenn, a technológiai fejlődés gyors üteme optimizmusra ad okot, hogy ezek az akadályok leküzdhetők.

¹³⁷ GAFNI Ruti – LEVY Yair: The role of artificial intelligence (AI) in improving technical and managerial cybersecurity tasks' efficiency. *Information and Computer Security*, 2024/32. 711–728. o.

Felhasznált irodalom:

AGYEPONG Enoch – CHERDANTSEVA Yulia – REINECKE Philipp – BURNAP Pete: Challenges and performance metrics for security operations center analysts: a systematic review. *Journal of Cyber Security Technology*, 2020/4., 11-21. o. DOI: 10.1080/23742917.2019.1698178

AL-HAJIA Qasem Abu: Human factors in cyber defense. *The Art of Cyber Defense: From Risk Assessment to Threat Intelligence*, CRC Press, Boca Raton, 2024. 396-401. o. ISBN: 978-1-032-71480-6

ANSARULLAH Syed Immamul – WAHID Abdul Wali – RASHEED Irshad – ZADA Peer Rayees: AI-powered strategies for advanced malware detection and prevention. *The Art of Cyber Defense*. CRC Press, Boca Raton, 2024, 49. o. ISBN: 978-1-032-71480-6

BAKKER Pascal: Automating the Cybersecurity Triage Process. Előadás: *Twente Student Conference on IT*. University of Twente, Twente, 2024. július 5.

BASTA Alfred – BASTA Nadine – ANWAR Waqar – ESSAR Mohammad Ilyas: *Open-Source Security Operations Center (SOC): A Complete Guide to Establishing, Managing, and Maintaining a Modern SOC*. John Wiley & Sons, New Jersey, 2024. 46-383. o. ISBN: 978-1-394-20162-4

BERZSENYI Dániel – GYARAKI Réka – HÁMORNIK Balázs Péter – HIRSCH Gábor – KISS Attila – MARSÍ Tamás – ORBÓK Ákos – SIMON Béla – SOLYMOS Ákos – TIKOS Anita – ZSÍROS Péter: *Incidentsmenedzsment*. Dialóg Campus Kiadó, Budapest, 2017. 119-120. o. ISBN: 978-615-5764-99-8

BRIDGES Robert – RICE Ashley – OESCH Sean – NICHOLS Jeffrey – WATSON Cory – SPAKES Kevin – NOREM Savannah – HUETTEL Mike – JEWELL Brian – WEBER Brian – GANNON Connor – BIZOVI Olivia – HOLLIFIELD Samuel – SAMANTHA Erwin: Testing SOAR tools in use. *Computers Security*, 2023/129. 15-16. o. DOI: 10.1016/j.cose.2023.103201

CHHETRI Mohan Baruwal – TARIQ Shahroz – SINGH Ronal – JALALVAND Fatemeh – PARIS Cecile – NEPAL Surya: Towards Human-AI Teaming to Mitigate Alert Fatigue in Security Operations Centres. *ACM Transactions on Internet Technology*, 2024/3. 1-22. o. DOI: 10.1145/3670009

CHUI Michael – HAZAN Eric – ROBERTS Roger – SINGLA Alex – SMAJE Kate – SUKHAREVSKY Alex – YEE Lareina – RODNEY Zimmel: The economic potential of generative AI: The next productivity frontier. McKinsey & Company, 2023. Elérhető: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#introduction> (Letöltés ideje: 2025. 01. 04.)

FAHEEM Muhammad Ashraf – KAKOLU Sridevi – ASLAM Muhammad: The Role of Explainable AI in Cybersecurity: Improving Analyst Trust in Automated Threat Assessment Systems. *Iconic Research And Engineering Journals*, 2022/4., DOI: 10.13140/RG.2.2.13984.39685

FREITAS Scott – KALAJDIESKI Jovan – GHARIB Amir – MCCANN Robert: AI-Driven Guided Response for Security Operation Centers with Microsoft Copilot for Security. h.n., 2024, 1-10. DOI: 10.48550/arXiv.2407.09017

FURNELL Steven: The cybersecurity workforce and skills. *Computers & Security*, 2021/100. DOI: 10.1016/j.cose.2020.102080

GAFNI Ruti – LEVY Yair: The role of artificial intelligence (AI) in improving technical and managerial cybersecurity tasks' efficiency. *Information and Computer Security*, 2024/32. 711–728. o. DOI: 10.1108/ics-04-2024-0102

GOPAL Deepti – MCMULLEN Leigh – WALLS Andrew – ADDISCOTT Richard – FURTADO Paul – PORTER Craig – ISAKA Oscar – CHARLIE Winckless: Predicts 2023: *Cybersecurity Industry Focuses on the Human Deal*. *Gartner*, 2023 Elérhető: <https://www.gartner.com/en/documents/4023308> (Letöltve 2025. 01. 03.)

GUPTA Maanak – AKIRI Charankumar – ARYAL Kshitiz – PARKER Eli – LOPAMUDRA Praharaj: From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access*, 2023/11., 17. o. DOI: 10.1109/ACCESS.2023.3300381

HATZIVASILIS George – IOANNIDIS Sotiris – SMYRLIS Michail – SPANOUDAKIS George – FRATI Fulvio – GOEKE Ludger – HILDEBRANDT Torsten – TSAKIRAKIS George – OIKONOMOU Fotis – LEFTHERIOTIS George – HRISTO Koshutansk: Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Applied Sciences*, 2020/10. DOI: 10.3390/app10165702

HOLDER Eric – WANG Ning: Explainable artificial intelligence (XAI) interactively working with humans as a junior cyber analyst. *Human-Intelligent Systems Integration*, 2021/3. DOI: 10.1007/s42454-020-00021-z

HÁMORNIK Balázs Péter – KRASZNAV Csaba: A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers. Előadás: *International Conference on Applied Human Factors and Ergonomics*. Los Angeles, 2017. július 20.

JADA Irshaad – MAYAYISE ThembeKile: The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, 2024/8. DOI: 10.1016/j.dim.2023.100063

KEARNEY Paul – ABDELSAMEA Mohammed – SCHMOOR Xavier – SHAH Fayyaz – IAN Vickers: Combating Alert Fatigue in the Security Operations Centre. *SSRN Electronic Journal*, 2023, 1-34. o. DOI: 10.2139/ssrn.4633965

KNERLER Kathryn – PARKER Ingrid: *11 Strategies of a World-Class Cybersecurity Operations Center*. The MITRE Corporation, Bedford, 2022. 65-67. o. ISBN: 979-8-9856450-7-1

LAWSON Craig – SHOARD Pete: Market Guide for Security Orchestration, Automation and Response Solutions. *Gartner*, 2023. Elérhető: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1kfPW> (Letöltés ideje: 2025. 01. 04.)

MALACH Alon – WUDALI Prasanna – MOMIYAMA Satoru – FURUKAWA Jun – ARAKI Toshinori – ELOVICI Yuval – ASAF Shabtai: CyberShapley: Explanation, prioritization, and triage of cybersecurity alerts using informative graph representation. *Computers & Security*, 2024, 1-14. o. DOI: 10.1016/j.cose.2024.104270

MUGHAL Arif Ali: Building and Securing the Modern Security Operations Center (SOC). *International Journal of Business Intelligence and Big Data Analytics*, 2022/5. 10-11. o.

NOBLES Calvin: Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *HOLISTICA – Journal of Business and Public Administration*, 2022/13. 6-15. o. DOI: 10.2478/hjbpa-2022-0003

NTALAMPIRAS, Stavros – MISURACA Gianluca – ROSSEL Pierre: Artificial intelligence and cybersecurity research – ENISA research and innovation Brief. European Union Agency for Cybersecurity, Athens, 2023. 06. 07. Elérhető: <https://www.enisa.europa.eu/sites/default/files/publications/Artificial%20Intelligence%20and%20Cybersecurity%20Research.pdf> (Letöltés ideje: 2025. 01. 04.)

NYRE-YU Megan – MORRIS Elizabeth – SMITH Michael – MOSS Blake – CHARLES Smutz: Explainable AI in Cybersecurity Operations: Lessons Learned from xAI Tool Deployment. Előadás: *Usable Security and Privacy (USEC) Symposium*. USEC, San Diego, 2022. 04. 28

PAWAR Shekar: Role Of Authentication, Role Management & Access Control as Integral Part Of SOC Capabilities. EC-Council, 2023. 08. 16 Elérhető: <https://www.eccouncil.org/cybersecurity-exchange/security-operation-center/role-of-authentication-access-management-in-soc/>. (Letöltés ideje: 2025. 03. 13.)

RAFIEY Pasha – NAMADCHIAN Amin: Using LLMs as AI Agents to Identify False Positive Alerts in Security Operation Center. *International Journal of Information Security*, é.n., 1-15. o. DOI: 10.21203/rs.3.rs-5420741/v1

RAHMAN Abdul: *A Qualitative Study on The Reduction of Dwell Time Exceeding 200 Days*. PhD-disszertáció. Capella University School of Business, Technology and Health Care Administration, 2024. 13-39. o.

REUTHER Albert – MICHALEAS Peter – JONES Michael – GADEPALLY Vijay – SAMSI Siddharth – JEREMY Kepner: AI and ML Accelerator Survey and Trends. Előadás: *IEEE High Performance Extreme Computing Conference (HPEC)*. IEEE, Waltham, 2022. 09. 21.

ROGERS Liz: Bringing the Security Analyst into the Loop: From Human-Computer Interaction to Human-Computer Collaboration. Előadás: *Ethnographic Praxis in Industry Conference Proceedings*. EPIC, Providence 2019. 11. 11.

SALEM Aya – AZZAM Safaa – EMAM Osama – ABOHANY Amr: Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, 2024/11, 1-34. o. DOI: 10.1186/s40537-024-00957-y

SARKER Iqbal: AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability. *Springer Nature Switzerland*, Cham, 2024. 28-196. o. DOI: 10.1007/978-3-031-54497-2

SARKER Iqbal: Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. *Annals of Data Science*, 2023/10. DOI: 10.1007/s40745-022-00444-2

SHCHAVINSKY Yurii – MUZHANOVA Tetiana – YAKYMENKO Yuriy – ZAPOROZHCHENKO Mykhailo: Application of Artificial Intelligence for Improving Situational Training of Cybersecurity Specialists. *Information Technologies and Learning Tools*, 2023/97. 1-10. o. DOI: 10.33407/itlt.v97i5.5424

SINGH Yuvraj – PATEL Narottam Das – SHANDILYA Shishir Kumar: Enhancing Security Operations Center Efficiency through Multi-Model Integration of Large Language Models and SIEM Systems. *International Journal of Information Security*, é.n., 1-26. o. DOI: 10.21203/rs.3.rs-5615639/v1

Sz.n.: AI in Cybersecurity: Define Your Direction. Gartner, 2024. Elérhető: <https://emt.gartnerweb.com/ngw/globalassets/en/cybersecurity/documents/ai-in-cybersecurity-define-your-direction.pdf> (Letöltés ideje: 2025. 01. 04.)

Sz.n.: Cyber Resilient Organization Report 2020. IBM, 2020. Elérhető: <https://www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/#/> (Letöltés ideje: 2025. 01. 03.)

Sz.n.: Cybersecurity Workforce Study. ISC2, 2024. Elérhető: <https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study>. (Letöltés ideje: 2024. 12. 28.)

Sz.n.: Global Security Operations Center Study Results. IBM, 2023. Elérhető: <https://www.ibm.com/downloads/documents/us-en/10c31775a05401a5> (Letöltés ideje: 2024. 12. 28)

Sz.n.: How to Become a SOC Analyst. SANS, 2024. 07. 16. Elérhető: <https://www.sans.org/blog/how-to-become-a-soc-analyst/>. (Letöltés ideje: 2025. 03. 13.)

Sz.n.: QRadar Advisor With Watson - v7.5.0+. IBM, 2023. 04. 26. Elérhető: <https://exchange.xforce.ibmcloud.com/hub/extension/7f9a33b3090e223aaa56868d961f0fc3> (Letöltés ideje: 2024. 12. 28.)

Sz.n.: State of Cybersecurity 2023. ISACA, 2023. Elérhető: https://www.isaca.org/resources/reports/state-of-cybersecurity-2023?utm_campaign=ISACA+Main&utm_content=1696361826&utm_medium=social&utm_source=twitter&tfa_next=/responses/last_success?jsid=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJmVhbnZlODQ5ODM1MzE3NTM3NDZhNmMyNDZlZTY1Ilg.hXEmj5sg4A6WtxVehKQ-rAhASiYvawyGoZ_5GpVmp8#LeadForm (Letöltés ideje: 2025. 01. 02.)

Sz.n.: The 2020 State Of Security Operations. Forrester, 2020. Elérhető: <https://www.itsecuritydemand.com/whitepaper/security/2020-forrester-state-of-security-operations/> (Letöltés ideje: 2024. 12. 28)

TADDEO Mariarosaria – MCCUTCHEON Tom – FLORIDI Luciano: Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, 2019/1, 2-3. o. DOI: 10.1038/s42256-019-0109-1

TILBURY Jack – FLOWERDAY Stephen: Automation Bias and Complacency in Security Operation Centers. *Computers*, 2024/13, 2. o. DOI: 10.3390/computers13070165

VIELBERTH Manfred – BÖHM Fabian – FICHTINGER Ines – PERNUL Günther: Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, 2020/8, 8-18. o. DOI: 10.1109/ACCESS.2020.3045514

WONG Lily: AI Security 101. MITRE Corporation, 2024. November 1. Elérhető: <https://github.com/mitre-atlas/atlas-website/blob/main/public/content/ai-security-101.md> (Letöltés ideje: 2025. 01. 02.)

ZHANG Zhibo – HAMADI Hussam Al – DAMIANI Ernesto – YEUN Chan Yeob – TAHER Fatma: Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access*, 2022. 1-36. o. DOI: 10.1109/ACCESS.2022.3204051

A KIBERTÉRI MŰVELETEK FEJLŐDÉSÉNEK ÁTTEKINTŐ VIZSGÁLATA A MEGVÁLTOZOTT NEMZETKÖZI RENDSZER TÜKRÉBEN

A XXI. században az országok között vívott háborús konfliktusok során megjelent formaként tekintettünk a hibrid háborúra. A hibrid háború során alkalmazott módszerek kiterjednek a kibertér használatára is, amely proxyháborúként tekintve indirekt beavatkozásra ad lehetőséget. A kibertér háborús irányba történő használata folyamatos módosulást mutat az információs társadalomba betöltött szerepének változásával párhuzamosan. Az időszak legjelentősebb, orosz–ukrán konfliktusa is rámutatott, hogy a két szembenálló fél eltérő módszereket alkalmaz a siker kivívásának érdekében, illetve a konfliktus elhúzódása is folyamatos átalakulást mutat. A háborút megelőző, illetve annak során alkalmazott kibertéri eljárások változnak, ezzel is erősítve a hibridjellegét, és fegyelembé véve a terület nemzetközi értelmezését.

Kulcsszavak: kibertér, kiberművelet, hibrid háború, proxyháború, nemzetközi konfliktus

AN OVERVIEW OF THE EVOLUTION OF CYBERSPACE OPERATIONS IN THE LIGHT OF THE CHANGED

In the 21st century, we have seen hybrid warfare as an emerging form of war conflicts between countries. The methods used in hybrid warfare include the use of cyberspace, which can be seen as a proxy war for indirect intervention. The use of cyberspace as warfare is more frequent as its role in the information society changed due to the influence of the information society. The most significant conflict of the period, Russia's Ukraine, highlighted this, that the two opposing sides are using different methods to achieve success and the protracted nature of the conflict shows a continuing transformation. The cyberspace procedures before and during the war are changing, reinforcing the hybrid nature and considering the international understanding.

Keywords: cyberspace, cyber operation, hybrid war, proxy war, international conflict

Bevezetés

Az információs és kommunikációs technológiák robbanásszerű fejlődése az elmúlt évtizedekben alapjaiban formálta át mindennapi életünket, gazdaságunkat és nem utolsósorban biztonságpolitikánkat. Az internet és a digitális rendszerek elterjedésével egyre nagyobb jelentőséget kapnak a kibertéri műveletek, amelyek új kihívások elé állítják a nemzetközi közösséget. A kibertéri műveletek nem csupán technológiai újításokat, hanem a nemzetközi rendszer dinamikus változásait is magukban

¹ ORCID-azonosító: 0009-0001-0702-756X

² ORCID-azonosító: 0009-0007-5981-9984

hordozzák, és alapvetően átalakítják a hadviselés, a hírszerzés és a diplomácia hagyományos fogalmait. A kibertéri hadviselés a modern hadviselés egyik legdinamikusabban fejlődő területe, amelyben az információs technológia hatékony alkalmazása révén a konfliktusok új dimenziót nyernek. A kibertér lehetőséget biztosít a szembenálló feleket támogató harmadik szereplő részére az indirekt beavatkozásra azzal a céllal, hogy befolyásolja az általa támogatott fél számára a konfliktus kimenetelét.³ A kiberműveletek céljai változatosak lehetnek a kormányzati rendszerek destabilizálásától kezdve az ipari kémkedésen át az infrastruktúrák megbénításáig. Az információs hadviselés eszköztára széleskörű, az adatlopásoktól és -manipulációktól kezdve a szolgáltatásmegtagadásos támadásokig (DDoS) terjed.

A globalizáció és a digitalizáció folyamatai mélyrehatóan átalakították a nemzetközi kapcsolatok szerkezetét és dinamikáját. Az államok mellett egyre fontosabb szereplővé válnak a nem állami szereplők, köztük a multinacionális vállalatok, a civil szervezetek és a kibertérben tevékenykedő egyének és csoportok. Ezzel párhuzamosan a hagyományos geopolitikai és gazdasági érdekek mellett a kiberbiztonság is központi szerepet kap a nemzetközi politikában. A kibertéri műveletek során szerzett tapasztalatok és technológiai fejlesztések révén az államok képesek lehetnek új stratégiák és taktikai megközelítések kialakítására. Ebben a kontextusban a kiberhadviselés nem csupán a védekezést, hanem az offenzív műveleteket is magában foglalja, amelyek révén az államok képesek lehetnek előnyhöz jutni a nemzetközi konfliktusok során.

A kibertérben zajló műveletek új kihívásokat jelentenek a nemzetközi jog számára is. A hagyományos nemzetközi jogi normák és szabályok gyakran nehezen alkalmazhatók a kibertérre, hiszen az információs hadviselés és a kiberhadviselés számos esetben elmosza a hagyományos háborús és békés időszak közötti határokat. Az államoknak és a nemzetközi közösségnek együtt kell működniük annak érdekében, hogy új jogi kereteket alakítsanak ki, amelyek figyelembe veszik a kibertéri műveletek sajátosságait és kihívásait.

Áttekintés

A XX. századi klasszikus háborús konfliktusok során alkalmazott különböző módszerek változásai kiemelten figyelhetők meg a kibertér alkalmazása során. A 2010-ben STUXNET néven elhíresült első katonai kibertérművelet végrehajtását követően a kibertérműveletek önálló alkalmazása eseti jelleggel történt, valamely más műveleti, így pl. klasszikus szárazföldi, légi műveleti vagy politikai célú diplomáciai tevékenységgel párhuzamosan.

A kibertérműveletek végrehajtása abból a szempontból is átalakul, hogy a kezdetben a rendszerek működését befolyásoló, így az elérést, hozzáférést akadályozó tevékenységek már akár ugyanezt a célt biztosító fizikai károkozást is megvalósító képességgé léptek elő. Kijelenthető, hogy a fizikai károkozás eléggé szélsőséges, és

³ MUMFORD, Andrew: Proxy warfare and the future of conflict. *RUSI Journal*, 2013b/2., 40. o.

kevésbé alkalmazott forma, ami vélhetően a befektetett energia és a szükséges pénzügyi forrás miatt van így.

Az első, hivatalosan is publikált, káros hatás elérése érdekében alkalmazott kód, a „The Reaper” néven vált ismertté, amely az internet elődjének tekintett ARPANET-en terjedt el. A kizárólag egy értesítési üzenetet megjelenítő vírust követően a fejlődés eljutott a végeredményében kibertérműveletként tekinthető „STUXNET” névre keresztelt támadásig. Az elsőhöz képest, amelynél egy személy egy korlátozott cél, a figyelem felhívása érdekében tevékenykedett, az utóbbi művelet egy összehangolt támadás volt. Az amerikai és izraeli kivitelezésű támadás célja az iráni atomképességek és ezeken keresztül az iráni vezetés reputációjának csökkentése volt. A művelet során a kormányzati támogatással végrehajtott feladatok összehangoltan, több atomcentrifugát célozva, egy időben kerültek végrehajtásra, ami több elkövetőt feltételez, akiknek céljuk a nemzeti érdekek érvényesítése volt.

A modern hadviselés és konfliktusok egyre komplexebbé és sokrétűbbé válnak, a hagyományos és nem hagyományos hadviselési módszerek egyesítése új stratégiák és taktikák kialakításához vezet. A hibrid konfliktusok olyan összetett cselekmények, amelyekben egyaránt alkalmazzák a hagyományos katonai erőket, a nem hagyományos taktikákat, valamint az információs és pszichológiai hadviselés eszközeit. Ezen konfliktusok során az államok és a nem állami szereplők egyaránt igyekeznek kihasználni az ellenfelek sebezhetőségeit, és megzavarni azok működését anélkül, hogy nyílt fegyveres összecsapásra kerüljön sor. A hibrid konfliktusok természetének megértése kulcsfontosságú a modern hadviselés és biztonságpolitika szempontjából. Az információs, a gazdasági, a katonai és a nem hagyományos eszközök együttes alkalmazása révén a hibrid konfliktusok új kihívásokat és lehetőségeket teremtenek a nemzetközi közösség számára. A hatékony válaszok és megoldások kidolgozása érdekében elengedhetetlen a hibrid hadviselés elemeinek és dinamikájának alapos megértése, valamint a nemzetközi együttműködés erősítése.

A kibertér, mint a hibrid konfliktusok egyik helyszínének vizsgálata során részben osztjuk Simicskó István a hibrid hadviselésről írt tanulmányában megfogalmazott gondolatait, hogy *„A negyedik generációs modell leírásában – egyebek mellett – olyan jellemzőket találunk, mint az (időközben önálló hadviselési kategóriává fejlődött) aszimmetrikus hadviselés, az a tény, hogy a béke és a háború közötti határ elmosódik, továbbá, hogy nincs felismerhető harctér, nincs hadüzenet. Ezek olyan jellemzők, amelyeket napjainkban legtöbbször a hibrid hadviselés kifejezéshez társítanak.”*⁴

A hibrid háború az indirekt hadviselés egyik formájaként írható le,⁵ amely során az államok más államok ellen nem hagyományos katonai módszereket és megtévesztésre alkalmas eszközöket alkalmaznak. A felhasznált eszközök jellege alapján azonosítható a hibrid háborúk célja is. Mivel ezek az alkalmazott eszközök megtévesztőek lehetnek,

⁴ SIMICSKÓ István: A hibrid hadviselés előzményei és aktualitásai, *Hadtudomány*, 2017/3-4., 6. oldal, 5. bekezdés.

⁵ JÓJÁRT Krisztián: A hibrid hadviselés és a jövő háborúja. *Honvédségi Szemle*, 2020/1., 8. o.

a kitűzött cél általában viszonylag kisebb jelentőségű, amely önmagában nem indokolná egy közvetlen háború kirobbantását. Ugyanakkor ezek a célok állami érdekeket szolgálnak, amelyeket az ellenség félrevezetésével, legtöbbször a civil társadalom környezetében próbálnak elérni. A hibrid háborúban alkalmazott megtévesztő eszközök, valamint az ehhez kapcsolódó alacsonyabb jelentőségű politikai célok azt is eredményezik, hogy az ilyen típusú hadviselésben az erőszak alkalmazása általában mérsékelt intenzitású.⁶

A hibrid hadviselés több különböző elemből áll össze, amelyek egymást erősítve hatékonyabbá teszik a konfliktuskezelést. Ezek az elemek a következők:

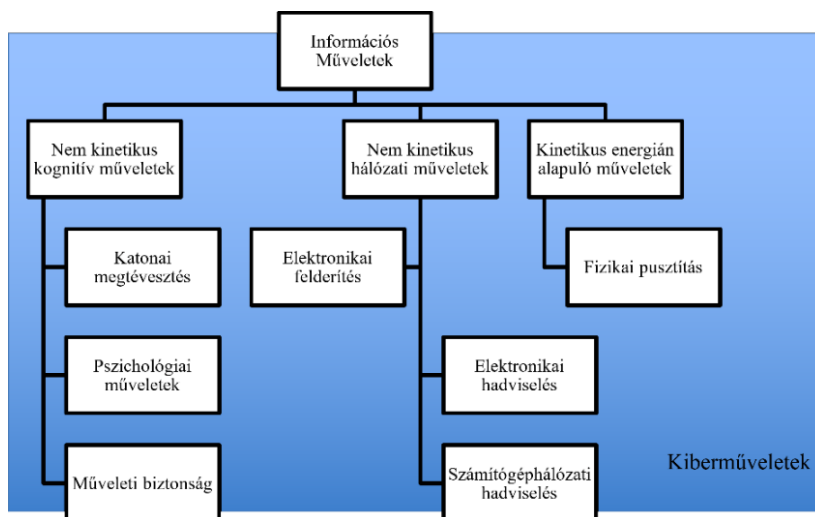
1. **Katonai erők:** A hagyományos hadviselés részeként a katonai erők alkalmazása továbbra is központi szerepet játszik a hibrid konfliktusokban. Az államok katonai erejük felhasználásával képesek közvetlenül beavatkozni a konfliktusokba, valamint demonstrálni hatalmukat és elrettentő képességüket.
2. **Nem hagyományos taktikák:** A gerilla-hadviselés, a terrorizmus és más, nem hagyományos taktikák szintén fontos szerepet játszanak a hibrid konfliktusokban. Ezek a módszerek lehetővé teszik a gyengébb szereplők számára, hogy aszimmetrikusan szembeszálljanak a hagyományos katonai erőkkel rendelkező ellenfelekkel.
3. **Információs hadviselés:** Az információs hadviselés célja az ellenséges információs rendszerekben tárolt információk megszerzése és manipulálása, valamint a közvélemény befolyásolása. Ez magában foglalja a propaganda terjesztését, az álhírek és dezinformációk elterjesztését, valamint a kiberhadviselés eszközeinek alkalmazását.
4. **Gazdasági eszközök:** A gazdasági nyomásgyakorlás, mint például a gazdasági szankciók, bojkottok és a kereskedelmi embargók szintén a hibrid konfliktusok eszköztárába tartoznak. Ezek az eszközök lehetővé teszik az államok számára, hogy közvetett módon érvékeljék el politikai és stratégiai céljait.
5. **Politikai és diplomáciai nyomás:** A hibrid konfliktusok során az államok gyakran alkalmaznak politikai és diplomáciai nyomásgyakorlást is. Ez magában foglalhatja a nemzetközi szervezetekben való befolyásolást, szövetségek kialakítását, valamint a diplomáciai csatornákon keresztül történő nyomásgyakorlást.

A nemzetközi jog és a szabályozási keretek gyakran nehezen alkalmazhatók a hibrid konfliktusokra, mivel ezek a konfliktusok elmoszák a hagyományos háborús és békés időszak közötti határokat. Az államoknak és a nemzetközi közösségnek együtt kell működniük annak érdekében, hogy hatékony válaszokat és megoldásokat találjanak ezekre az új típusú konfliktusokra.

A kibertér, mint a hibrid hadviselés egyik jellemző helyszínének alkalmazása a XX. és XXI. század technikai fejlődésével párhuzamosan fejlődött. Az időszakban megfigyelhető információs infrastruktúrától való függés miatt a kibertér, mint a

⁶ BODA Mihály: A hibrid háború etikája: az igazságos hibrid háború elmélete, In: M. SZABÓ Miklós (szerk): *A Hadtudomány aktuális kérdései*. I. kötet, Ludovika Egyetemi Kiadó, 2022. 95-108. o.

társadalmi interakciót biztosító közeg is kiemelt jelentőségű. Ennek eredményeként a NATO 2016-os varsói csúcstalálkozóján az országok vezetői egyetértettek abban, hogy a kibertér önálló hadszíntér, ezért a védelme részét képezi a NATO kollektív védelmi feladatainak, ebben a tekintetben a Szövetségnek ugyanúgy képesnek kell lennie megvédenie a tagállamokat, mint a hagyományos hadszíntereken vívott harcok során.



1. ábra: A kiberműveletek helye az információs műveletekben⁷

A háborús konfliktusokat megelőzően is jelen volt már a gazdasági érdekből elkövetett vagy a társadalom és a kormányzat működését fenyegető kibertéri szereplőkre és tevékenységükhöz kapcsolódó, a folyamatos felkészülés és reagálás igénye minden érintett szereplő részéről. Érintett szereplő lehet az információs társadalom minden résztvevője az információt előállító, megjelenítő, közvetítő elemektől a felhasználókon keresztül a társadalom működését jelentő kormányzati elemekig. A kibertérben bekövetkező cselekmények az elvárt szintjük fenntartása mellett akár könnyen negatívan is befolyásolhatják ezen szereplők működését.

Az orosz–ukrán konfliktus során alkalmazott kibertérműveletek már túlmutatnak a fentiekben bemutatott negyedik generációs modell azon részein. Megfigyelhető a kezdeti kritikus infrastruktúrákat célzó hadszíntér, emellett a képességek kiiktatásának, korlátozásának célja annak az információs műveleti üzenetnek a tolmácsolása is, hogy az orosz fél minden rendelkezésére álló eszközzel csökkenteni tudja az ukrán és támogató szövetséges kormányzati törekvéseket, ezáltal fölényben vannak az ukránok fölött.

Különösen fontos kiemelni, hogy a XXI. századi fegyveres cselekmények közül kiemelkedik az orosz–ukrán konfliktus, mivel ez a területi fontossága miatt a környező és világi hatalmi szereplők figyelmét is folyamatosan leköti. „Érdekessége, hogy amíg

⁷ HAIG Zsolt – VÁRHEGYI István: A kibertér és a cyberhadviselés értelmezése. *Hadtudomány*, 2008/E. alapján Knapp Gábor szerkesztése.

orosz oldalról hibrid hadviseléssel kezdődött, addig ukrán részről már a tízes évektől támaszkodtak a nyugati országok – tanács- adói, kiképzői – segítségére, azaz az eseménysor a módszerek, a hibrid és a proxyhadviselés konfliktusa is volt egyben. 2022-től a háború orosz részről és ukrán részről direkt háborúvá vált, amely azonban továbbra is magában foglal olyan hibrid elemeket, mint az információs hadviselés, ideértve a hackertámadásokat, a dezinformációt és a propagandát is. Emellett a nyugati országok egy része (többek között az Amerikai Egyesült Államok és az Európai Unió, illetve annak számos országa is) és Ukrajna proxyviszonyt alakítottak ki, amelyben igyekeznek az említett állam önvédelmét támogatni, illetve saját céljaikat is elérni.”⁸

Az orosz–ukrán konfliktus során megfigyelhető a kibertérműveletek átalakulása a hibrid háborúban. Ezen változás alapján a kibertérben végzett műveletek evolúciója több szakaszra bontható, amelyek mindegyike új kihívásokat és lehetőségeket hozott a hibrid hadviselésben is. Kralovánszky Kristóf A kibertér fejlődése című tanulmányát feldolgozva legalább 4 szakasz azonosítható.

Az első, kezdeti szakaszban előtérben vannak az információs műveletek és a pszichológiai hadviselés. Az internet és a közösségi média elterjedésének kihasználásával az álhírek és dezinformációk gyors terjesztése lehetséges, amelynek célja a társadalom megosztása és az állami intézményekbe vetett bizalom megingatása. Erre példaként felhozható, hogy a konfliktushoz kapcsolódó, de időszakban azt megelőző Krím-félsziget 2014-es orosz annektálása során is folytatott átfogó dezinformációs kampányt Oroszország, hogy legitimálja saját lépéseit és destabilizálja Ukrajnát. Ugyancsak Oroszországhoz köthető a 2016-os amerikai elnökválasztás során hackerek és mesterségesen létrehozott profilok által terjesztett álhírekkel való beavatkozás ténye, amely módosított információkat megfelelő technikák alkalmazása esetén valós médiaplatformok is átvettek azok hitelességének ellenőrzésétől eltekintve.

Következő szakaszként kell tekinteni a kritikus infrastruktúrák elleni támadásokra, például az energiaellátó rendszereket, a vízellátást és a közlekedési hálózatokat célozva. Ezek a támadások komoly zavart okozhatnak egy ország működésében, és alááshatják a lakosság biztonságérzetét. 2015 decemberében Ukrajnában egy ilyen támadás következtében több százezer ember maradt áram nélkül, amikor hackerek behatoltak az energiaszolgáltató rendszerekbe és leállították azokat. 2017-ben a NotPetya nevű zsarolóvírus támadást indított, amely világszerte számos vállalatot és intézményt érintett, különösen Ukrajnában.

A kibertérműveletek következő érettségi szakaszát már a fejlett kiberfegyverek és az állami szereplők jelenléte jellemzi. Ezek a csoportok képesek komplex támadások végrehajtására, beleértve a kémkedést, a szabotázszt és a politikai befolyásolást. Példaként a korábban említett Stuxnet féregvírust lehet felhozni, amelyet a

⁸ BODA Mihály: A proxyháború filozófiai és etikai megközelítésben. Honvédségi Szemle, 2023/6. 28. o. 2. bek.

feltételezések szerint állami támogatással fejlesztettek ki. A 2020-ban felfedezett SolarWinds támadás során orosz hackerek behatoltak számos amerikai kormányzati és magánintézmény rendszerébe, hónapokon keresztül észrevétlenül gyűjtve érzékeny információkat.

A XXI. századi fejlettségi szakaszt már a mesterséges intelligencia (továbbiakban: MI) és automatizált támadások jellemzik. Az MI segítségével automatizált támadásokat lehet végrehajtani, amelyek gyorsabbak és nehezebben észlelhetők. Emellett az MI-t felhasználják a korábban első, kezdeti szakaszban azonosított eszközök, így a dezinformáció terjesztésére is, például hamis videók (deepfake) készítésére, amelyekkel manipulálni lehet a közvéleményt.

Úgy gondoljuk, hogy a hibrid hadviseléshez kapcsolódóan új, aktuálisan legmagasabb fejlettségi szakaszként lehet azonosítani a kiber- és hagyományos hadviselés integrációját. Az orosz–ukrán konfliktusban a kibertámadások gyakran kísérik a hagyományos katonai műveleteket, bár még megfigyelhető az orosz kiberműveletek egyik gyengeségeként a kiber- és a hagyományos támadások közötti koordináció hiánya.

Kijelenthető, hogy a hibrid háborúban a kibertérben végzett műveletek folyamatosan fejlődnek, változnak, alkalmazkodva a hagyományos és politikai területeken elvárt célokhoz. A példák jól mutatják, hogyan változtak és fejlődtek a kibertérben zajló műveletek az orosz–ukrán konfliktus során is, és egyben rávilágítanak a modern hadviselés új kihívásaira és dinamikájára.

Az orosz kiberműveletek történetét tekintve kijelenthető, hogy a technikai fejlődéssel lépést tartva Oroszország alkalmazza a kibertér eszközeit, technikáit és eljárásait a riválisai ellen való hosszú távú versengés során. 2014 előtt Moszkva kampányai inkább a politikai hadviselésre és a kémkedésre összpontosítottak, azonban megértve a dinamikus változó biztonsági környezet kihívásait megkezdte saját technikai alapú képességeinek kialakítását. Ezek közül is az észtországi és grúziai műveletei voltak a legkiemelkedőbbek.

2007-ben Észtországot célozva Oroszország egy masszív, a teljes lakosságot érintő, a pénzügyi és informatikai szektort célzó szolgáltatásmegtagadási műveletekkel vette célba. A kibertérművelet előzményeként Észtország áthelyezte a Bronzkatona néven ismert orosz emlékművet. A 2007-es Észtország elleni kibertámadások először világtottak rá a NATO-országok, az intézményeik és a társadalmuk, sőt maga a NATO esetleges sebezhetőségére az információs és kommunikációs rendszerük megzavarásával. A NATO Kibervédelmi Kiválósági Központ (NATO CCD COE) Észtországban történő megalakításakor a lokáció kiválasztása szimbolikus jelentőséggel is bírt, így üzenve a világnak, hogy a kibertérben elkövetett cselekedeteknek súlyuk van, és azokat a NATO figyelemmel kíséri.⁹

⁹ MANESS, Ryan – VALERIANO, Brandon: *Russia's Coercive Diplomacy: Energy, Cyber, and Maritime Policy as New Sources of Power*. Palgrave Macmillan, 2015.

A 2008-as orosz-grúz konfliktus során Oroszország kibertámadásokat használt fel, hogy lehetővé tegye a Grúzia elleni információs műveleteket. Ez az első dokumentált alkalom, hogy a kibertérműveletek hibrid formában, egy másik műveleti területre is kiterjedően került felhasználásra. Az orosz információs műveletek célja itt a potenciális ellenfelek döntéshozatalának befolyásolása, megzavarása, korrumpálása vagy kisajátítása volt, miközben aktívan fellépett a saját vezetési és irányítási rendszerének védelme érdekében.

Ezt követően a kibertérműveletek alkalmazása a grúz példában is megmutatott párhuzamos, kiegészítő alkalmazás mellett valamilyen egyéb műveleti tevékenység kiegészítése, támogatása formájában valósult meg, ezzel teljesítve a hibrid műveletek követelményeit.

Az ukrán kritikus infrastruktúra megsemmisítésére irányuló katonai kampányának előzményeként Oroszország kiberműveleteket is alkalmazott Kijev áramellátásán keresztül történő célzott korlátozásainak elérése érdekében. A Krím 2014-es illegális annektálását követően a fejlett tartós fenyegetések (APT) csoportjai, mint például a „Sandworm”, részt vettek a 2015-ös „BlackEnergy” kampányban, amely az ukrán áramtermelés és -elosztás ellen irányult. Bár a támadások címlapokra kerültek, a hatékony kibervédelmi eljárások miatt csak korlátozott hatást váltottak ki. 2017-ben az oroszokhoz kötődő csoportok elindították a „NotPetya” kampányt, amely olyan hatásokat váltott ki, amelyek a tervezett célpontokról, ukrán vállalatokról már átterjedtek a globális logisztikai szereplőkre is, így világméretű hatásokat is képesek voltak kiváltani.

Muellerék ugyanakkor egy 2023-ban írt tanulmányban már azt állítják, hogy a kibertérműveletek fókusza elmozdult, és a kezdeti, kritikusinfrastruktúra-elemekre vonatkozó célok helyett a kibertámadások aktuális fókusza immár az Ukrajnát segítő szövetségesek együttműködését hivatott gátolni.¹⁰ Oroszország a kiberműveleteket a politikai hadviselés egyik formájaként is felhasználta, a propaganda keverékét használva a társadalmak polarizálására és a politikai ellenlábasai befolyásolására.

Muellerék a helyi kibertámadásoktól eltérő fókuszú megközelítését szintén alátámasztják, hogy igazoltan megfigyelhető, hogy Oroszország kiberelemeként is tartalmazó hibrid műveletei az orosz–ukrán konfliktus közvetlen helyszínére nem korlátozódnak. A konfliktussal összefüggésben és ezzel párhuzamosan folyik a posztszovjet országok irányába folytatott hibridtevékenység is. Az elmúlt év során Oroszország egyre agresszívebben használta fel a hibridfenyegetés eszköztárát, különösen a balti-tengeri régióban, de máshol is. A balti-tengeri térség országainak Oroszországhoz való közelsége és a Fehéroroszországgal, valamint az érintett országok kibertéri kitettségén keresztül elérhető proxyjellegű kapcsolatok együtt egyaránt sebezhetővé teszik az érintetteket, illetve lehetőségeket adnak a fenyegetések kutatására az érintett országokban. Oroszország tanulva a korábbi tapasztalatokból az

¹⁰ MUELLER, Grace B. – JENSEN, Benjamin – VALERIANO, Brandon – MANESS, Ryan C. – MACIAS, Jose M.: *Cyber Operations during the Russo-Ukrainian War*. 2023, Online, 11. o., 3. bek.

információs műveletek teljes spektrumának vizsgálatát hajtja végre jelenleg, amelyek olyan katonai és nem katonai műveletek összességei, amelyeknek célja, hogy befolyásolják, zavarják, megghiúsítsák vagy irányítsák az ellenfél információs rendszereit és folyamatait, miközben saját információs rendszereik védelmét biztosítják. Ezzel összhangban, Oroszország Ukrajnában és minden érintett országban változatos taktikákat alkalmaz, mint például dezinformáció, kibertámadások, pszichológiai nyomásgyakorlás, illetve szabotázsakciók, hogy nyomást gyakoroljon és destabilizálja azokat. Ugyanakkor megfigyelhető az is, hogy az érintettek a folyamatos célpontként való szereplésük ellenére ellenállónak bizonyulnak és eltökéltséget tanúsítanak az ilyen jellegű fenyegetésekkel szemben, fenntartva így a belső koherenciát és az elvárt „situation awareness”-t. Igazolt, hogy erős szövetségekre és proaktív intézkedésekre van szükség a hatékony védelemhez, amihez az EU és NATO szövetséges tagországok különböző képességei és támogatásai biztosításával járulnak hozzá.

Oroszország azonban továbbra is kitart taktikájának kiigazítása mellett, és reakciókat tesz, ami potenciálisan fokozhatja a feszültséget. Az elfogadhatóság határainak elmozdulásával szembeni ellenállás, a tudatosság növelése és az elrettentés fokozása létfontosságú az EU, a NATO és tagállamai számára, amelynek változását folyamatosan figyelemmel kell kísérni.

A hibridműveletek során tanulmányozott kibertérműveleti elemek – a kapcsolódó elektronikus információs rendszerek fizikai domáinokon (is) átívelő kihatása miatt – egyéni megközelítést igényelnek. A műveleti terület többdimenziós bemutatását az érintett domáinok, így a szárazföld, a NATO és egyes haditengerészettel is rendelkező államok esetében a vízfelület, a légtér és a világűr, mint fizikai domáinok, és a kibertér összefüggésében kell vizsgálni, amelyet az alábbi ábra szemléltet:



2. ábra: A műveleti terület többdimenziós bemutatása az érintett domáinok vonatkozásában¹¹

¹¹ DONELLY, Jared – FARLEY Jon: Defining the ‘Domain’ in Multi-Domain. *Conference 2019 Read Aheads*, Joint Air Power Competence Centre, 2019. június 9. o. táblázatát fordította Knapp Gábor.

Annak érdekében, hogy a nemzetek gyors és hatékony válaszokat tudjanak adni a kiber hadszíntér sajátosságából adódó kihívásokra, összhangban a katonai sajátosságokból adódó feladatrendszerrel, domain specifikus komponens parancsnokságokat (Cyber Command) hoztak létre. Ezek feladatrendszere folyamatosan alakul át, egészül ki figyelembe véve a korábban felsorolt tényezőket. Megállapítható, hogy a korábban csak katonai specifikumként kezelt tényezők egyre inkább elmozdulnak a civil szektor irányába, így is felértékelve a civil-katonai kapcsolatok jelentőségét.

Oroszország Ukrajna elleni konfliktusa során alkalmazott hibrid műveletei alátámasztják ezt a különböző hadszínterek közötti megközelítést, hiszen a műveletek során a kibertéri és így hibrid műveletei a szárazföldi és légi erők támogatása érdekében fejt ki hatást. A kifejtett erők ugyanakkor az elektromágneses spektrumon keresztül érintettek mind a politikai, katonai, gazdasági, szociális, infrastruktúra és nem utolsósorban az információs rendszereken keresztül.

Összegzés

A kibertéri műveletek fejlődésének és a megváltozott nemzetközi rendszer kapcsolatának elemzése során nyilvánvalóvá válik, hogy a technológiai előrehaladás és a digitális átalakulás jelentős hatással van a globális biztonságpolitikai és geopolitikai viszonyokra és ezek elérése érdekében alkalmazott módszerekre. Az információs és kommunikációs technológiák robbanásszerű fejlődése, valamint az internet és digitális rendszerek széleskörű elterjedése új kihívások és lehetőségek elé állítja a nemzetközi közösséget. A lehetséges kibertéri műveletek az elmúlt években jelentős mértékben fejlődtek, ezzel új dimenziót nyitottak a hadviselés, a hírszerzés és a diplomácia területén, illetve lehetőséget biztosítanak a felek és őket támogató szereplők indirekt beavatkozására. A kibertérben zajló műveletek számos formában valósulhatnak meg, beleértve a kormányzati és a katonai rendszerek elleni támadásokat, az ipari kémkedést, az infrastruktúrák megbénítását, valamint az információs hadviselést. Az ilyen típusú műveletek a hagyományos fegyveres konfliktusokkal szemben nem igényelnek közvetlen fizikai jelenlétet, ezzel is erősítve az indirekt konfliktusok során megfigyelteket, ami radikálisan megváltoztatja a hadviselés és a védekezés stratégiáját és taktikáját.

A globalizáció és a digitalizáció folyamatai mélyrehatóan átalakították a nemzetközi kapcsolatok szerkezetét, és új szereplőket emeltek a színpadra. A nem állami szereplők, mint például a multinacionális vállalatok, civil szervezetek és egyének, egyre nagyobb szerepet játszanak. A kibertéri műveletek és a nemzetbiztonság közötti kapcsolat szoros összefonódása új stratégiák és politikai megközelítések kialakítását követeli meg. Ebben a kontextusban kiemelten fontos, hogy új jogi és szabályozási kereteket alakítsanak ki, amelyek figyelembe veszik a kibertéri műveletek sajátosságait és kihívásait. A nemzetközi jogi normák és szabályok gyakran nehezen alkalmazhatók a kibertérre, és az információs hadviselés sok esetben a hagyományos háborús és békés időszak közötti határokat elmossa.

Összességképpen elmondható, hogy a kibertéri műveletek fejlődése és a megváltozott nemzetközi rendszer szoros összefüggésben áll egymással. Az információs és kommunikációs technológiák fejlődése révén a kibertérben zajló műveletek jelentős mértékben befolyásolják a nemzetközi kapcsolatok szerkezetét és dinamikáját. Az államok és a nemzetközi közösség számára kulcsfontosságú, hogy képesek legyenek hatékonyan reagálni ezekre az új kihívásokra, és megfelelő jogi és szabályozási kereteket alakítsanak ki a kiberbiztonság érdekében. A kibertéri műveletek és a nemzetközi rendszer közötti kölcsönhatások megértése és elemzése elengedhetetlen a jövőbeni globális biztonsági kihívások kezelése és a nemzetközi béke és stabilitás megőrzése érdekében.

Felhasznált irodalom:

BODA Mihály: A hibrid háború etikája: az igazságos hibrid háború elmélete, In: M. SZABÓ Miklós (szerk): *A Hadtudomány aktuális kérdései*. I. kötet, Ludovika Egyetemi Kiadó, 2022. 95-108. o.

BODA Mihály: A proxyháború filozófiai és etikai megközelítésben. *Honvédségi Szemle*, 2023/6. 28. o. 2. bek.

DONELLY, Jared – FARLEY Jon: Defining the 'Domain' in Multi-Domain. *Conference 2019 Read Aheads*, Joint Air Power Competence Centre, 2019. június 9. o. Elérhető: <https://www.japcc.org/defining-the-domain-in-multi-domain/> (Letöltés ideje: 2025. 01. 06.)

HAIG Zsolt – VÁRHEGYI István: A cybertér és a cyberhadviselés értelmezése. *Hadtudomány*, 2008/E. Elérhető: <https://ojs.mtak.hu/index.php/hadtudomany/article/view/6402> (Letöltés ideje: 2025. 01. 07.)

JÓJÁRT Krisztián: A hibrid hadviselés és a jövő háborúja. *Honvédségi Szemle*, 2020/1., 8. o.

MUELLER, Grace B – JENSEN, Benjamin – VALERIANO, Brandon – MANESS, Ryan C.– MACIAS, Jose M.: *Cyber Operations during the Russo-Ukrainian War*. 2023, Online, Elérhető: <https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war> (Letöltés ideje: 2024. 12. 27.)

MUMFORD, Andrew: Proxy warfare and the future of conflict. *RUSI Journal*, 2013b/2.

MANESS, Ryan – VALERIANO, Brandon: *Russia's Coercive Diplomacy: Energy, Cyber, and Maritime Policy as New Sources of Power*. Palgrave Macmillan, 2015.

SIMICSKÓ István: A hibrid hadviselés előzményei és aktualitásai, *Hadtudomány*, 2017/3-4., 6. oldal, 5. bekezdés.

KORSZERŰ, GYORS FELDOLGOZÁST LEHETŐVÉ TÉVŐ MESTERSÉGESINTELLIGENCIA-ALAPÚ KÉPFELDOLGOZÁSI TECHNOLÓGIÁK²

A tanulmány a mesterségesintelligencia-alapú képfeldolgozás legújabb technológiáit tárgyalja, amelyek számos iparágban és alkalmazási területen jelenleg már elengedhetetlenek a nagy mennyiségű képi információk gyors és pontos feldolgozásában. A kutatás bemutatja, hogyan egészítik ki vagy váltják fel a hagyományos képfeldolgozási módszereket a modern AI-technológiák, elsősorban a neurális hálózatok, gépi tanulás és mélytanulás alkalmazásával. A tanulmány részletesen tárgyalja a konvolúciós neurális hálózatok (CNN) és a Generative Adversarial Networks (GAN) neurális hálózatok működésének alapelveit, valamint ezek fő alkalmazási lehetőségeit a képfeldolgozásban és annak egyes részfolyamataiban. Emellett rávilágít arra is, hogy mely területeken használhatóak leginkább ezek a technológiák. A tanulmányt a képfeldolgozásban legelterjedtebb neurális hálózati modellek értékelése zárja, rámutatva az alkalmazásukkal járó kihívásokra is.

Kulcsszavak: mesterséges intelligencia, képfeldolgozás, mélytanulás, konvolúciós neurális hálózatok, generatív ellenfél hálózatok

RESEARCH ON MODERN ARTIFICIAL INTELLIGENCE-BASED IMAGE PROCESSING TECHNOLOGIES ENABLING RAPID PROCESSING

This paper discusses the latest advancements in artificial intelligence-based image processing technologies, which have become essential for the rapid and accurate handling of large amounts of visual data across numerous industries and application areas. Modern AI technologies, primarily neural networks, machine learning, and deep learning, increasingly complement or replace traditional image processing methods. The paper details the fundamental operating principles and capabilities of Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs), highlighting their key applications within various image processing tasks and sub processes. Furthermore, it identifies the industrial sectors and practical fields where these technologies offer the greatest benefits. Finally, the paper concludes with an evaluation of the most widely used neural network models in image processing, outlining the challenges associated with their application.

Kulcsszavak: Artificial intelligence, Image processing, Deep learning, Convolutional Neural Networks, Generative Adversarial Networks

¹ ORCID-azonosító: 0009-0006-7370-9637

² Jelen Mű a TKP2021-NVA-24 azonosítószámú projekt keretén belül a Kulturális és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a Tématerületi Kiválósági Program 2021 – Nemzetvédelem, nemzetbiztonság pályázati alprogram finanszírozásában valósult meg. 2024. június.

Bevezetés

A mesterséges intelligencia (AI³) és a gépi látás technológiái napjainkban gyors ütemben fejlődnek, jelentős hatást gyakorolva számos iparágra és alkalmazási területre. A képfeldolgozás, mint az AI egyik kiemelkedő alkalmazása, különösen fontos szerepet tölt be a modern katonai műveletekben, ahol az információk gyors és pontos feldolgozása elengedhetetlen a sikeres döntéshozatalhoz és műveleti hatékonysághoz. Az AI és a gépi látás technológiái lehetőséget biztosítanak arra, hogy a katonai egységek valós idejű adatokat gyűjtsenek, elemezzenek és értelmezzenek, ezzel növelve a műveletek hatékonyságát és biztonságát.

A tanulmány tárgyalja a legújabb fejlesztéseket és technikákat, amelyek lehetővé teszik a nagy mennyiségű kép- és videóadat gyors és hatékony feldolgozását. Bemutatjuk a konvolúciós neurális hálózatok (CNN⁴), a generatív ellenfél hálózatok (GAN⁵) és más gépi tanulási modellek alkalmazásait ezen a területen, amelyek jelentős előrelépéseket hoztak a képfeldolgozás terén.

A tanulmány célja, hogy átfogó pillanatképet nyújtson erről a dinamikusan fejlődő területről, a korszerű, gyors feldolgozást lehetővé tevő képfeldolgozási technológiákról, amelyek hozzájárulhatnak a hadsereg operatív képességeinek növeléséhez és a katonai műveletek sikeres végrehajtásához.

Képfeldolgozás alapfogalmak

Digitális képfeldolgozás

A digitális képfeldolgozás (image processing) célja, hogy az algoritmus segítségével történő feldolgozás eredményeként egy új képet kapjon a felhasználó, amely valamilyen szempontból a felhasználó számára előnyösebb, mint az eredeti kép(ek). Magában foglalja a képek javítását, tömörítését, helyreállítását és elemzését. Ezek az eljárások gyakran a képek ember általi láthatóságát vagy további feldolgozását segítik.

Digitális vs. analóg képfeldolgozás

A képfeldolgozás területe digitális képfeldolgozásra és analóg képfeldolgozásra osztható. A digitális képfeldolgozást (képközzététel) úgy definiálják, mint digitális képek feldolgozását bizonyos algoritmusok, digitális számítógépek segítségével, míg az analóg képfeldolgozás minden olyan képfeldolgozási feladat, amely kétdimenziós analóg jeleken végezhető el analóg eszközökkel.⁶

³ AI – Artificial Intelligence – mesterséges intelligencia

⁴ CNN – Convolutional Neural Networks – konvolúciós neurális hálózatok

⁵ GAN – Generative Adversarial Networks – generatív ellenfél hálózatok

⁶ SARFRAZ, Muhammad (szerk.): *Digital Imaging*. London, IntechOpen, 2020. 1. o.

Számítógépes látás, mintafelismerés és digitális képfeldolgozás

A számítógépes látás (computer vision) és a mintafelismerés (pattern recognition) területei fogalomhasználat és -értelmezés terén átfedésben vannak a digitális képfeldolgozás területével.

A számítógépes látás arra irányul, hogy a számítógépek képesek legyenek megérteni és értelmezni a vizuális világot. Ez magában foglalja a képek és videók elemzését, feldolgozását és értelmezését.

A digitális képfeldolgozás a digitális képek feldolgozásának és manipulálásának tudománya, amely magában foglalja a képek javítását, tömörítését, helyreállítását és elemzését. Célja, hogy a képekből hasznos információkat nyerjen ki, vagy azok minőségét javítsa különböző alkalmazási területeken.

A mintafelismerés olyan eljárások összessége, amelyek célja, hogy azonosítsák és osztályozzák a mintákat adathalmazokban. Ez magában foglalja a jellegzetességek kinyerését és a kategóriák közötti megkülönböztetést gépi tanulási algoritmusok segítségével. A mintafelismerés rendszerint alapvető szerepet játszik a számítógépes látás és a digitális képfeldolgozás rendszereiben.

A digitális képfeldolgozás gyakran az alapvető előfeldolgozási lépéseket biztosítja a számítógépes látás és mintafelismerés számára, például a zajcsökkentést és élesítést. A számítógépes látás magasabb szintű feladatok elvégzésére használatos, mint az objektumfelismerés és helyzetértékelés, gyakran a digitális képfeldolgozás által előkészített képeket használva.

A mintafelismerés a képekben és videóknál található minták és jellemzők felismerésére szolgál, amelyek fontosak mind a számítógépes látás, mind a digitális képfeldolgozás során.

Ezen területek közös célja, hogy a vizuális adatokat hatékonyan és pontosan elemezzék és értelmezzék különböző alkalmazási területeken. ⁷

A képfeldolgozás rövid története

A képfeldolgozás története több évtizedre nyúlik vissza, a kezdeti analóg képfeldolgozási módszerektől egészen a mai modern, AI által támogatott technikákig. Az 1960-as években a NASA⁸ fejlesztette ki a Holdról készült képeinek feldolgozására az első olyan rendszert, amelyet a digitális képfeldolgozásra alkalmaztak. E rendszer célja az volt, hogy a műholdfelvételek tisztításával és részletgazdagabbá tételével

⁷ SZEMENYEI Márton: *Számítógépes Látórendszerek*. Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar, Irányítástechnika és Informatika Tanszék, 2022. 9. o.

⁸ NASA – National Aeronautics and Space Administration

lehetővé tegye a tudósok számára, hogy behatóbban tanulmányozzák a holdfelszínt. Főként olyan képfeldolgozási technikákat használtak, mint a geometriai korrekció, a gradiens transzformáció és a zajeltávolítás.⁹

Az 1970-es és 1980-as években a digitális képfeldolgozás gyors fejlődésen ment keresztül a számítógépes technológia előrehaladásának köszönhetően. Ebben az időszakban számos alapvető algoritmust és technikát fejlesztettek ki, mint például a Fourier-transzformációt a képrekonstrukcióhoz, valamint az élfelismerési algoritmusokat, amelyek jelentős mértékben hozzájárultak a képek elemzésének és értelmezésének pontosságához és hatékonyságához, különösen az orvosi és műszaki alkalmazásokban.

A képfeldolgozás története során több olyan technológiai áttörés történt, amelyek mind hozzájárultak ahhoz, hogy a mai modern rendszerek képesek legyenek valós idejű, nagy pontosságú képelemzést és értelmezést végezni.

Az 1990-es évek folyamán a képfeldolgozás technológiája egyre szorosabban integrálódott a számítógépes látás rendszerekbe, ahol a cél már nem csak a képek feldolgozása, hanem azok értelmezése is volt. Ebben az időszakban kezdett elterjedni a gépi tanulás alkalmazása, különösen a neurális hálózatok bevonása a képfeldolgozásba. A képosztályozás és objektumfelismerés technikái egyre kifinomultabbá váltak, és széles körben kezdtek elterjedni az ipar több területén, beleértve a gyártást, a biztonsági rendszereket és a szórakoztatóipart.

Az ezredfordulót követően a képfeldolgozás és a számítógépes látás területén a konvolúciós neurális hálózatok (CNN) jelentették a következő nagy áttörést. A CNN DL¹⁰ algoritmusok különösen eredményesek olyan komplex képfeldolgozási feladatokban, mint a képklasszifikáció, szegmentáció és az objektum detektálás. Ezeknek a technológiáknak az alkalmazása jelentős előrelépést eredményezett számos iparágban és területen, köztük az arcfelismerés, önvezető autók és a robotika területén.

A közelmúltban a generatív ellenfél hálózatok (GAN) megjelenése tovább bővítette a képfeldolgozás lehetőségeit. Ezek a modellek képesek rendkívül részletes és valóságos képek generálására is képessé válnak, ami új távlatokat nyitott meg a képfeldolgozás terén, különösen az orvosi képalkotásban és a valós idejű videofeldolgozásban.¹¹

⁹ TOMAYKO, James E: *Computers in Spaceflight: The NASA Experience*. Kansas, NASA, 1988. 287-288. o.; SARFRAZ 2020, 2.

¹⁰ DL – Deep learning – mélytanulás

¹¹ DULARI, Bhatt –PATEL, Chirag –TALSANIA, Hardik –PATEL, Jigar –VAGHELA, Rasmika –PANDYA, Sharnil – MODI, Kirit – GHAYVAT, Hemant: CNN Variants for Computer Vision: History, Architecture, Application, Challenges and Future Scope. *MDPI Electronics*, 2021/20., 16. o.

Korszerű képfeldolgozási technológiák áttekintése

Hagyományos képfeldolgozási módszerek

A hagyományos képfeldolgozási módszerek szolgáltatnak alapot a modern képfeldolgozási technikákhoz. Ezek a módszerek olyan alapvető algoritmusok és technikák sorozatának alkalmazását jelentik, amelyek elősegítik a képek elemzését és feldolgozását. A mai napig nélkülözhetetlenek a képelemzés területén, különösen akkor, amikor gyors és hatékony megoldásokra van szükség alacsony számítási kapacitás mellett. Ugyanakkor az új technológiák és algoritmusok folyamatos fejlesztése lehetőséget nyújt még pontosabb és robusztusabb képfeldolgozási megoldások kialakítására.

A képfeldolgozás legfőbb lépései a képhelyreállítás (előfeldolgozás), képjavítás, képszegmentálás, jellemzőkinyerés (feature extraction) és osztályozás területeit foglalják magukba.

A képhelyreállítás célja a torzult vagy romlott képek integritásának és vizuális minőségének visszaállítása annak érdekében, hogy a rejtett részletek láthatóvá váljanak. Ez különösen fontos olyan digitális képalkotási problémák vagy utófeldolgozási eljárások esetében, amelyek hátrányosan befolyásolják a képminőséget. A zaj, például a Gauss-zaj és a só-bors zaj (véletlenszerűen váltakozó fekete-fehér pixelek) eltávolítása kritikus lépés.

Hagyományos módszerei között megtalálhatóak a korlátozott legkisebb négyzetes szűrők, vak dekonvolúció, Wiener és inverz szűrők, valamint az adaptív szűrések. Ezek a technikák az elmosódás és zaj csökkentésére törekednek, hogy helyreállítsák a képek élességét és részleteit. A modern megközelítések, mint a teljes variációs zajcsökkentés és a Non-Local Means, szintén fontos szerepet játszanak, mivel hatékonyan csökkentik a véletlenszerű zajt, miközben megőrzik a képrészleteket.

A DL-modellek további javulást hoznak, mivel képesek tanulni és alkalmazkodni a különböző zaj- és torzítási mintákhoz, tovább növelve a kép helyreállításának hatékonyságát.¹²

A hagyományos képfeldolgozási részfeladatok mindegyikének ismertetése a tanulmány kereteit meghaladja, kiemelésért érdemelnek az alábbi technikák:

1. Éldetektálás (Edge Detection): Az éldetektálás az egyik alapvető módszer, amely a kép élein található intenzitásváltozások azonosítására szolgál. Az olyan operátorok, mint a Sobel, Prewitt és Canny operátorok, gyakran használatosak az élek detektálásában.

¹² ARCHANA, R. – JEEVARAJ, P. S. Eliahim: Deep learning models for digital image processing: a review. *Artificial Intelligence Review*, 2024/11, 1-33. o.

2. Fourier-transzformáció: A Fourier-transzformáció a képek frekvenciatartományban történő elemzésére szolgál. Ez a technika különösen hasznos a képrekonstrukcióban és a zajszűrésben, mivel lehetővé teszi a különböző frekvenciakomponensek szétválasztását és manipulálását.
3. Szegmentálás: A képszegmentálás a kép különálló régiókra bontására szolgál, amelyek hasonló jellemzőkkel rendelkeznek. A k-means clustering és a thresholding (küszöbölés) technikák a szegmentáció alpmódszerei közé tartoznak.
4. Szűrés: A képszűrés a zaj eltávolítására és a képminőség javítására szolgál. Az olyan szűrők, mint a Gauss-szűrő és a median-szűrő gyakran használatosak a kép simítására és a zaj csökkentésére.¹³

Az utóbbi években a ML¹⁴ és DL integrációja a hagyományos módszerekkel jelentős előrelépést hozott a képfeldolgozás terén. Kifejlesztettek olyan hibrid modelleket is, amelyek kombinálják a hagyományos és a DL technikákat, és javítják a képszegmentálás pontosságát és megbízhatóságát.

Mesterséges intelligencia és mélytanulás a képfeldolgozásban

Neurális hálózatok

A neurális hálózat egy fejlett számítási modell, amely az emberi agy összekapcsolt neuronjainak szerkezetét és funkcióit modellezi. Ez a modell olyan egymással összekapcsolt egységekből, úgynevezett „neuronokból” áll, amelyek több rétegben szerveződnek, és ezek a rétegek képesek az adatokból származó összetett mintázatokat és kapcsolatokat feldolgozására és értelmezésére.

Egy neurális hálózat általánosságban három fő típusú rétegből tevődik össze: egy bemeneti rétegből, egy vagy több rejtett rétegből és egy kimeneti rétegből. A bemeneti réteg fogadja az adatokat, a rejtett rétegek feldolgozzák ezeket az adatokat, és a kimeneti réteg adja meg a hálózat által generált választ vagy eredményt. Minden egyes neuron kapcsolatban áll a következő réteg neuronjaival súlyozott élekkel, amelyek a kapcsolatok erősségét szabályozzák. Ezek a súlyok dinamikusan módosulnak a tanulási folyamat során, amely során a hálózat az adatokból tanul és finomítja a belső paramétereit.

A neurális hálózatok különösen hatékonyak olyan feladatok elvégzésében, mint a mintafelismerés, az osztályozás, a regresszióanalízis és a jellemzőkinyerés. Az ilyen típusú hálózatok azon képessége, hogy nagy adathalmazokból tanuljanak és összetett mintákat azonosítsanak, döntő jelentőségű a modern gépi tanulásban. Az adatokból való tanulás és az ismeretek felfedezése által a neurális hálózatok lehetővé teszik a

¹³ SONKA, Milan – HLAVAC, Vaclav – BOYLE, Roger: *Image Processing, Analysis, and Machine Vision, Fourth Edition*. Cengage Learning, Stanford, USA, 2013. 130-135. o.; SZEMENYEI 2020, 34-39., 129.

¹⁴ ML – Machine learning – gépi tanulás

gépek számára, hogy önállóan hozzanak döntéseket és javítsák teljesítményüket különböző alkalmazási területeken.

Mélytanulás a képfeldolgozásban

A képfeldolgozás sokrétű terület, amely számos módszert alkalmaz értékes információk kinyerésére a képekből. Az AI birodalmában a ML olyan alcsoportként jelenik meg, amely lehetővé teszi a modellek számára, hogy strukturált adatkészletekből önállóan extrapoláljanak eredményeket, jelentősen csökkentve ezzel az emberi beavatkozás szükségességét a döntéshozatali folyamatban.

A mélytanulás, mint a gépi tanulás egy speciális irányt képviselő terület, túllép a hagyományos adatkezelési technikákon, különösen strukturálatlan adatok, mint például képek és hangok feldolgozásában.

A hagyományos képfeldolgozási módszerek és a DL-modellek két külön megközelítést képviselnek a képelemzési feladatoknál. A hagyományos módszerek gyakran kézzel készített algoritmusokon és heurisztikákon alapulnak, amelyek előre meghatározott lépések sorozatával dolgozzák fel a képeket. A DL-modellek közvetlenül az adatokból tanulják meg a jellemző reprezentációkat, lehetővé téve, hogy automatikusan kinyerjék azokat a bonyolult jellemzőket, amelyeket a hagyományos módszerek esetleg nem vesznek észre.

A DL rendkívüli pontosságot képes elérni, gyakran meghaladva az emberi teljesítményt. Ezen kiemelkedő teljesítmény azonban jelentős adatmennyiséget igénylő, összetett neurális hálózatok tanításától függ.

A DL az utóbbi években jelentős előrelépés a ML világában, különösen a képfeldolgozás területén. Ez a technológia neurális hálózatokon alapul, amelyek összetett, rétegzett algoritmusokból állnak, és ezek az emberi agy neuronális szerkezetének működését modellezzik. Ezen algoritmusok rétegei az adatokból történő tanulási folyamat során egymással összekapcsolt neuronokat utánoznak, ahol minden egyes neuron az adatok egy bizonyos aspektusára reagál.

Ez az agy által inspirált struktúra lehetővé teszi a mélytanulási modellek számára, hogy összetett mintázatokat és jellemzőket ismerjenek fel, amelyek a hagyományos ML-modelleknél jóval bonyolultabbak. Ennek köszönhetően a DL sokkal hatékonyabban képes feldolgozni és értelmezni a vizuális információkat, javítva ezzel a képfeldolgozási feladatok teljesítményét olyan területeken, mint az arcfelismerés, objektumdetektálás vagy akár a komplex jelenetek elemzése.

A mélytanulás tehát nem csupán egy újabb lépés a gépi tanulás fejlődésében, hanem egy forradalmi ugrás, amely radikálisan megváltoztatta, hogyan közelítenek meg különböző problémákat az adatokból történő tudás kinyerése és a döntéshozatali folyamatok automatizálása terén.

Konvolúciós neurális hálózatok (CNN)

Az AI-alapú képfeldolgozás területén a CNN-ek és a GAN-ok adják azt a két alapvető technológiát, amelyek döntő szerepet játszottak a számítógépes látás fejlődésében. A CNN-eket és a GAN-okat a képfeldolgozás kontextusában külön-külön, és egyes aspektusait összehasonlítva is szükséges bemutatni, feltárva erősségeiket, gyengeségeiket és alkalmazási lehetőségeiket a képfeldolgozás területén.

A CNN-ek regularizált, feed-forward típusú neurális hálózatok, amely a jellemzők kinyerését a szűrők optimalizálása révén öntanuló módon végzik. A feed-forward hálózatok olyan neurális hálózatok, amelyekben az információ csak egy irányban terjed, a bemeneti rétegből a kimeneti rétegek felé. Ezek a hálózatok nem tartalmaznak visszacsatolást vagy hurkokat, ami azt jelenti, hogy a bemeneti adatok áthaladnak a rejtett rétegeken (ha vannak ilyenek), és végül eléri a kimeneti réteget anélkül, hogy visszatérnének bármelyik korábbi rétegbe.

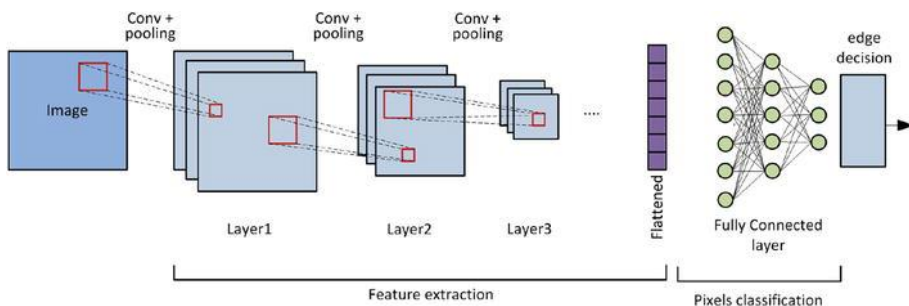
A CNN a vizuális adatok, mint például képek és videók feldolgozására és elemzésére tervezett neurális hálózattípus. A számítógépes látás területén központi szerepet tölt be, alapvetően megváltoztatva azt, ahogyan a gépek képeket érzékelnek és elemeznek.

Egy CNN több rétegből tevődik össze, amelyek különféle műveleteket hajtanak végre a bemeneti adatokon, és konvolúciós rétegeket használnak a bemeneti képekből történő jellemzők kinyerésére. A konvolúciós műveletek során egy tanulásra képes szűrőkészletet alkalmaznak a bemeneti képen, ami olyan jellemzőtérképeket eredményez, amelyek rögzítik a kép tartalmának különböző aspektusait. A jellemzőtérképek méretét pooling rétegek csökkentik le, redukálva ezzel a hálózat térbeli dimenzióit és számítási komplexitását. A max-pooling és az átlag-pooling technikák gyakran használatosak erre a célra.

A jellemzők kinyerését követően a CNN-ek gyakran teljesen összekapcsolt rétegeket használnak a predikciók elkészítésére. Ezek a rétegek kombinálják a kinyert jellemzőket és előállítják a végső kimenetet, amelyek képosztályozási feladatokban például osztálycímkek lehetnek.¹⁵

Egy tipikus CNN architektúrája látható az ábrán, ahol a rétegek sorban végzik el az adatokon az előfeldolgozást, jellemzőkinyerést, és végül a kimeneti réteg adja meg a hálózat által generált eredményt.

¹⁵ BENHAJYOUSSEF, Anis –SAIDANI, Asma: Recent Advances on Image Edge Detection In CUEVAS, Francisco Javier – MAZZEO, Pier Luigi – BRUNO, Alessandro: *Digital Image Processing - Latest Advances and Applications*. London, IntechOpen, 2024. 6-9. o.



1. ábra: CNN architektúra sematikus váza¹⁶

A CNN-ekre jellemző továbbá, hogy a transfertanulást is használják, ahol előre betanított modelleket – mint például a VGG¹⁷, ResNet¹⁸, vagy Inception – finomhangolnak speciális feladatokra. Ez csökkenti a nagy modellek nulláról történő betanításának szükségességét, és javítja a teljesítményt.

A CNN-ek a képfeldolgozás területén főként az alábbi feladatok elvégzésére alkalmasak:

- Jellemzőkinyerés: A CNN-ek képesek azonosítani a képeken lévő fontos jellemzőket, amelyek elengedhetetlenek a további feldolgozási lépésekhez.
- Képszegmentálás: A CNN-ek képesek a képeket olyan területekre szegmentálni, melyek a feldolgozás szempontjából érdekesek, így lehetővé téve az objektumok pontos lokalizációját.

Objektumfelismerés: A CNN-ek képesek azonosítani és lokalizálni objektumokat a képeken. A népszerű Faster R-CNN¹⁹ és a YOLO²⁰-modellek gyakran alkalmazottak objektumfelismerésre.

- Képosztályozás: A CNN-eket elterjedten használják képek előre meghatározott kategóriákba sorolására, kiemelkedő pontosságuk miatt.
- Arcfelismerés: A CNN-ek jelentős szerepet játszanak az arcfelismerő rendszerek fejlesztésében, amelyek kiterjednek a biztonsági és biometrikus alkalmazásokra is.
- Stílusátvitel: A CNN-eket használhatják bizonyos művészeti stílusok más képekre történő átvitelére, alkalmazására, vizuálisan vonzó átalakítások létrehozására.

Az említett jellemzőket jelenleg az alábbi területeken hasznosítják:

- Önvezető autók rendszerei: CNN-ekre alapozott rendszerek tárgyfelismerés, sávfelismerés és útvonaltervezési feladatokra képesek. Az objektumok, gyalogosok és más járművek felismerése elengedhetetlen a biztonságos autonóm vezetés terén.

¹⁶ Forrás: BENHAYOUSSEF – SAIDANI 2024, 7.

¹⁷ VGG – Visual Geometry Group

¹⁸ ResNet – Residual Network

¹⁹ R-CNN – Region-Based Convolutional Neural Network

²⁰ YOLO – You Only Look Once

- Orvosi képelemzés: A CNN-ek segítséget nyújtanak a képi diagnosztikában. Azonosítani képesek röntgenfelvételeken, MRI²¹-ken és CT²²-vizsgálati képeken különféle anomáliákat, valamint szegmentálási feladatokra is alkalmasak (pl. szervek, daganatok).
- Kereskedelem: A CNN-eket képalapú termékelismerésre és ajánló rendszerek működtetésére használják.
- Mezőgazdaság: A CNN-eket növény megfigyelésre, betegségfelismerésre és terméshozam-becslésre használják, drónokkal vagy műholdakkal készített képek elemzésével.²³

Generatív ellenfél hálózatok (GAN)

A GAN-ok, vagyis generatív ellenfél hálózatok, egy olyan neurális hálózat architektúra típust jelölnek, amelyet 2014-ben vezettek be. Egy GAN-ban két neurális hálózat verseng egymással, zéró összegű játék formájában, azaz az egyik ágens nyeresége a másik ágens vesztesége. Egy betanító halmaz alapján ez a technika megtanul új adatokat generálni, amelyek statisztikailag megegyeznek a betanító halmazzal. Például egy fotókon betanított GAN képes új fényképeket generálni, amelyek legalább felületesen hitelesnek tűnnek az emberi megfigyelők számára. Bár eredetileg a nem felügyelt tanulás generatív modelljeként javasolták, a GAN-ok hasznosnak bizonyultak félig felügyelt tanulásban, teljesen felügyelt tanulásban és megerősítéses tanulásban is.

A GAN-ok elsődlegesen adatgenerálásra lettek tervezve. Ezek a hálózatok képesek olyan adatokat és képeket generálni, amelyek rendkívül valóságűek, olyannyira, hogy gyakran megkülönböztethetetlenek a valódi adatoktól.

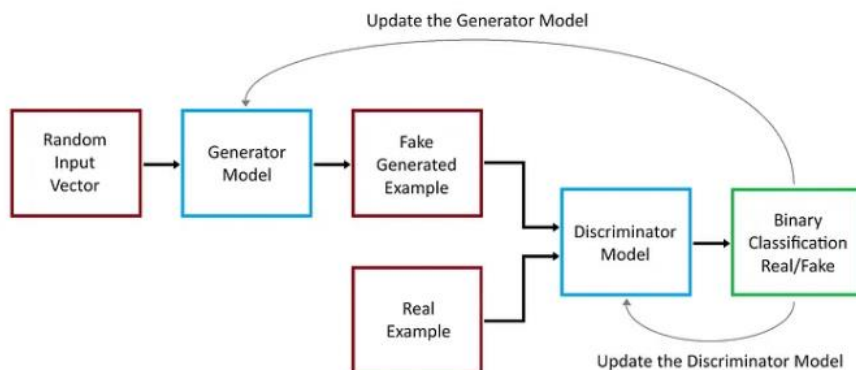
Az ellenfélalapú képzési módszer két összekapcsolt neurális hálózattal a GAN-ok legfőbb újítása, amelyben a generátor és a diszkriminátor folyamatosan versengenek egymással. A generátor feladata a realiztikusnak látszó adatok létrehozása, arra törekszik, hogy olyan valóságű adatokat készítsen, hogy a diszkriminátort kb. az esetek 50%-ában megtéveszse. Eközben a diszkriminátor folyamatosan fejleszti képességét a valódi és hamis adatok megkülönböztetésében. A generátor ellenfeleket generál a rendszer megtévesztésére, míg a diszkriminátor folyamatosan azon dolgozik, hogy azonosítsa és elkülönítse ezeket az ellenfeleket a valós képektől. Ez az együttműködés tehát egy egyedi tanulási folyamatot eredményez, ahol a GAN-ok ellenfélként működnek.²⁴

²¹ MRI – Magnetic Resonance Imaging – Mágneses rezonancia képalkotás

²² CT – Computed Tomography – Számítógépes tomográfia

²³ Sz.n.: CNN vs GAN: A Comparative Analysis in Image Processing for Computer Vision Systems. Sciotech, é.n.; BENHAJYOUSSEF 2024, 8-9.

²⁴ DEL PRA, Marco: Generative Adversarial Networks. Medium, 2023. október. 30.



2. ábra: GAN működési modellje²⁵

A GAN-ok különösen alkalmasak valós idejű környezetekben történő használatra és magas felbontású képek generálására, mivel a generátor fokozatosan tanulja meg javítani a pixelértékeket. A GAN-oknak számos változata létezik, mint például a DCGAN,²⁶ cGAN,²⁷ Cross-GAN²⁸ és IDSGAN,²⁹ a CycleGAN³⁰-ok és a StyleGAN³¹-ok, amelyeket különféle célokra és alkalmazásokra fejlesztettek, így biztosítva az adott technológiai igényeknek történő megfelelést. A konvolúciós rétegeket használó DCGAN-ok megjelenése fontos mérföldkő volt, különösen hatékonyak magas minőségű, valóság-hű képek generálásában. A CycleGAN ismert felhasználása a képi esztétika átalakítása, a hiper-realisztikus emberi arcok szintézisében a StyleGAN kiemelkedő.

Számos tanulmány dicséri a GAN-ok rugalmasságát, a rendszer biztonságát, az alkalmazkodóképességüket más eszközökkel/alkalmazásokkal való együttműködésben, valamint képességüket arra, hogy magas felbontású képek nagy adathalmazain tanuljanak. Az okklúziók és képfelbontási problémák megoldására is alkalmasak.³²

A GAN-ok a képfeldolgozás területén főként az alábbi feladatok elvégzésére alkalmasak:

²⁵ Forrás: DEL PRA 2023

²⁶ DCGAN – Deep Convolutional Generative Adversarial Network

²⁷ cGAN – Conditional Generative Adversarial Network

²⁸ Cross-GAN – Cross-Domain Generative Adversarial Network

²⁹ IDSGAN – Identity-Preserving Generative Adversarial Network

³⁰ CycleGAN – Cycle-Consistent Generative Adversarial Network

³¹ StyleGAN – Style-Based Generative Adversarial Network

³² AL JABERI, Saeed Matar – PATEL, Asma – AL-MASRI, Ahmed N.: *Object tracking and detection techniques under GANN threats: A systemic review*. Applied Soft Computing, 2023/139., 11-12. o.; és DEL PRA 2023.

- Képgenerálás: A GAN-ok egyik legismertebb jellemzője arról, hogy magas minőségű, szintetikus képeket képesek generálni. Ez hasznos lehet realiztikus, számítógéppel generált környezetek létrehozásában, művészeti alkotások létrehozásában és egyéb képfeldolgozási feladatokban is.
- Kép-kép transláció: A kondicionális GAN-ok olyan feladatok végrehajtásában használhatók, mint például a műholdas képek térképekké konvertálása vagy vázlatok fotóvá alakítása. Ezek a hálózatok megtanulják, hogyan alakíthatók egymásba az egyes képtípusok.
- Szuperfelbontás: A GAN-ok a kép felbontás és képminőség javításában is kiválóak. Alacsony felbontású képek alapján nagy felbontású változat generálására használhatók.
- Stílusátvitel: A GAN-ok alkalmazhatók kreatív feladatokra, például egyik kép művészeti stílusa alapján másik kép átformálására. A StyleGAN különösen megfelelő erre a feladatra.
- Adatnövelés: A számítógépes látás feladatokban gyakorta előfordul, hogy korlátozott a rendelkezésre álló adat. A GAN-ok különösen hasznos jellemzője, hogy a képzési adatkészleteket további, szintetikus adatok generálásával képesek kiegészíteni.

A GAN-ok említett jellemzőit jelenleg főként az alábbi területeken hasznosítják:

- Művészeti alkotás generálás: A GAN-ok művészeti alkotások készítésében újfajta kreatív eszközként használhatók (pl. festmények, zene, irodalmi művek).
- Deepfake: A GAN-ok deepfake technológia hasznos eszközei, képesek manipulálni és megváltoztatni videókat és képeket.
- Orvosi kép szintetizálás: A GAN-ok szintetikus orvosi képeket generálását is elvégzik, amelyek kutatási vagy képzési célokra hasznosíthatók, orvosi állapotok szimulálásában, valamint gépi tanulási modellek adatkészleteinek bővítésében is szerepük lehet.
- Divat és dizájn: A divatszakmában ruhatervezésre, személyre szabott ajánlásokra és szövetek megjelenésének szimulálására alkalmaznak GAN-okat.

CNN vs. GAN a képfeldolgozásban

A képfeldolgozás és a számítógépes látás területén a CNN-ek és a GAN-ok majdhogynem egyedülállóak erősségeik és sokszínű alkalmazási módjuk tekintetében. A CNN-ek alapvető szerepet töltenek be olyan feladatok ellátásában, amelyek jellemzőkinyerést, objektumfelismerést és képklasszifikációt igényelnek. A GAN-ok viszont a képgenerálásban és manipulálásban érnek el kiemelkedő eredményeket. Ezek a technikák olyan területeken bizonyulnak hasznosnak, ahol műalkotások generálása, deepfake-technológia vagy a kép-kép átalakítás áll a középpontban.

A GAN-ok különösen alkalmasak valós idejű környezetekben történő használatra, mivel szemben a CNN-ekkel, amelyek kis objektumok észlelésében jók, a GAN-ok sokkalta skálázhatóbbak.

A CNN-ek és GAN-ok képfeldolgozásban hasznosítható főbb jellemzőit összesíti a következő táblázat.³³

Tulajdonság	CNN-ek	GAN-ok
Jellemzőkinyerés	Konvolúciós rétegeket használ a hierarchikus jellemzők kinyerésére, erős előnyt biztosítva.	Nem elsődleges célja a jellemző kinyerés, inkább adatgenerálásra összpontosít.
Adatgenerálás	Nem gyakori alkalmazási mód, de egyes CNN variánsok, mint a Variational Autoencoder-ek, alkalmazhatók erre a feladatra.	Kiválóak szintetikus adat generálásra, realiztikus képek létrehozására, szuperfelbontásra és stílusátvitelre.
Tanulás átvitel	Kiválóak erre a feladatra. Előre betanított modellek elérhetők, ezek finomhangolhatók specifikus feladatokra.	Ritkábban használják erre, de néhány előre betanított modell elérhető.
Diszkriminatív vagy generatív modell	Diszkriminatív, adat felismerésére és osztályozására fókuszál.	Generatív, új, a valóditól nehezen megkülönböztethető szintetikus adatok létrehozására tervezték.
Realizmus és minőség	Nem generálnak képeket, meglévő képeket dolgoznak fel.	Realisztikus képek generálására képesek, mérföldkövet jelentenek ezen a területen.
Számítási komplexitás	Betanítás folyamán magas, de betanítás után gyors előrejelzésekre képesek.	Szintén magas a betanítás folyamán, de a képek generálása is jelentős erőforrást igényel.
Etikai és biztonsági aggályok	Magánéleti, torzítási és megfigyelési aggályok merülnek fel, pl. arcfelismerés kapcsán.	Rengeteg aggályt vetnek fel a deepfake generálás lehetősége miatt.

1. táblázat: CNN és GAN hálózatok főbb jellemzőinek összehasonlítása képfeldolgozási alkalmazás céljára³⁴

A konkrét számítógépes látási feladat specifikus igényei határozzák meg, hogy a CNN-eket vagy a GAN-okat érdemes-e alkalmazni. Míg a CNN-ek ideálisak olyan feladatokhoz, ahol a meglévő adatok felismerése és elemzése a cél, addig a GAN-okat ott részesítik előnyben, ahol az adatgenerálás, képszintézis és a kreatív kifejezés áll a középpontban.

³³ Sz.n.: CNN vs GAN: A Comparative Analysis in Image Processing for Computer Vision Systems.

³⁴ saját szerkesztés a SCIOTEX: i. m. alapján

E két technológia gyakran egymást kiegészítve is működhet egy adott rendszeren belül. Bizonyos alkalmazásokban a CNN-ek biztosíthatják a jellemzőkinyerést, míg a GAN-ok a szintetikus adatok generálását végzik, például adatkészlet-kiegészítés vagy stílusátvitel céljából.

Ahogy a számítógépes látás szakterület tovább fejlődik, mind a CNN-ek, mind a GAN-ok kulcsszerepet játszanak majd a vizuális észlelés és megértés jövőjének formálásában. Ezek a technológiák nemcsak megkönnyítik és hatékonyabbá teszik a képfeldolgozást, hanem új lehetőségeket is megnyitnak a kreatív kifejezés és a mesterséges intelligencia alkalmazásai terén.

Neurális hálózat modellek értékelése a képfeldolgozásban

Ahogy az előzőekben leírtakból már érzékelhető, a digitális képfeldolgozás területén számos DL módszer fellelhető, amelyek olyan feladatokat végeznek, mint a zajcsökkentés, képjavítás, szegmentáció, jellemzőkinyerés és osztályozás. Mindegyik módszer hozzájárul a képek megértésének javításához, az alapvető információk kinyeréséhez és a vizuális adatok alapján megalapozott döntések meghozatalához.

A képfeldolgozási művelet során a gerinchálózatok olyan alaparchitektúrákat jelentenek, amelyeket a mély neurális hálózatok kiindulási konfigurációiként használnak. Ezek a gerinchálózatok szolgáltatják azt az alapot, amelyre speciálisabb architektúrák és algoritmusok épülnek a különféle képfeldolgozási feladatok hatékony végrehajtásához. A legnépszerűbb gerinchálózat a VGG-k, a ResNets és az Inception v1 – GoogleNet.³⁵

A közelmúltban több tanulmány született a képfeldolgozásban alkalmazott DL-modellekről. Archana és Jeevaraj néhány hónapja publikált átfogó tanulmányt a témában, mely a képfeldolgozás részfolyamataiban átfogó értékelésre tett kísérletet a jelenleg használt modellek körében.

A képi zajcsökkentés terén kiemelkedőnek találunk olyan technikákat, mint a Self2Self NN,³⁶ a Denoising CNN³⁷-ek, a DFT-Net³⁸ és az MPR-CNN,³⁹ amelyek csökkentett zajszintet kínálnak, miközben az adatrövelés és paraméterhangolás kihívásaival küzdenek.

A Self2Self NN egy speciális deep learning modell, amely sem a CNN-ek, sem a GAN-ok közé nem sorolható be egyértelműen. Ez a modell önszupervíziós tanulást alkalmaz, ahol saját bemeneti képéből tanul zajcsökkentési célokkal, külső címkézett adatok nélkül. Főként képzajcsökkentésre és képrekonstrukcióra használják. A mélytanulási

³⁵ BENHAJYOUSSEF 2024, 9.

³⁶ Self2Self NN – Self-Supervised Denoising Neural Network

³⁷ Denoising CNN – Denoising Convolutional Neural Network

³⁸ DFT-Net – Discrete Fourier Transform Network

³⁹ MPR-CNN – Multiple Pattern Representation Convolutional Neural Network

modellek között a Self2Self NN különlegessége, hogy az adatrövidítés dependenciájának csökkentésével mérsékli a költségeket a képzajcsökkentés területén.

A DFT-Net egy neurális hálózat, amelyet a diszkrét Fourier-transzformáció megvalósítására terveztek. Ez a hálózat nem tartozik a hagyományos CNN-ek vagy GAN-ok közé. A DFT-Net célja, hogy a DFT számításait hatékonyan és párhuzamosan végezze el, lehetővé téve az adatok előfeldolgozását vagy frekvenciatartományban történő elemzését. A DFT-Net kezelni tudja a képcímkek egyensúlytalanságát, miközben fennáll a részletek elvesztésének kockázata. Gyakran használják olyan feladatokban, ahol a frekvenciatartomány információi fontosak, például jelfeldolgozásban vagy spektrális elemzésben.

A Denoising CNN-ek speciális CNN-ek, amelyeket zajcsökkentésre terveztek. Ezek a hálózatok képesek eltávolítani a zajt a képekről, megőrizve a fontos részleteket és jellemzőket. A Denoising CNN-ek tehát pontosságot növelnek, miközben erőforrás-kihívásokat jelent a használatuk. Különösen hasznosak olyan alkalmazásokban, ahol a képminőség javítása kritikus, például orvosi képalkotásban, távérzékelésben és biztonsági rendszerekben.

Az MPR-CNN-t kiemelkedő robusztusság és finomhangolható hiperparaméterek jellemzik. Többféle mintázat-reprezentációs algoritmust alkalmaz az adatok előzetes jellemzőinek kinyerésére. Speciálisan úgy tervezték, hogy hatékonyan tanuljon különböző mintázatok alapján, és az előzetesen kinyert jellemzőket felhasználja a további feldolgozási feladatokhoz.

A képjavítást elősegítő megközelítések, mint az R2R⁴⁰ és az LE-net,⁴¹ a vizuális minőség javításának lehetőségét kínálják, bár a valós világ jeleneteinek összetettsége és a képi hitelesség problémái fennállnak.

Az R2R algoritmust, amely sem GAN-ok, sem CNN-ek közé nem sorolható, azzal a céllal fejlesztették ki, hogy hatékonyabban csökkentse a zajt a képeken anélkül, hogy a tanulási folyamathoz szükség lenne valóság-hű (ground truth) képekre. Az R2R-zajcsökkentés egyensúlyt teremt az eredmények és a számítási igények között. Az R2R-módszer a zajos képek párosításával definiál egy költségfüggvényt, amely statisztikailag ekvivalens a felügyelt tanulásban használt zajos/valós képpárok költségfüggvényével. Ezzel a módszerrel sikerült jelentősen javítani az önfelügyelt zajcsökkentők teljesítményét, és versenyképes eredményeket értek el a felügyelt zajcsökkentőkkel szemben.⁴²

⁴⁰ R2R – Reconstructing to Recognize

⁴¹ LE-Net – Light Enhancement Network

⁴² PANG, Tongyao – ZHENG, Huan – QUAN, Yuhui – Ji, Hui: Recorruped-to-Recorruped: Unsupervised Deep Learning for Image Denoising. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Nashville, TN, USA, 2021., 2045. o.

Az LE-Net, amely sem GAN-ok, sem CNN-ek közé nem sorolható, egy olyan képfeldolgozási feladatokra optimalizált neurális hálózat, amelyet általában a képek világosságának és kontrasztjának javítására használnak. Alacsony fényviszonyok mellett készült képeket javítására használható, így azok részletgazdagabbá és vizuálisan jobb minőségűvé válnak.

A képszegmentálási technikák, mint a PSPNet⁴³ és a Mask-RCNN,⁴⁴ az objektumizolációban kiemelkedően pontosak, miközben olyan összetett feladatokban is igéretesek, mint az átfedő objektumok problémaköre és a robusztusság kérdései.

A PSPNet egy speciális, szegmentálási feladatokra készült CNN. Hatékonyan kezeli a különböző méretű objektumokat és a kontextusokat a képek szegmentálásakor. Ezt egy piramis pooling modullal éri el, amely különböző méretarányokban aggregálja a globális kontextus információit, javítva a hálózat képességét a részletes és pontos szegmentációra.⁴⁵

A Mask R-CNN egy objektumdetektálásra és képszegmentálásra tervezett CNN, amely az R-CNN család tagja. Ez a hálózat a Faster R-CNN továbbfejlesztett változata, és nemcsak az objektumokat detektálja, hanem pixelpontos maszkokat is készít az egyes objektumokhoz. Ezzel ötvözi az objektumdetektálást és a szegmentálást egyetlen modellben.⁴⁶

A jellemzőkinyerés terén olyan hálózatok, mint a CNN-ek és az HLF-DIP,⁴⁷ az automatizált felismerést teszik lehetővé, ám gyakran kompromisszumot kell kötni az értelmezhetőség és az összetettség között. A CNN-architektúrák hatékonyan gátolják meg a túllillesztést a zajmentesítési folyamat során.

A Faster R-CNN algoritmus két egységet használ: az első egy FCN⁴⁸, amely a javasolt régiókat határozza meg, a második egység pedig a megtaláló. A rendszer egy egységként működik az objektumészlelési feladat során. A Faster R-CNN alkalmas nagy területeken tárgyak észlelésére, például parkolók megfigyelésére.⁴⁹

⁴³ PSPNet – Pyramid Scene Parsing Network

⁴⁴ Mask-RCNN – Mask Region-Based Convolutional Neural Network

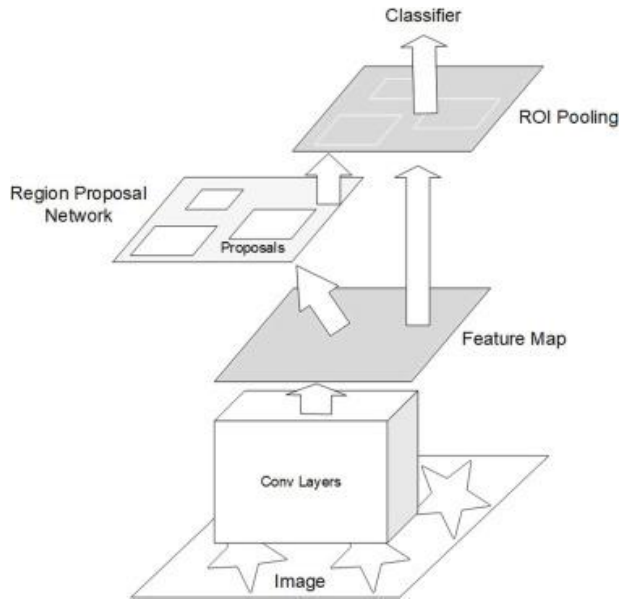
⁴⁵ ZHAO, Hengshuang – SHI, Jianping – QI, Xiaojuan – WANG, Xiaogang – JIA, Jiaya: Pyramid Scene Parsing Network. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Honolulu, HI, USA, 2017., 6230. o.

⁴⁶ HE, Kaïming – GKIÖXARI, Georgia – DOLLÁR, Piotr – GIRSHICK, Ross: Mask R-CNN. *IEEE International Conference on Computer Vision (ICCV)*, Venice, Italy, 2017., 2980. o.

⁴⁷ HLF-DIP – Huber Loss Function with Deep Image Prior

⁴⁸ FCN – Fully Convolutional Network

⁴⁹ AL JABERI 2023.



3. ábra: Faster R-CNN architektúra⁵⁰

Az HLF-DIP egy speciális mélytanulási algoritmus, amelyet hiperspektrális képek zajcsökkentésére használnak. A DIP-technikára épül, és a Huber veszteségfüggvényt használja. Az HLF-DIP előzetes betanítás nélkül, hatékonyan csökkenti a zajt a képeken, javítva ezzel a képminőséget. Ennek a kombinációnak köszönhetően a jellemzőkinyerés során csökkenthetők a túlillesztés és a zaj okozta problémák, miközben megőrzi a kép részleteit és minőségét. Ez különösen hasznos lehet olyan alkalmazásokban, ahol a képminőség és a zajcsökkentés egyaránt fontos.⁵¹

Az osztályozási technikák, mint például a ResNet és a CNN-LSTM,⁵² különösen ígéretesek a pontos osztályozás terén. Ezek a módszerek azonban számos kihívással néznek szembe, beleértve az adatfüggőséget, a számítási komplexitást és a modellek értelmezhetőségét.

A ResNet egy CNN-típusú hálózat, amely 2015-ben kimagasló újításként jelent meg a számítógépes látás és a mélytanulás területén. Különlegessége az „identity shortcut connection”, azaz az átugrások kapcsolata, amely lehetővé teszi, hogy a hálózati rétegek kihagyjanak bizonyos rétegeket, és közvetlenül továbbítsák az információt egy másik rétegbe. Ez a mechanizmus segít megoldani a degradációs problémát, amely a mély hálózatok teljesítményének romlásához vezethet, különösen akkor, amikor a hálózat száz vagy akár ezer réteget is magában foglal.

⁵⁰ Forrás: AL JABERI 2023.

⁵¹ NIRESI, Keivan Faghieh – CHI, Chong-Yung: Unsupervised Hyperspectral Denoising Based on Deep Image Prior and Least Favorable Distribution. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 2022/15., 5967. o.

⁵² CNN-LSTM – Convolutional Neural Network – Long Short-Term Memory

A ResNet használatával például többosztályos osztályozással 99%-os pontosság érhető el például MRI-képek osztályozásában. A ResNet, köszönhetően az erős reprezentációs képességének, kiemelkedő jelentőségre tett szert a számítógépes látás különböző feladataiban, mint az objektumfelismerés, arcfelismerés és képosztályozás.⁵³

A CNN-LSTM egy hibrid neurális hálózati architektúra, amely ötvözi a CNN-t és az LSTM előnyeit, amely speciális típusú, visszacsatolt neurális hálózat. Ebben a megközelítésben a CNN-eket használják az adatok térbeli jellemzőinek kinyerésére, majd az LSTM-eket az időbeli vagy sorozatos mintázatok feldolgozására. Ez a kombináció különösen hasznos olyan alkalmazásokban, ahol mind a térbeli, mind az időbeli jellemzők fontosak, például videóelemzés, mozgásfelismerés és többdimenziós időbeli adatok feldolgozása. Orvosi alkalmazásokban (pl. diabeteses retinopathia felismerés) 95% feletti pontosságot képesek elérni a CNN-LSTM használatával.⁵⁴

A YOLO egy olyan CNN-típus, amely kifejezetten valós idejű objektumdetektálásra lett kifejlesztve. A YOLO-architektúra egyedülálló jellemzője, hogy egyetlen lépésben képes az objektumok lokalizálására és osztályozására, ellentétben más, több lépésben vagy fázisban dolgozó módszerekkel. Ez a megközelítés teszi a YOLO-t rendkívül gyors és pontos detektálási eszközzé, így kiemelkedően hasznos olyan alkalmazásokban, ahol az idő kritikus tényező, mint például a valós idejű videófeldolgozás.

A YOLO számos különböző modellben használatos a tárgykövetésre és -azonosításra, és az egyszerűsége ellenére ígéretes alkalmazást nyújt valós idejű környezetekben. A teljes képeken történő betanítás és a célobjektumok egyszerűsített reprezentációja lehetővé teszi, hogy a YOLO gyorsan azonosítsa a tárgyakat. Azonban a nagy adatkészletek és teljes képek korlátozott elérhetősége jelentős kihívást jelenthet, amikor YOLO-t használnak objektumdetektálásra. Emiatt a YOLO-modellek fejlesztőinek nagyfokú szakértelemre van szükségük ahhoz, hogy képesek legyenek kezelni ezeket a korlátozásokat, beleértve a képzés során történő manuális címkézést is.

A YOLOv3 továbbfejlesztett változata hatékonyan és pontosan képes több kis objektum észlelésére a deep-sort megközelítésen keresztül, bár a deep-sort hatékonysága valós idejű környezetben vitatott. Alternatív megoldásként a KCF⁵⁵ használata javasolt, amely csökkenti a számítási komplexitást a tárgykövetés és -azonosítás során, tovább erősítve a YOLO adaptációs képességét különféle kihívásokra.⁵⁶

⁵³ ISMAEL, Sarah Ali Abdelaziz – MOHAMMED, Ammar – HEFNY, Hesham: An enhanced deep learning approach for brain cancer MRI images classification using residual networks. *Artificial Intelligence in Medicine*, 2020/102. 1.o; BENHAJYOUSSEF 2024.

⁵⁴ BENHAJYOUSSEF 2024, 11-28.

⁵⁵ KCF – Kernelized Correlation Filter

⁵⁶ AL JABERI 2023.

A modern képfeldolgozás jövőbeli irányai

A digitális képfeldolgozó rendszereket jelenleg a legkülönbözőbb kontextusokban használják, és egyre lenyűgözőbb eredményeket képesek elérni alkalmazásukkal. A modern képfeldolgozásban az AI alkalmazása lehetővé teszi a képek különböző algoritmusok segítségével történő feldolgozását, manipulálását és javítását. Az elmúlt néhány évben exponenciálisan megnövekedett az érdeklődés a DL-módszereket alkalmazó képfeldolgozó rendszerek iránt. A digitális képfeldolgozás területén a képzajcsökkentés, javítás, szegmentálás, jellemzőkinyerés és osztályozás feladatokra jelenleg alkalmazott mesterséges intelligencia, DL-alapú módszerek széles köre elérhető. Jelen tanulmány nemcsak az egyes technikák egyedi erősségeit emeli ki, hanem rámutat az alkalmazásukkal járó kihívásokra is.

A hagyományos ML-módszerek a képfeldolgozásban továbbra is gyakran használatosak olyan területeken, mint például a betegségek diagnosztizálása és előrejelzése vagy speciális feladatok segítése, ám gyakran más, összetettebb AI-módszerekkel párosulnak.

Az AI és DL fejlődése a képfeldolgozást számos iparágban megújítja és tökéletesíti, beleértve az orvostudományt, a mérnöki tudományokat, a biztonsági ipart, a mezőgazdaságot, a gyártást és a közlekedést. Kutatási fókuszterületekként azonosítható az orvostudomány, az önvezető autók, de a grafikus keresőmotorok és a tartalomalapú képkereső rendszerek is a képfeldolgozás érdekes kutatási témájaként jelennek meg.

A szakirodalom alapján megállapítható, hogy a kutatók a konkrét, valós problémák megoldásában a modellek teljesítményének javítására, a számítási erőforrások és idő csökkentésére, valamint a modellek alkalmazásának kiterjesztésére összpontosítanak. A terület előtt álló kihívások között említik a DL-technikák finomítását az objektumfelismerés pontosabbá tételének és az objektumok kontextuális megértésének fejlesztése céljából, a 3D⁵⁷ képpalkotás és mélységérzékelés fejlesztését, amely a térbeli kapcsolatok és környezetek kifinomultabb értelmezését segíti, valamint a valós idejű feldolgozást támogató gyorsabb és hatékonyabb algoritmusok fejlesztését. Ugyanakkor olyan komplex irányok is megjelennek a képfeldolgozás és gépi látás kutatásában, mint a vizuális adatok kombinálása más szenzoros adatokkal (pl. hanggal) a látható információk komplexebb megértése érdekében.⁵⁸

Összefoglalva, az AI- és a mélytanulás-alapú technológiák alkalmazása a digitális képfeldolgozásban nemcsak új lehetőségeket teremt a különböző iparágak számára, hanem új kihívásokat is jelent, amelyek megoldása a kutatók és fejlesztők számára folyamatos innovációt és együttműködést igényel, valamint a felhasználók részéről az ismeretek és készségek folyamatos fejlesztését és a technológiai változásokhoz való alkalmazkodást követeli meg.

⁵⁷ 3D – Three dimensional – háromdimenziós

⁵⁸ VALENTE, Jorge – ANTÓNIO, João – MORA, Carlos – JARDIM, Sandra: Developments in Image Processing Using Deep Learning and Reinforcement Learning. *J. Imaging*, 2023/10., 1-22. o.

Felhasznált irodalom

AL JABERI, Saeed Matar – PATEL, Asma – AL-MASRI, Ahmed N.: *Object tracking and detection techniques under GANN threats: A systemic review*. Applied Soft Computing, 2023/139. DOI: 10.1016/j.asoc.2023.110224

ARCHANA, R. – JEEVARAJ, P. S. Eliahim: Deep learning models for digital image processing: a review. *Artificial Intelligence Review*, 2024/11, 1-33. o. Elérhető: <https://link.springer.com/article/10.1007/s10462-023-10631-z>
(Letöltés ideje: 2024. 05. 04.)

BENHAIYOUSSEF, Anis – SAIDANI, Asma: Recent Advances on Image Edge Detection In CUEVAS, Francisco Javier – MAZZEO, Pier Luigi – BRUNO, Alessandro: *Digital Image Processing – Latest Advances and Applications*. London, IntechOpen, 2024. DOI: 10.5772/intechopen.1003763

DEL PRA, Marco: Generative Adversarial Networks. Medium, 2023. október. 30. Elérhető: <https://medium.com/@marcodelp/generative-adversarial-networks-dba10e1b4424> (Letöltés ideje: 2024. 05. 20.)

DULARI, Bhatt – PATEL, Chirag – TALSANIA, Hardik – PATEL, Jigar – VAGHELA, Rasmika – PANDYA, Sharnil – MODI, Kirit – GHAYVAT, Hemant: CNN Variants for Computer Vision: History, Architecture, Application, Challenges and Future Scope. *MDPI Electronics*, 2021/20. Elérhető: <https://www.mdpi.com/2079-9292/10/20/2470> (Letöltés ideje: 2024. 05. 20.)

HE, Kaiming – GKIOXARI, Georgia – DOLLÁR, Piotr – GIRSHICK, Ross: Mask R-CNN. *IEEE International Conference on Computer Vision (ICCV)*, Venice, Italy, 2017. Elérhető: <https://ieeexplore.ieee.org/document/8237584> (Letöltés ideje: 2024. 05. 21.)

HRYNIEWICZ, Renata: *Seeing the Future: An Introduction to Computer Vision in AI*. 2024. január 10. Elérhető: <https://neurosys.com/blog/introduction-to-computer-vision-in-ai>
(Letöltés ideje: 2024. 04. 30.)

ISMAEL, Sarah Ali Abdelaziz – MOHAMMED, Ammar – HEFNY, Hesham: An enhanced deep learning approach for brain cancer MRI images classification using residual networks. *Artificial Intelligence in Medicine*, 2020/102. Elérhető: <https://pubmed.ncbi.nlm.nih.gov/31980109/> (Letöltés ideje: 2024. 04. 30.)

NIRESI, Keivan Faghih – CHI, Chong-Yung: Unsupervised Hyperspectral Denoising Based on Deep Image Prior and Least Favorable Distribution. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 2022/15. Elérhető: <https://ieeexplore.ieee.org/document/9813381> (Letöltés ideje: 2024. 05. 21.)

SARFRAZ, Muhammad (szerk.): *Digital Imaging*. London, IntechOpen, 2020. Elérhető: <https://www.intechopen.com/books/9239> (Letöltés ideje: 2024. 05. 20.)

SONKA, Milan – HLAVAC, Vaclav – BOYLE, Roger: *Image Processing, Analysis, and Machine Vision, Fourth Edition*. Cengage Learning, Stanford, USA, 2013. Elérhető: <https://www.cl72.org/090imagePLib/books/sonka,hlavac,boyle-imageProc.pdf>
(Letöltés ideje: 2024. 05. 20.)

SZEMENYEI Márton: *Számítógépes Látórendszerek*. Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar, Irányítástechnika és Informatika Tanszék, 2022. Elérhető: https://vik.wiki/images/1/15/Szl_jegyzet.pdf (Letöltés ideje: 2024. 05. 20.)

Sz.n.: CNN vs GAN: A Comparative Analysis in Image Processing for Computer Vision Systems. Sciutex, é.n. Elérhető: <https://sciotex.com/cnn-vs-gan-a-comparative-analysis-in-image-processing-for-computer-vision-systems/> (Letöltés ideje: 2024. 05. 20.)

TOMAYKO, James E: *Computers in Spaceflight: The NASA Experience*. Kansas, NASA, 1988. Elérhető: <https://ntrs.nasa.gov/citations/19880069935> (Letöltés ideje: 2024. 05. 15.)

PANG, Tongyao – ZHENG, Huan – QUAN, Yuhui – Ji, Hui: Recorrupted-to-Recorrupted: Unsupervised Deep Learning for Image Denoising. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Nashville, TN, USA, 2021. Elérhető: <https://ieeexplore.ieee.org/document/9577798> (Letöltés ideje: 2024. 05. 15.)

VALENTE, Jorge – ANTÓNIO, João – MORA, Carlos – JARDIM, Sandra: Developments in Image Processing Using Deep Learning and Reinforcement Learning. *J. Imaging*, 2023/10., 1-22. o. Elérhető: <https://www.mdpi.com/2313-433X/9/10/207> (Letöltés ideje: 2024. 05. 20.)

ZHAO, Hengshuang – SHI, Jianping – Qi, Xiaojuan – WANG, Xiaogang – JIA, Jiaya: Pyramid Scene Parsing Network. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Honolulu, HI, USA, 2017. Elérhető: <https://ieeexplore.ieee.org/document/8100143> (Letöltés ideje: 2024. 05. 20.)

DR. MAGYAR SÁNDOR¹ – Dr. BÁNYÁSZ PÉTER² – BÁNYÁSZ-VÁCZI KINCSŐ BORÓKA³ – PÁL ANITA⁴

MAGYARORSZÁG KIBERVÉDELMI STRATÉGIÁINAK ÖSSZEHOSONLÍTÁSA ÉS FEJLŐDÉSI ÍVE 2013 ÉS 2025 KÖZÖTT

A tanulmány Magyarország kibervédelmi stratégiáinak fejlődési ívét vizsgálja 2013 és 2025 között. Elemzi, hogyan alakult át a nemzeti kiberbiztonsági gondolkodás az elvi és deklaratív megközelítésektől a technológiailag megalapozott, társadalmi szereplőket integráló stratégiai szemlélet felé. A kutatás összehasonlító módszerrel elemzi a három releváns kormányzati dokumentumot, kiemelve azok nemzetközi illeszkedését, a digitális szuverenitás narratívájának változását és az intézményfejlesztési folyamatokat. A szerzők arra a következtetésre jutottak, hogy Magyarország nemcsak alkalmazkodó, hanem alakító szereplővé is válhat a nemzetközi kibertér szabályozásában, ha saját fejlesztéspolitikai eszközeit stratégiai módon illeszti az EU és a NATO elvárásaihoz.

Kulcsszavak: kiberbiztonság, stratégia, reziliencia, digitális szuverenitás, hibrid fenyegetések

DIGITAL SECURITY AND ADAPTATION: THE DEVELOPMENT PATH OF HUNGARY'S CYBERSECURITY STRATEGIES BETWEEN 2013 AND 2025

The study explores the thematic evolution of Hungary's national cybersecurity strategies between 2013 and 2025. It examines how the country's approach shifted from declarative frameworks toward a more operational, technologically grounded and socially integrated model. The research compares three key strategy documents, analysing their alignment with international standards, the inclusion of societal actors, and the role of digital sovereignty. Particular attention is paid to the strategic incorporation of EU and NATO cybersecurity expectations. The paper concludes that Hungary's cybersecurity thinking reflects increasing maturity, and argues that Hungary could play not only a participating but also a shaping role in international cybersecurity governance through sovereign software development and sector-specific risk assessment systems.

Keywords: cybersecurity, strategy, resilience, digital sovereignty, hybrid threats

¹ ORCID-azonosító: 0000-0002-6085-0598, MTMT-azonosító: 10045839

² ORCID-azonosító: 0000-0002-7308-9304, MTMT-azonosító: 10033398

³ ORCID-azonosító: 0009-0008-4824-0923, MTMT-azonosító: 10096282

⁴ ORCID-azonosító: 0000-0003-4750-193X, MTMT-azonosító: 10088363

Bevezetés

A kiberbiztonsági dokumentumok meghatározó jelentőséggel bírnak a nemzeti szintű kiberbiztonsági politikák és stratégiák megalapozásában, mivel rendszerszintű keretet biztosítanak az elektronikus információs rendszerekben tárolt és továbbított információk védelmére. Ezen dokumentumok egyre nagyobb hangsúlyt fektetnek a kiberbiztonság szerepére, amely napjainkban már nem csupán az állami-, hanem a magánszektorhoz, valamint a honvédelmi szervezetekhez is szervesen kapcsolódik.^{5,6,7} A kiberbiztonsági szabályzók egyrészt stabil alapot kínálnak a komplex, nemzeti kiberbiztonsági szerkezet kialakításához, másrészt olyan fejlesztési irányvonalat képviselnek, amelyre a jövőbeni szabályozási mechanizmusok épülhetnek.⁸ A dokumentumok jelentősége továbbá abban is megmutatkozik, hogy hozzájárulnak az információs javak védelméhez, és következetes, multidiszciplináris megközelítést tesznek lehetővé a kiberbiztonság jogi, technológiai és szervezeti aspektusaiban.^{9,10}

A nemzeti kiberbiztonsági dokumentumok tartalmi struktúrájára jellemző, hogy konkrét problémakörökre és szűkebb fókuszú célterületekre irányulnak, amelyek megvalósítása többnyire lépcsőzetesen történik.¹¹ Emellett figyelembe veszik a globális biztonsági kihívások alakulását, az egyedi kibertérbeli események elemzését, valamint a technológiai innováció és fejlesztés stratégiai szerepét, ezáltal reflektálnak a nemzetközi biztonsági környezet folyamatos változásaira.^{12,13,14} A dokumentumok kiemelt figyelmet szentelnek a különböző szinteken – helyi, nemzeti és globális – megvalósuló együttműködési lehetőségeknek, különösen az informatikai rendszerek védelme és a létfontosságú infrastruktúrák megóvása tekintetében.^{15,16}

⁵ HARKNETT, Richard J. – STEVER, James A.: The new policy world of cybersecurity. *Public Administration Review*, 2011/3. 455–460. o.

⁶ KARAHAN, Saltuk – WU, Hongyi – ARMISTEAD, Leigh: *Evolution of US cybersecurity strategy*. In: *International Conference on Cyber Warfare and Security*. Academic Conferences International Limited, 2019. 168–176. o.

⁷ ELKHANNOUBI, Hasna – BELAISSAOUI, Mustapha: A framework for an effective cybersecurity strategy implementation: Fundamental pillars identification. *15th International Conference on Intelligent Systems Design and Applications (ISDA) 2015*. IEEE, 2015(a). 1–6. o.

⁸ HARKNETT – STEVER 2011, 455-460.

⁹ ELKHANNOUBI – BELAISSAOUI 2015(a), 1-6.

¹⁰ ELKHANNOUBI, Hasna – BELAISSAOUI, Mustapha: Fundamental pillars for an effective cybersecurity strategy. *IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA) 2015.*, IEEE, 2015(b). 1–2. o.

¹¹ HARKNETT – STEVER 2011, 455-460.

¹² KARAHAN – WU – ARMISTEAD 2019, 168-176.

¹³ KOVÁCS László – KRASZNAY Csaba: Digitális Mohács 3.0. *Hadtudomány*, 2024/3. 40-55. o.

¹⁴ KRASZNAY Csaba: *Taktikák és stratégiák a kiberhadviselésben*. Ludovika Egyetemi Kiadó, Budapest, 2023.

¹⁵ KSHETRI, Nir – MURUGESAN, San: EU and US cybersecurity strategies and their impact on businesses and consumers. *Computer*, 2013/10. 84–88. o.

¹⁶ ÇİFCİ, Hasan – ERGÜNER, Esmá: Analysis of National Cybersecurity Strategies of G20: objectives, latent themes, latest trends and comparisons. *Data & Policy*, 2025/e7.

A kiberbiztonsági dokumentumok érdemi hozzájárulást nyújtanak a nemzeti szintű stratégiai gondolkodás fejlődéséhez, ugyanis kijelölik a védekezés főbb súlypontjait, valamint tükrözik a döntéshozók és érintetti körök biztonság tudatos szemléletét.¹⁷ Ezen túlmenően kulcsszerepet játszanak a folyamatosan fejlődő, egyre kifinomultabb kiberfenyegetések kezelésében, illetve a társadalmakat és a gazdaságokat egyre inkább átható információs-kommunikációs technológiák iránti növekvő függőség mérséklésében.¹⁸ Világszerte egyre több ország fogalmaz meg és valósít meg ilyen típusú stratégiákat, amelyek elsődleges célja a kibertérből eredő kockázatokkal szembeni reziliens válaszok kidolgozása.¹⁹

Mindazonáltal a koherens, horizontálisan és vertikálisan is integrált kiberbiztonsági politika kialakítása nem mentes a kihívásoktól. Több esetben tapasztalható, hogy a stratégiák megvalósítását hiányos vagy életképtelen keretrendszerek akadályozzák, illetve a meglévő tervek túlságosan szegmentáltak és szakaszosan kerülnek bevezetésre.²⁰ A kibertámadások körül kialakult információs aszimmetria, valamint a szervezetek rezilienciát biztosító mechanizmusainak transzparenciahiánya tovább nehezíti az átfogó helyzetértékelést és a különböző szereplők közötti tudásmegosztást.²¹ A kiberbiztonsági érettség mérésére szolgáló modellek jelenlegi állapotukban több esetben általánosított eredményeket nyújtanak, és nem tükrözik kielégítően a valós kapacitásokat és képességeket.²²

A kiberreziliencia – azaz a szervezetek és államok azon képessége, hogy képesek adaptívan és konstruktívan reagálni a negatív kibereseményekre – új szemléleti dimenzióként jelenik meg a kiberbiztonsági érettség értékelésében. Ennek kialakulását az ismert és ismeretlen kockázatok elkerülhetetlensége is motiválja. A megfelelő szintű kiberreziliencia eléréséhez elengedhetetlen a nemzeti kiberbiztonsági stratégiák célorientált kidolgozása és implementációja, különös figyelemmel a kritikus infrastruktúrák és rendszerek védelmére.²³

A kiberbiztonság napjainkra nem csupán technológiai, hanem nemzetbiztonsági, gazdaságstratégiai és társadalmi kihívássá is vált. Magyarország kiberbiztonsági válaszai az elmúlt évtizedben folyamatos fejlődést mutattak. A 2013-as

¹⁷ KARAHAN – WU – ARMISTEAD 2019, 168-176.

¹⁸ AGYEMAND, Raymond – FURNELL, Steven – MULLER, Tim: A Profile-Based Cyber Security Readiness Assessment Framework at Country Level. *International Symposium on Human Aspects of Information Security and Assurance*. Springer Nature Switzerland, Cham. 2024. 93–106. o.

¹⁹ CRAM, W. Alec – YUAN, Jonathan: Out with the old, in with the new: examining national cybersecurity strategy changes over time. *Journal of Cyber Policy*, 2023/1. 26–47. o.

²⁰ HARKNETT – STEVER 2011, 455-460.

²¹ TSEN, Elinor – KO, Ryan KL – SLAPNICAR, Sergeja: An exploratory study of organizational cyber resilience, its precursors and outcomes. *Journal of Organizational Computing and Electronic Commerce*, 2022/2. 153–174. o.

²² AGYEMAND– FURNELL – MULLER 2024, 93-106.

²³ CRAM – YUAN 2023, 26-47.

Nemzeti Kiberbiztonsági Stratégia,²⁴ a 2018-as Hálózati és információs rendszerekre vonatkozó Stratégia,²⁵ valamint a 2025-ben megjelent Kiberbiztonsági Stratégia²⁶ – amely hatálytalanította az előző két dokumentumot – egyre komplexebb válaszokat adtak a kiberfenyegetettség többdimenziós kihívásaira.²⁷

A NATO kibervédelmi stratégiája – különösen a 2021-es frissítést követően – egyértelműen deklarálja, hogy a kibertér önálló műveleti területként kezelendő. A szövetség célja a kollektív védelem kiterjesztése a kibertámadásokra is, amelyek súlyos esetben aktiválhatják az 5. cikkelyt. A „NATO 2030” kezdeményezés részeként prioritást élvez a szövetséges tagállamok közötti interoperabilitás, a kritikus infrastruktúrák védelme, valamint a biztonsági műveleti központok és kibervédelmi gyakorlatok rendszerének fejlesztése.

Az Európai Unió 2020 végén hirdette meg a „Cybersecurity Strategy for the Digital Decade” című programját, amely az NIS2 irányelv végrehajtásán²⁸, az EU SOC-ok²⁹ hálózatának kiépítésén, valamint a Joint Cyber Unit (JCU) működtetésén keresztül kívánja megerősíteni a tagállamok kibereellenálló-képességét. A stratégiai célok 2030-ig terjedő horizonton belül valósulnak meg, szorosan kapcsolódva az EU digitális autonómia és szuverenitás narratívájához.

Magyarország 2025-ös Kiberbiztonsági Stratégiája ezekkel összhangban fogalmazza meg célkitűzéseit, valamint integrálja a NATO és az EU ajánlásait,³⁰ továbbá célként tűzi ki a hazai CSIRT³¹-, SOC- és ISAC³²-rendszerek megerősítését, a nemzeti szoftverfejlesztés támogatását és a mesterségesintelligencia-alapú védelem fokozatos bevezetését.

A kutatás során az alábbi célkitűzéseket fogalmaztuk meg:

KC1: A stratégiai szemléletmód tematikus fejlődésének vizsgálata. Célunk annak feltárása, hogyan változott a magyar kiberbiztonsági stratégiák fókusza a deklaratív és elvi szinttől a technológiai, majd társadalmi alapú megközelítésig.

²⁴ 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

²⁵ 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról

²⁶ 1089/2025. (III. 31.) Korm. határozat Magyarország Kiberbiztonsági Stratégiájáról

²⁷ KELEMEN Roland – FARKAS Ádám: *Nemzeti biztonság és kibertér*. Médiatudományi Intézet, Budapest, 2023. 44. o.

²⁸ KRASZNAY Csaba Dr.: A NIS2 irányelv kihívásai és gyakorlati alkalmazása. *Védelem Tudomány a Katasztrófavédelem online szakmai, tudományos folyóirata*, 2024/9.ksz. 1-5. o.

²⁹ SOC – Security Operations Centre – Biztonsági műveleti központ

³⁰ BIHALY, Barbara: Kibervédelem a NATO-ban és az EU-ban. *Hadtudományi Szemle*, 2022/4. 37-49. o.

³¹ CSIRT – Computer Security Incident Response Team – Számítógép-biztonsági incidenskezelő csoport

³² ISAC – Information Sharing and Analysis Centre – Információmegosztó és -elemző központok

KC2: A társadalmi szereplők integrációjának elemzése. Célunk annak vizsgálata, hogy milyen mértékben és milyen formában jelentek meg az állami, piaci és civil szereplők a stratégiákban az egyes időszakokban.

KC3: A nemzeti digitális szuverenitás diskurzusának alakulása. Végül célunk annak feltárása, hogy a nemzeti szuverenitás fogalma milyen súllyal és tartalommal jelent meg a stratégiai dokumentumokban.

KC4: Annak vizsgálata, hogy a 2013 és 2025 között megalkotott magyar kibervédelmi stratégiák milyen mértékben képesek reagálni a technológiai, geopolitikai és nemzetközi jogi környezet változásaira, különös tekintettel a NATO és az Európai Unió kiberbiztonsági elvárásaira, valamint a hazai intézményrendszer fejlődésére.

Fentiekből következően az alábbi kutatási kérdésekre keressük a válaszokat:

KK1: Milyen irányban változott a magyar nemzeti kiberbiztonsági stratégiák tartalmi fókusza 2013 és 2025 között?

KK2: Hogyan alakult a társadalmi szereplők (állami, piaci, civil) stratégiai szerepének bemutatása az egyes időszakok stratégiáiban?

KK3: Milyen tendenciák figyelhetők meg a digitális szuverenitás tematizálásában a három dokumentumban?

KK4: Hogyan illeszkednek a magyar kibervédelmi stratégiák (2013–2025) célkitűzései és intézményi fejlesztései az EU és NATO közötti kibervédelmi együttműködés követelményeihez, és milyen szerepet tölthet be Magyarország ezen a téren közreműködőként vagy alakítóként?

A kutatás során az alábbi hipotéziseket fogalmaztuk meg:

H1: A magyar kiberbiztonsági stratégiák tematikai fókusza egyre inkább elmozdult az elvi keretalkotástól a gyakorlatorientált, végrehajtásközpontú szemlélet felé.

H2: A társadalmi szereplők szerepe a stratégiákban 2013 és 2025 között jelentősen kiszélesedett, különösen a civil és üzleti szféra vonatkozásában.

H3: A digitális szuverenitás kulcskategóriája egyre erősebben jelent meg a stratégiákban, reflektálva a globális politikai és technológiai kihívásokra.

H4: Magyarország kibervédelmi stratégiái egyre szorosabban igazodnak a NATO és az EU elvárásaihoz, azonban a két szervezet közötti jogharmonizációs és interoperabilitási hiányosságok csak akkor kezelhetők hatékonyan, ha Magyarország saját fejlesztéspolitikáját stratégiai szinten integrálja a nemzetközi rendszerbe – ezáltal nemcsak követő, hanem alakító szerepet is betölthet.

Módszertan

A jelen elemzés három kormányhatározatban rögzített dokumentum strukturált és tartalmi összehasonlítására épül. A kiemelt témakörök vizsgálatának első lépéseként mindhárom elemzett stratégiai dokumentumban azonosítottuk a leggyakrabban előforduló kifejezéseket és trigramokat, azaz azokat a nyelvi elemeket, amelyek a szövegek tematikai súlypontjait tükrözhetik. Az elemzés célja az volt, hogy feltárja a

dokumentumok tartalmi fókuszait, valamint azok időbeli változásait, ezért elsődlegesen szógyakorisági elemzést alkalmaztunk.

A leggyakoribb szóalakok meghatározása során a dokumentumok teljes szövegét elemeztük, beleértve a lábjegyzeteket is, mert úgy véltük, hogy ezek az elemek is értékes kiegészítő információkat hordozhatnak a dokumentum témaköreiről. Az elemzés alapját a lemmatizált szavak képezték, vagyis a ragozott és különböző alakokban előforduló szavakat alapalakra hoztuk (pl. „védjük”, „védelem”, „védelmi” → „védelem”), ezzel biztosítva a jelentés szerinti összehasonlíthatóságot. A lemmatizálás egy természetes nyelvfeldolgozási (NLP) technika, amely a szavakat nyelvtani szempontból egységes formára alakítja, és ezáltal csökkenti a nyelvi változatosság miatti redundanciát.

Annak érdekében, hogy a számunkra tartalmilag irreleváns szavak – például névelők (a, az), kötőszók (és, vagy), segédigék (van, lesz), illetve gyakori, de tematikailag üres szavak – ne torzítsák az eredményeket, egy magyar nyelvű stop word listát alkalmaztunk. A stop word lista olyan gyakran előforduló szavakat tartalmaz, amelyek általában nem hordoznak lényegi információt az adott szöveg témájáról, így eltávolításuk segít a valóban releváns kulcsszavak kiemelésében.

Ezt követően azonosítottuk az ún. trigramokat, vagyis három egymást követő szóból álló kifejezéseket. A trigram-elemzés célja az volt, hogy ne csak az egyedi szavak, hanem a gyakori kifejezésstruktúrák és tematikus összefüggések is megjelenjenek az elemzésben. Az ilyen típusú n-gram alapú nyelvi vizsgálatok lehetővé teszik a stratégiai dokumentumokban jellemző nyelvi mintázatok és diskurzusok mélyebb megértését.

A fenti lépések együttes alkalmazása előkészítette a tematikus kulcsszó-kategóriák (például védelem, szuverenitás, együttműködés stb.) és a klaszterelemzés bevezetését, amely révén a dokumentumok belső szerkezete és szemléleti változásai is feltárhatóvá váltak.

Eredmények

Az elmúlt évtized kiberstratégiai fejlődése egy olyan rendszer kialakulását mutatja, amely egyre érzékenyebben reagál a nemzetközi trendekre, és amelyben a társadalmi, katonai, technológiai komponensek összehangolása megkezdődött. A 2025-ös stratégia már nemcsak az infrastruktúrák védelmére fókuszál, hanem a társadalmi reziliencia erősítésére is, hangsúlyozva a civil szereplők bevonását és a mesterséges intelligenciára épülő adaptív védelem fontosságát.

Magyarország kibervédelmi stratégiáinak fejlődése jól tükrözi a nemzetközi környezet komplexitását és a fenyegetettségi spektrum kiszélesedését. A külpolitikai szuverenitás-védelem, ha ötvöződik digitális képességfejlesztéssel és tudatos nemzetközi részvétellel, olyan normateremtő erővé válhat, amely nemcsak a belső védelmet erősíti, hanem stratégiai értéket is képvisel a nemzetközi térben.

A 2013-as stratégia megalapozó jellegű volt, amely a szuverenitás, a jogi szabályozás és a nemzeti védelmi rendszer kialakítását helyezte előtérbe. A kitűzött célok közül több is megvalósult, így létrejött a Nemzeti Kibervédelmi Intézet (NKI), és megerősödött a Kormányzati Eseménykezelő Központ. A jogi háttér is fejlődött, például az elektronikus információbiztonságról szóló 2013. évi L. törvény révén.

A 2018-as stratégia célkitűzései közül kiemelendő az ipari szereplők bevonása, amely részben megvalósult az ipari CSIRT-ek létrehozásával és a kritikus infrastruktúrákra vonatkozó kockázatelemzési követelmények meghatározásával. Előrelépés történt a tudatosságnövelés és az állampolgári edukáció terén is, többek között a kibervédelmi hónapok és kampányok révén.

A 2025-ös stratégia céljai közül még folyamatban van számos intézkedés, azonban már érzékelhető a mesterséges intelligenciára és dezinformációra fókuszáló szakpolitikai figyelem. A Nemzeti SOC-k (Security Operations Center) fejlesztése és az ISAC-ok (Information Sharing and Analysis Centers) hálózatosítása megkezdődött. A NIS2 irányelv implementációja folyamatban van, és az állami–piaci együttműködések szintén fejlődnek, különösen a kiberbiztonsági szolgáltatások tanúsítása és auditálása területén.

A magyar kibervédelmi stratégiák fejlődési íve világosan mutatja, hogy a kiberbiztonság már nem elkülönülten kezelendő szakpolitikai terület, hanem a nemzetbiztonsági stratégia szerves része. 2007 óta a geopolitikai környezet és a kibertér jellege is alapvetően megváltozott. A hibrid hadviselés, a digitális befolyásolási műveletek és a mesterséges intelligencia térnyerése új biztonsági kockázatokat hozott. Ebben a környezetben a nemzeti szuverenitás megőrzése csak akkor lehet hiteles és hatékony, ha a technológiai fejlesztések, különösen a szoftveres védelmi architektúrák nemcsak követik, hanem alakítják is a nemzetközi szabályozási trendeket.

Az 1. táblázat szemlélteti az intézményi együttműködés fokozatos bővülését, különösen a 2025-ös stratégia esetében, ahol már megjelennek a speciális incidenskezelő csoportok (CSIRT-ek), biztonsági műveleti központok (SOC-ok), valamint az információmegosztó és elemző központok (ISAC-ok) is.

Intézmény	2013-as Stratégia	2018-as Stratégia	2025-ös Stratégia
Nemzeti Biztonsági Felügyelet (NBF)	✓	✓	✓
Nemzeti Kibervédelmi Intézet (NKI)	✓	✓	✓
Kormányzati Eseménykezelő Központ	✓	✓	✓
Elektronikus Információbiztonsági Hatóság (NEIH)	✓		
Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)		✓	✓

Intézmény	2013-as Stratégia	2018-as Stratégia	2025-ös Stratégia
Honvédelmi Minisztérium	✓	✓	✓
Belügyminisztérium		✓	✓
Nemzeti Fejlesztési Minisztérium (ma TIM)		✓	✓
Állami és ipari CSIRT-ek			✓
Nemzeti SOC-ok			✓
ISAC hálózatok			✓

1. táblázat: A magyar kibervédelmi stratégiákban (2013, 2018, 2025) részt vevő intézmények köre
(saját szerkesztés)

A 2. táblázat jól szemlélteti a stratégiai dokumentumok bővülését, valamint a célkitűzések számosságának fokozatos növekedését, amely tükrözi a kibert fenyegetések komplexitásának és a nemzetközi megfelelési kényszereknek a fokozódását.

Stratégiai dokumentum	Megfogalmazott célok száma
1139/2013. (III. 21.) Korm. határozat	17
1838/2018. (XII. 28.) Korm. határozat	55
1089/2025. (III. 31.) Korm. határozat	64

2. táblázat: A megfogalmazott célok száma a magyar kibervédelmi stratégiákban (1139/2013., 1838/2018., 1089/2025. Korm. hat.)
(saját szerkesztés)

A Fejlődési irányok tekintetében a 2013-as stratégia egyfajta kiindulási alapot jelentett, amelyben a nemzeti szuverenitás védelme, a kiberkoordináció és az EU-NATO konformitás jelentették a fő pilléreket. A 2018-as dokumentum ezt kiterjesztette a gyakorlat irányába. Megjelentek a kritikus infrastruktúrák, a gyermekvédelem, az ipari szereplők, és a DJP 2.0 integrálása. A 2025-ös stratégia radikálisan megnövelte a komplexitást. A digitális állampolgárság, a dezinformáció, az AI-alapú rendszerek és az ellátási láncok védelme a teljes társadalmi rendszerre kiterjedő válaszokat kényszerített ki.

Új területek megjelenése esetében az állami koordinációtól a társadalmi ellenállóképességig vezető út látható. A 2018-as stratégia integrálta a civil szférát és az ipari szektort, beemelte az információs és hálózati rendszerek egységes biztonsági képzését. A 2025-ös dokumentum pedig a mesterséges intelligenciát, az IoT-t, a dezinformációs kampányokat, valamint a CSIRT-, SOC- és ISAC-rendszereket emeli be a nemzeti védelmi válaszok közé.

Minden stratégia illeszkedik az Alaptörvény elveihez, a NATO kibervédelmi politikájához és az EU-s direktívákhoz. 2018-tól kezdve a NIS-direktívák, majd 2025-ben a NIS2-irányelv hazai implementációja válik hangsúlyossá. A válaszképesség is fejlődik, amely esetében 2013-ban még reakcióként jelent meg a kiberbiztonság, 2025-ben már proaktív, nemzeti és nemzetközi szintereken szervezett fellépést irányoz elő.

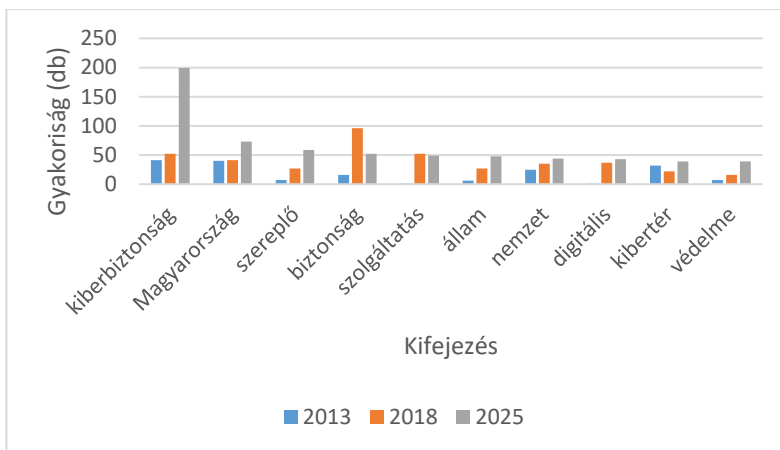
2013-ban az intézményi és operatív struktúrák esetében a Nemzeti Kiberbiztonsági Koordinációs Tanács megalkotása és a jogi keretek kialakítása szerepelt célkitűzésként. 2018-ra az NKI (Nemzeti Kibervédelmi Intézet) szerepe megerősödött, a 2025-ös stratégia pedig tárgyalja az MH kibervédelmi erőinek, a Rendőrség kiberbűnügyi szervezeteinek, valamint a Kiberbiztonsági Hatóság és a Nemzeti Kiberbiztonsági Munkacsoport (NKM) integrált működését.

A 2013-ban megalkotott Nemzeti Kiberbiztonsági Stratégia elsődleges célkitűzése a kiberbiztonság fogalmi és intézményi kereteinek megalapozása volt. Az elemzett dokumentumban leggyakrabban előforduló kifejezések – úgymint *kiberbiztonság, Magyarország, kibertér, nemzet és együttműködés* – egyértelműen arra utalnak, hogy a stratégia középpontjában a kibertér, mint új stratégiai dimenzió bevezetése, valamint a nemzeti szuverenitás védelme állt. Kiemelt hangsúlyt kapott továbbá a kormányzati koordináció megerősítése és a nemzetközi partnerségi kapcsolatok kiépítése. A dokumentum deklarált célja egy biztonságos, szabad és megfelelően szabályozott kibertér kialakítása volt.

2018-ra a stratégiai fókusz elmozdult a rendszerszintű védelem és az információbiztonság irányába. A leggyakoribb szókészlet – például *rendszer, biztonság, információs, kiberbiztonság, szolgáltatás, információbiztonság* – azt jelzi, hogy a dokumentum középpontjába a hálózati és információs rendszerek védelme került. Ezzel összefüggésben megnövekedett az elektronikus szolgáltatások és az állami adatinfrastruktúrák biztonságának szerepe, különös tekintettel a közigazgatási rendszerek védelme. A stratégia ezen szakasza világosan tükrözi a technikai és a jogi szabályozási keretrendszer megerősítésére irányuló törekvést.

A 2025-re előirányzott stratégia már egy sokkal átfogóbb, társadalmi szintű megközelítést képvisel. Az elemzett szógyakorlat (*kiberbiztonság, Magyarország, szereplő, biztonság, szolgáltatás, állam, digitális*) alapján a dokumentum a kiberbiztonságot osztársadalmi feladatként értelmezi. Jelentős hangsúlyt kap az állami, a piaci és civil szereplők együttműködésének szükségessége, valamint a digitális állam és a közszolgáltatások biztonságának megerősítése. A stratégia integrált módon kezeli a digitális transzformáció és a kiberbiztonság összefüggéseit, hangsúlyozva, hogy a technológiai fejlődés kizárólag megfelelő védelmi keretek mellett lehet fenntartható és biztonságos.

A három stratégiai dokumentumban leggyakrabban előforduló kifejezések és azok relatív gyakorisága az 1. számú ábrán kerülnek szemléltetésre.



1. ábra: A vizsgált stratégiák leggyakoribb kifejezései
(saját szerkesztés)

Összeségében megállapítható, hogy a magyar kiberbiztonsági stratégiák tematikus súlypontjai az elmúlt évtized során fokozatosan bővültek és elmélyültek. A 2013-as dokumentum elsősorban a kibertér alapvető stratégiai jelentőségének meghatározására, a nemzeti szuverenitás védelmére és az elvi keretalkotásra koncentrált, miközben nemzetközi kontextusba ágyazottan értelmezte a kiberbiztonság kérdéskörét. E kezdeti megközelítést elsősorban deklaratív jelleg és az alapelvek kijelölése jellemezte.

A 2018-as stratégia paradigmaváltást tükrözött, amely a technológiai és jogi keretek megerősítésére helyezte a hangsúlyt. A dokumentum világosan behatárolta a védendő hálózati és információs infrastruktúrákat, különös figyelmet fordítva az állami és közigazgatási rendszerek védelmére. Ezzel párhuzamosan erősödött a normatív szabályozási környezet szerepe, különösen az elektronikus szolgáltatások biztonságát érintő kihívások kezelése tekintetében.

A 2025-ös stratégia egy ennél is komplexebb szemléletet képvisel, amely a kiberbiztonságot már nem csupán mint technikai vagy jogi kihívást, hanem mint összetársadalmi jelentőségű feladatot értelmezi. A digitális állam koncepciójának megjelenése, a piaci és civil szereplők aktív bevonása, valamint a kiberbiztonság közszolgáltatásként való kezelése új tematikus hangsúlyokat eredményezett. A stratégia horizontális, interszektoriális kormányzási logikát követ, amely a társadalmi szereplők közötti együttműködésre és közös felelősségvállalásra épít.

Ez a tematikus fejlődési ív – az elvi és deklaratív megalapozástól a rendszerszintű technikai védelemig, majd a társadalmi integráció irányába való elmozdulás – szorosan illeszkedik a globális kiberbiztonsági trendekhez. Nemzetközi szinten is megfigyelhető, hogy a kiberbiztonság egyre inkább interdiszciplináris és több szereplőt integráló területté válik, amelyben az állami, gazdasági és civil szféra együttműködése elengedhetetlenné válik a hatékony védelem biztosítása érdekében.

A kutatás következő lépéseként a vizsgált dokumentumokban leggyakrabban előforduló trigramokat – azaz három egymást követő szóból álló kifejezés-együtteseket – azonosítottuk. A trigram-elemzés célja az volt, hogy feltárja a dokumentumokban megjelenő jellemző nyelvi mintázatokat, kifejezésstruktúrákat, valamint ezek tematikus súlypontjait az egyes időszakokban. Az ilyen típusú elemzés lehetővé teszi a tartalmi fókuszok és a szövegkörnyezetek pontosabb meghatározását, hozzájárulva a stratégiai dokumentumok fejlődési ívének feltérképezéséhez.

A 2013-as Kiberbiztonsági Stratégia esetében az olyan trigramok, mint „*Magyarország nemzeti kiberbiztonsági*”, „*kiberbiztonsági stratégiájáról hatályos*”, illetve „*civil gazdasági tudományos*” egyértelműen tükrözik a dokumentum deklaratív, alapozó jellegét. A stratégia hangsúlyozta a nemzeti szintű stratégiai célkitűzések kijelölését, és kiemelten kezelte a civil, gazdasági és tudományos szereplők integrálásának szükségességét. A dokumentum szemléletmódja előremutató, koncepcionális kereteket alkotó, amely a társadalmi együttműködés ösztönzését helyezte előtérbe.

A 2018-ban kiadott Stratégia esetében a leggyakoribb trigramok – például „*elektronikus információs rendszerek*”, „*létfontosságú rendszerek létesítmények*”, vagy „*bejelentés köteles szolgáltatást*” – már sokkal inkább a jogi és technológiai szempontú megközelítés dominanciáját tükrözik. A dokumentum hangsúlya egyértelműen elmozdult a gyakorlati végrehajtás irányába, részletesen meghatározva a kritikus infrastruktúrák, elektronikus szolgáltatások és állami felügyeleti rendszerek védelmére vonatkozó kereteket. Ez az időszak a stratégiai célok technikai operacionalizálásának kezdete.

A 2025-ös stratégia trigramjai – úgymint „*Magyarország kiberbiztonsági stratégiájáról*”, „*stratégiájáról hatályos lekérdezés*”, valamint „*IKT termékek szolgáltatások*” – a dokumentum végrehajtási szakaszának, valamint a digitális állam és a közszolgáltatások működtetéséhez kapcsolódó konkrét aspektusoknak a középpontba kerülését jelzik. Habár egyes trigramok formai vagy adminisztratív természetűek, más kifejezések rávilágítanak az információs és kommunikációs technológiák (IKT) védelmének, illetve az állampolgári interakciók biztonságának fokozódó jelentőségére.

Az elemzés eredményei megerősítik a korábbi tartalmi megállapításokat. A 2013 és 2025 közötti időszakban a magyar kiberbiztonsági stratégiák tematikája fokozatosan elmozdult a deklaratív, elvi alapozástól a technikai, végrehajtási részletek felé, miközben folyamatosan bővült a stratégiába bevont társadalmi és gazdasági szereplők köre.

A trigram-elemzést követően tematikus kulcsszógyakoriság-vizsgálatot végeztünk annak érdekében, hogy feltárjuk, mely fogalmak, diskurzusok és tartalmi irányok domináltak az egyes stratégiákat. Az elemzés öt kulcskategóriára épült, amelyek a következők voltak: **védelem**, **kockázat**, **szuverenitás**, **együttműködés**, valamint **kutatás és oktatás**.

- A **védelem** kategória (kulcsszavak: *véd, biztonság, megelőz, kezel, felügyel*) az információs rendszerek és adatok védelmét célzó intézkedéseket jelenítette meg.
- A **kockázat** dimenzió (kulcsszavak: *kockázat, sérül, sebez, támad, zsarol, incidens, fenyeget*) a fenyegetettség és sebezhetőségek stratégiai diskurzusát ragadta meg.
- A **szuverenitás** kategória (kulcsszavak: *szuverenitás, szuverén, nemzeti, érdek, önrendelkezés*) a nemzeti digitális önállóság és állami kontroll hangsúlyait tükrözte.
- Az **együtműködés** kulcskategória (kulcsszavak: *együtműködés, szövetség, koordinál, partner, NATO, Európai Unió, EU*) a hazai és nemzetközi kapcsolatrendszer, különösen a transznacionális szövetségek jelentőségét erősítette.
- A **kutatás és oktatás** (kulcsszavak: *oktat, tudomány, képzés, fejlesztés, innováció*) a tudástranszfer, az innováció és a humán kapacitások hosszú távú fejlesztésének fontosságát emelte ki.

Az eredmények alapján jól körvonalazódik, hogy a magyar kiberstratégiák tematikus hangsúlyai dinamikusan változtak. Míg 2013-ban az elvi és szuverenitási kérdések domináltak, 2018-ban a technológiai és jogi keretek megerősítésére került a fókusz, 2025-re pedig a társadalmi szereplők bevonása, a szolgáltatások védelme és az interszektorális együttműködés váltak meghatározóvá.

Az egyes kulcskategóriákhoz rendelt szavak előfordulási gyakoriságát az 3. táblázat tartalmazza.

Kulcsszó-kategóriák	Kulcsszó-kategóriákba sorolt szavak előfordulási gyakorisága az egyes években (db)			Változás mértéke (db)	
	2013	2018	2025	Változás 2013-ról 2018-ra	Változás 2018-ról 2025-re
Védelem	51	189	170	138	-19
Kockázat	17	54	103	37	49
Szuverenitás	38	66	106	28	40
Együtműködés	61	122	104	61	-18
Oktatás/Kutatás	23	64	69	41	5

3. táblázat: A kulcskategóriák előfordulási gyakorisága
(saját szerkesztés)

A védelem tematikus kategóriája 2018-ban érte el a legmagasabb értéket 189 kulcsszavas említéssel. Ez a tendencia jól illusztrálja, hogy a stratégia e szakaszában a figyelem középpontjában elsősorban a technikai és szervezeti védelmi rendszerek kiépítése állt. A 2025-ös dokumentumban az említésszám enyhén csökkent (170), ami arra utalhat, hogy a stratégia fókusza részben szélesedett, és egyre nagyobb hangsúlyt kap a társadalmi szereplők bevonása a védelem komplex rendszerébe.

A *kockázat* témaköre látványos növekedést mutat. Míg 2013-ban mindössze 17 kulcsszavas említést azonosítottunk, addig ez a szám 2025-re 103-ra emelkedett. Ez az emelkedés egyértelműen tükrözi a kiberfenyegetettségek és támadások súlyának felismerését, valamint ezek kezelésének stratégiai jelentőségét. A legújabb stratégiai dokumentum már egyértelműen reagál a növekvő fenyegetettségi környezetre, és ennek megfelelően emeli be azokat a tematikai súlypontok közé.

A *szuverenitás* kérdésköre – különös tekintettel a nemzeti érdekek és a digitális önrendelkezés megjelenésére – szintén erősödő tendenciát mutat. A vizsgált kulcsszavak előfordulása 38-ról 106-ra emelkedett, különösen a 2025-ös dokumentumban figyelhető meg markáns növekedés. Ez a változás összhangban van a nemzetközi diskurzusokkal, ahol a digitális szuverenitás egyre hangsúlyosabb stratégiai tényezővé válik.

Az *együttműködés* kategóriája 2018-ban mutatta a legmagasabb aktivitást (122 említés), azonban 2025-re ez a szám 104-re csökkent. Ez a változás arra enged következtetni, hogy míg a korábbi stratégia a nemzetközi szövetségek (különösen az EU és a NATO) jelentőségét emelte ki, addig a legújabb dokumentum már inkább a belső rendszerintegrációra és az autonóm nemzeti képességfejlesztésre koncentrált.

A *kutatás és oktatás* tematikája kevésbé domináns, ugyanakkor folyamatos növekedést mutatott. A releváns kulcsszavak előfordulási száma 23-ról 69-re nőtt. E kategória keretében az oktatás, a tudományos fejlesztés és az innováció egyre inkább a stratégia részévé válik, ám még mindig nem éri el a védelem- vagy a kockázatkezelés-szintű hangsúlyt.

A fentiek tekintetében elmondható, hogy a vizsgált kiberbiztonsági dokumentumok tematikus szerkezete egyre gazdagabbá vált. 2025-ben átlagosan 72 kulcsszóval több tematikus említést rögzítettünk, mint 2013-ban. Míg a korai stratégia elsősorban deklaratív, keretalkotó jellegű volt, a 2018-as dokumentum inkább technokrata és normatív megközelítést alkalmazott. A 2025-ös stratégia ezzel szemben egyértelműen komplex, rendszerszintű és fenyegetésorientált szemléletet képvisel. A *védelem* és a *kockázat* témaköre egyre markánsabban jelenik meg, míg a *szuverenitás* és a *tudásalapú fejlesztés* továbbra is növekvő, de mérsékelt súlyú tartalmi elemekként értelmezhetők.

A vizsgálat utolsó fázisában a dokumentumokat klaszterelemzéssel dolgoztuk fel, amelynek célja az ismétlődő, tematikusan összetartozó szövegcsoportok azonosítása volt. A dokumentumokat bekezdésekre bontottuk, majd a szöveget előfeldolgoztuk (kisbetűsítés, számok és speciális karakterek eltávolítása), és a magyar nyelvű szavakat TF-IDF (Term Frequency–Inverse Document Frequency) súlyozással numerikus vektorokká alakítottuk. Ezt követően a *K-means* algoritmus alkalmazásával öt klasztert hoztunk létre mindhárom stratégiai dokumentumban.

A klaszterek értelmezését a tíz legjellemzőbb kulcsszó segítségével végeztük, amelyek minden egyes csoport esetében megragadták a legfontosabb tartalmi jegyeket. Ez a módszertani megközelítés lehetővé tette a dokumentumok belső struktúrájának tematikus feltárását, valamint az időbeli fejlődési trendek összehasonlítását.

A klaszterelemzés alapján világosan kirajzolódik a magyar nemzeti kiberbiztonsági stratégiák tartalmi fejlődése és tematikai átrendeződése. A 2013-as dokumentum még a stratégiai alapok lefektetésére és a nemzeti célkitűzések kijelölésére koncentrált. A 2018-as stratégia kiforrottabb, szabályozási és technológiai részletekre épülő struktúrát mutatott. A 2025-ös dokumentum ezzel szemben már egy gyakorlatorientáltabb szemléletet tükröz, amelyben kiemelt szerepet kapnak az állami és gazdasági informatikai rendszerek, valamint az operatív technológiai megoldások. A klaszterek főbb jellemzőit a 4. táblázat szemlélteti.

Szempont	2013	2018	2025
Nemzeti keretrendszer	Kiemelt hangsúlyt kapott a stratégia bevezetése és a nemzeti célkitűzések lefektetése.	Már stabilizált nemzeti jogszabályi háttér, a hangsúly az alkalmazáson van.	A nemzeti és állami szerepvállalás tovább erősödik, főként a „nemzeti kiberbiztonsági képességek” kontextusában.
Nemzetközi dimenzió	Kisebb súllyal, de megjelenik (EU, NATO).	Erőteljesen jelen van – kiberbiztonság globális és uniós vetületei.	Kevésbé hangsúlyos, a dokumentum elsősorban nemzeti és üzleti fókuszú.
Jogszabályi hivatkozások	Formális, technikai utalások (pl. határozatszámok).	Kiemelkedő rész, külön klaszter foglalkozik rendeletekkel, információbiztonsági törvényekkel.	Szintén megjelenik, de inkább kormányzati határozatokra való formai utalásokban.
Digitális állam és szolgáltatások	Gyermekvédelem és társadalmi szempontok megjelennek.	Elektronikus szolgáltatások és e-közigazgatás külön klasztert alkot.	Az üzleti szektor és állami informatika kap hangsúlyt (pl. lekérdezés, hálózat).
Kritikus infrastruktúra	Nem kap külön klasztert, csak általánosan említett.	Külön klaszterben szerepelnek a létfontosságú rendszerek.	Nincs egyértelműen jelen önálló klaszterként.
Technikai aspektusok	Kevésbé technikai – inkább stratégiai és jogi fókusz.	Közepes technikai hangsúly.	Jelentősebb technikai rész (pl. „lekérdezés”, „hálózat”, „üzleti” rendszerek).

4. táblázat: A vizsgált stratégiák klasztereinek főbb jellemzői
(saját szerkesztés)

A fentiekből megállapítható, hogy a 2013-as stratégiai dokumentum klaszterelemzése egyértelműen tükrözi a deklaratív és megalapozó jelleg dominanciáját. A klaszterek jellemző kulcsszavai a Nemzeti Kiberbiztonsági Stratégia célkitűzéseinek megfogalmazására, a kormányzati szerepvállalás meghatározására és a stratégiai dokumentumok formális nyelvezetére utalnak. Kiemelendő továbbá a gyermekvédelem tematikájának megjelenése, amely egy önálló klaszteren belül jelenik meg, jelezve a társadalmi szempontok kezdeti integrációját a kibertérrel kapcsolatos politikai gondolkodásba. A szakpolitikai integráció szintén megjelenik, különösen az oktatáspolitikai és nemzetbiztonsági vonatkozások összekapcsolásában. A 2018-as dokumentumban a tartalmi hangsúly egyértelműen eltolódik a jogszabályi és technológiai keretrendszerek felé. A klaszterelemzés alapján az információbiztonsági törvények, kormányrendeletek és a létfontosságú rendszerek védelme köré szerveződő szövegegységek kerülnek előtérbe. Ezek a klaszterek a szabályozás konkrétumait, az infrastruktúrávédelem gyakorlati megoldásait, valamint az állami felügyeleti logikát tükrözik. Emellett megjelenik a digitális tér nemzetközi dimenziója is, ami arra utal, hogy a stratégia már nem kizárólag nemzeti keretekben értelmezi a kiberbiztonságot, hanem egyre inkább reflektál a kibertér globalizálódására. Az *e-közigazgatás* és az *elektronikus állami szolgáltatások* külön klasztert alkotnak, jelezve a digitális állam fejlesztésének stratégiai jelentőségét. A 2025-ös stratégia klaszterszerkezete egy újabb tematikai átrendeződésre utal. Míg a nemzeti és állami kiberbiztonság továbbra is meghatározó elem, ezek már erőteljesebben kapcsolódnak az üzleti szférához és az informatikai rendszerek operatív működéséhez. A klaszterekben megjelenő kulcsszavak – például *lekérdezés, hálózat, üzleti, idő* – technológiai és működésbeli aspektusokra utalnak, amelyek a gyakorlati végrehajtás és a szolgáltatásbiztonság kérdésköreit emelik középpontba. Ebből adódóan a dokumentum nem csupán stratégiai iránymutatásként, hanem részben operatív kézikönyvként is értelmezhető, különösen az állami informatika és a piaci szereplők együttműködése szempontjából. A szöveg retorikájában és struktúrájában egyaránt technológiaközeli és kevésbé normatív, mint a korábbi évek stratégiái.

A három dokumentum klaszterszintű tartalomelemzése világosan kirajolja a nemzeti kiberbiztonsági gondolkodás fejlődési ívét. A kezdeti deklaratív és elvi megközelítést fokozatosan felváltja a szabályozási és végrehajtási logikára épülő szemlélet. A hangsúly eltolódása a stratégiai célkitűzésektől az infrastruktúrávédelem, majd az operatív és technikai alkalmazások irányába nem csupán tematikai változásokat jelez, hanem a magyar kiberbiztonsági szemlélet egyre érettebbé válását is. A 2025-ös stratégia már egy olyan komplex, többdimenziós rendszert tükröz, amely képes választ adni nemcsak az elméleti, hanem a gyakorlati kihívásokra is a digitális állam, a gazdasági szereplők és a társadalom metszetében.

Diszkusszió

A 2013, 2018 és 2025-ös stratégiák összevetése egy lineáris fejlődési ívet tár fel, amelyben a hangsúly a normatív irányoktól a gyakorlati, védelmi rendszerek felé mozdult el. A stratégiák egyre érzékenyebbé válnak a külső geopolitikai és technológiai környezetre, miközben a belső koordinációt is fokozzák. Magyarország kibérvédelmi

stratégiáinak értéke nemcsak azok tartalmi gazdagságában, hanem a bennük megfogalmazott szemléletváltásban és hosszú távú gondolkodásban ragadható meg.

A globalizáció és a határokon átnyúló kereskedelem átalakította a gazdasági struktúrákat, miközben fokozta a biztonságpolitikai sérülékenységet. Az Ipar 5.0 megoldások és az 5G technológia elterjedése nemcsak új lehetőségeket, hanem új támadási felületeket is létrehozott. Az ipari rendszerek digitalizálása fokozott kitétséget eredményezett, amit tovább súlyosbít a strukturált nemzetközi adatmegosztás hiánya. A dezinformációs kampányok és a titkosított kommunikációt alkalmazó bűnszervezetek tevékenységei komplex kihívásokat állítanak a nemzetbiztonság elé.

T1: A magyar kiberbiztonsági stratégiai gondolkodás fejlődése világos tematikus ívet követ, amely az elvi deklarációktól a komplex, rendszerszintű és interszektoriális megközelítés felé haladt.

T2: A 2025-ös stratégia paradigmaváltást képvisel, amelyben a kiberbiztonság már nemcsak technikai vagy állami feladatként, hanem közszolgáltatásként és társadalmi felelősségként is megjelenik.

T3: A digitális szuverenitás kérdésköre a nemzeti kiberbiztonsági diskurzusban egyre hangsúlyosabbá vált, jelezve a nemzetközi technopolitikai kihívásokra adott tudatos stratégiai válaszokat.

T4: A magyar kibervédelmi stratégiai dokumentumok tartalmi és intézményi fejlődése egyre erősebben reflektál az EU és a NATO kibervédelmi célkitűzéseire. Ugyanakkor a két szervezet közötti jogharmonizációs és interoperabilitási különbségek kezelésére irányuló stratégiai válaszok csak részben jelennek meg a dokumentumokban. Magyarország számára tehát nemcsak a megfelelés, hanem a proaktív, az alakító részvétel lehetősége is adott, amelyhez strukturált fejlesztéspolitikai vízió, digitális képességfejlesztés és szuverenitásvédelem-alapú stratégiai gondolkodás szükséges.

Felhasznált irodalom:

089/2025. (III. 31.) Korm. határozat Magyarország Kiberbiztonsági Stratégiájáról. Elérhető: <https://njt.hu/jogszabaly/2025-1089-30-22> (Letöltés ideje: 2025.04.03.)

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Elérhető: <https://njt.hu/jogszabaly/2013-1139-30-22.1> (Letöltés ideje: 2025.04.03.)

1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról. Elérhető: <https://njt.hu/jogszabaly/2018-1838-30-22> (Letöltés ideje: 2025.04.03.)

AGYEMAND, Raymond – FURNELL, Steven – MULLER, Tim: A Profile-Based Cyber Security Readiness Assessment Framework at Country Level. *International Symposium on Human Aspects of Information Security and Assurance*. Springer Nature Switzerland, Cham. 2024. 93–106. o. Elérhető: https://link.springer.com/chapter/10.1007/978-3-031-72559-3_7 (Letöltés ideje: 2025.04.03.)

BIHALY, Barbara: Kibervédelem a NATO-ban és az EU-ban. *Hadtudományi Szemle*, 2022/4. 37-49. o. Elérhető: <https://folyoirat.ludovika.hu/index.php/hsz/article/view/6084/5276> (Letöltés ideje: 2025.04.04.)

ÇİFCİ, Hasan – ERGÜNER, Esmâ: Analysis of National Cybersecurity Strategies of G20: objectives, latent themes, latest trends and comparisons. *Data & Policy*, 2025/e7. Elérhető: <https://www.cambridge.org/core/journals/data-and-policy/article/analysis-of-national-cybersecurity-strategies-of-g20-objectives-latent-themes-latest-trends-and-comparisons/3FF5B1542161A9C06FEFE33C410B4640> (Letöltés ideje: 2025.04.05.)

CRAM, W. Alec – YUAN, Jonathan: Out with the old, in with the new: examining national cybersecurity strategy changes over time. *Journal of Cyber Policy*, 2023/1. 26–47. o. Elérhető: <https://www.tandfonline.com/doi/abs/10.1080/23738871.2023.2238712> (Letöltés ideje: 2025.04.03.)

ELKHANNOUBI, Hasna – BELAISSAOUI, Mustapha: A framework for an effective cybersecurity strategy implementation: Fundamental pillars identification. *15th International Conference on Intelligent Systems Design and Applications (ISDA) 2015.*, IEEE, 2015(a). 1–6. o. Elérhető: <https://ieeexplore.ieee.org/document/7489156> (Letöltés ideje: 2025.04.03.)

ELKHANNOUBI, Hasna – BELAISSAOUI, Mustapha: Fundamental pillars for an effective cybersecurity strategy. *IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA) 2015.*, IEEE, 2015(b). 1–2. o. Elérhető: <https://ieeexplore.ieee.org/document/7507241> (Letöltés ideje: 2025.04.03.)

HARKNETT, Richard J. – STEVER, James A.: The new policy world of cybersecurity. *Public Administration Review*, 2011/3. 455–460. o. Elérhető: <https://onlinelibrary.wiley.com/doi/10.1111/j.1540-6210.2011.02366.x> (Letöltés ideje: 2025.04.04.)

KARAHAN, Saltuk – WU, Hongyi – ARMISTEAD, Leigh: *Evolution of US cybersecurity strategy*. In: *International Conference on Cyber Warfare and Security*. Academic Conferences International Limited, 2019. 168–176. o. Elérhető: <https://www.proquest.com/openview/e99648655450412bc2de4a0565938ad7/1.pdf?cbl=396500&pq-origsite=gscholar> (Letöltés ideje: 2025.04.03.)

KELEMEN Roland – FARKAS Ádám: *Nemzeti biztonság és kibertér*. Médiatudományi Intézet, Budapest, 2023. 44. o. Elérhető: <https://mtmi.hu/files/7ddaa0c7-9a10-4123-af9c-e2d86c49cf30.pdf> (Letöltés ideje: 2025.04.06.)

KOVÁCS László – KRASZNAY Csaba: Digitális Mohács 3.0. *Hadtudomány*, 2024/3. 40-55. o. Elérhető: <https://ojs3.mtak.hu/index.php/hadtudomany/article/view/18473> (Letöltés ideje: 2025.04.04.)

KRASZNAY Csaba Dr.: A NIS2 irányelv kihívásai és gyakorlati alkalmazása. *Védelem Tudomány a Katasztrófavédelem online szakmai, tudományos folyóirata*, 2024/9.ksz. 1-5. o. Elérhető: <https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/18114> (Letöltés ideje: 2025.04.05.)

KRASZNAY Csaba: *Taktikák és stratégiák a kiberhadviselésben*. Ludovika Egyetemi Kiadó, Budapest, 2023. Elérhető: https://webshop.ludovika.hu/wp-content/plugins/olvasoprobak/1079_Olvasoproba.pdf (Letöltés ideje: 2025.04.04.)

KSHETRI, Nir – MURUGESAN, San: EU and US cybersecurity strategies and their impact on businesses and consumers. *Computer*, 2013/10. 84–88. o. Elérhető: <https://ieeexplore.ieee.org/document/6649968> (Letöltés ideje: 2025.04.03.)

TSEN, Elinor – KO, Ryan KL — SLAPNICAR, Sergeja: An exploratory study of organizational cyber resilience, its precursors and outcomes. *Journal of Organizational Computing and Electronic Commerce*, 2022/2. 153–174. o. Elérhető: DOI: 10.1080/10919392.2022.2068906

A BIZTONSÁG SZEREPE ÉS FONTOSSÁGA A SZÖVETSÉGESI KRITIKUS INFRASTRUKTÚRA SZABÁLYOZÁSÁNAK KIALAKÍTÁSÁBAN

A biztonsági események és a technikai fejlődés indikátorként hat napjaink szabályozási rendszerére. A szükségleteink kielégítésében részt vevő szektorok és szolgáltatások határokon átnyúló kölcsönös, reziliens függőséget eredményeztek. Ezen folyamat a globalizáció eredményeként visszafordíthatatlan, megfelelő kezelése és értelmezése a biztonság, mint érzés megtartása mellett kell, hogy megvalósuljon.

A tanulmány időrendi sorrendben vizsgálja az Európai Unió kritikus infrastruktúra szabályozásának kialakításában releváns jogszabályokat a stratégiák és a nemzetközi biztonsági események mentén. A biztonsági események szerepeltetése kiemelten a – később beazonosított ágazat – kritikus infrastruktúrával való kapcsolódásuk szemszögéből kerül ismertetésre.

A tagolásban három biztonsági stratégia megjelenését alkalmazza, ábrákkal szemlélteti, olyan gondolati sík mellett, hogy az egyes szabályozási stratégiai célkitűzések elhatárolhatóak legyenek egymástól.

Kulcsszavak: biztonság, biztonsági események, kritikus infrastruktúra, szabályozás, kiberbiztonság

THE ROLE AND IMPORTANCE OF SECURITY IN THE DEVELOPMENT OF FEDERAL CRITICAL INFRASTRUCTURE REGULATION

Security events and technological developments are indicators of the regulatory system today. The sectors and services involved in meeting our needs have created a cross-border interdependence and resilience. This process is irreversible as a result of globalisation and must be properly managed and understood while maintaining a sense of security.

The document examines, in chronological order, the legislation relevant to the development of EU critical infrastructure regulation along the lines of strategies and international security events. Security events are included with a particular focus on their relationship with critical infrastructure, a sector identified later.

The structuring uses the representation of security strategies three illustrated with diagrams, alongside a plane of thought that allows each regulatory strategy objective to be distinguished from the others.

Keywords: security, security incidents, critical infrastructure, regulation, cybersecurity

Bevezetés

A biztonság, mint szükségérzet kialakulásának a történelem során az alábbi főbb mérföldköveit figyelhetjük meg: élet és vagyonvédelem, nukleáris biztonság, adatok és

szolgáltatások védelme. Mindegyik korszaknak megvolt, illetve van az a tényezője, amely köré a védelem szerveződik a biztonságérzet elérése érdekében. A várak, kerítések építése jelentette védelmet felváltotta a hidegháborús időszaki nukleáris fenyegetettség jelentette veszély, ezt követte a számítástechnikai eszközök megjelenésével az adatok adatgazda engedély nélküli továbbításának, tárolásának, másolásának kockázatai. A technológia további fejlődésével az emberek biztonságérzetére és fiziológia szükségletei kielégítésére szolgáló szolgáltatások egymásra épültek. A technológia fejlődése magával hozta az infrastruktúrák változását is, amelyek főként az ipari forradalmak hatására ugrásszerű átalakuláson mentek keresztül. A közlekedési eszközök fejlődése, a távközlés, a robotizáció, a tudományos felfedezések, az innovációban rejlő képességek és lehetőségek szinte folyamatosan változtatták és változtatják a biztonsági környezetet. Kiemelt figyelemmel kezelendő az információ- és távközlő szektor¹ és az összekapcsolt eszközök.² Ezen változások egyben generálják az infrastruktúrák és szolgáltatások közötti kölcsönös függőséget. Azonosításukhoz, detektálásukhoz, védelmük szükségességéhez több biztonsági esemény és jogszabály is köthető.

Vajon a jogalkotói tevékenységben beazonosíthatóak-e az egyes biztonsági események, azok szignifikációja hogyan hatott a szövetségi szabályozási keretrendszerhez? Milyen egymásra épülő események vezettek a napjainkban beazonosított, a kritikus infrastruktúrák, a létfontosságú rendszerelemek, a kritikus szervezetek, mint fogalmi keretek létrejöttéhez?

Jelen tanulmány nemzetközi megközelítésből vizsgálja a kritikus infrastruktúra-védelem szabályozásának kialakulását a jelenleg alkalmazandó előírásokig bezárólag.

Az infrastruktúra és az infrastruktúrák elleni biztonsági események

Az infrastruktúrák megléte az állami szervek működésének és a mindennapi életének alapvető feltétele. Az infrastruktúra latin eredetű szó, nyersfordításban „alapszerkezetet”, „alapépítményt” jelent. Paul N. Rosenstein-Rodan, lengyel származású amerikai közgazdász definíciója szerint „*feltételek komplexuma, amely a magántőke és a lakosság szükségletét elégíti ki, alapvető szolgáltatás, amely nélkül az árukat és a szolgáltatást nyújtó intézmények nem tudnak működni*”.³

A 21. század kezdetével a fizikai, digitális és biológiai technológiák összefonódásával és integrációjával megkezdődött a negyedik ipari forradalom kora,⁴ ezzel egyidejűleg a biztonságtudat-értelmezés is gyökeresen megváltozott. Az összefonódás egyben függőséget is eredményezett egyes szektorok esetében. Az infrastruktúrák

¹ SHIMODA, Atsushi: Study on Organizational Response Management to System Failures. IEEE, 2022. 08. 02. 1. o.

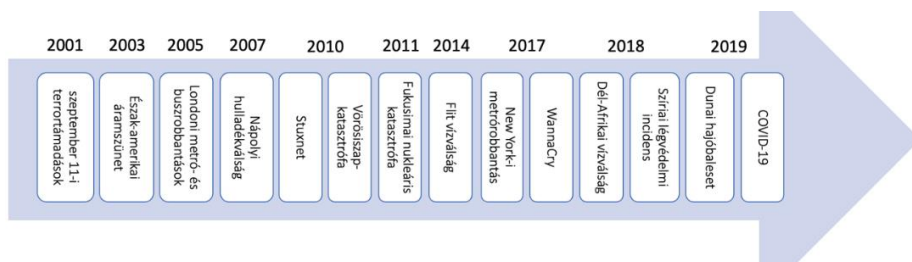
² KARIMIPOUR, Hadis – SRIKANTHA, Pirathayini – FARAG, Hany – WEI-KOCISIS, Jin: *Security of Cyber-Physical Systems – Vulnerability and Impact*. 2020. 01. 290. oldal

³ Sz.n.: Infrastruktúra. Közszolgálati Online Lexikon, é.n.

⁴ Sz.n.: Ipar 4.0. – Negyedik Ipari Forradalom. Pannon Egyetem Mérnöki Kar, 2023. 08. 14.

interdependenciáját a dekonstruktív szándékú személyek és szervezetek is felismerték és kihasználták.⁵

A főbb szakterület kialakulásában domináns szerepet játszó biztonsági eseményeket az 1. ábra szemlélteti.



1. ábra: Biztonsági események a kritikus infrastruktúra-védelem kialakulásában
(saját szerkesztés)

A 2001. szeptember 11-i terrortámadások⁶ alapvetően változtatták meg a biztonságról alkotott világméretű képét. Az Egyesült Államokat terrortámadás érte, amikor négy eltérített repülőgéppel pusztító csapásokat mértek a World Trade Centerre, a Pentagonra. A történet hatására került azonosításra az, hogy egyes rendszerek milyen függőségben vannak, illetve lehetnek egymással.

Az észak-amerikai áramszünet⁷ az Egyesült Államok és Kanada nagy részét érintette, több, mint 50 millió embert hagyva áram nélkül. Az áramkimaradás elsődleges oka egy szoftverhiba volt. Az egészségügyi intézmények biztonsági áramfejlesztői az áramkimaradás pillanatában átvették az energiaellátás feladatát, így a kórházakban nem volt nagyobb fennakadás. A nagyvárosokban ugyanakkor leállt a közlekedés: nem működtek a jelzőlámpák, és megállt a metró is.

A londoni metró- és buszrobbantások⁸ során több öngyilkos merénylő robbantott fel metrószereplvényeket és egy buszt Londonban. A történetek a tömegközlekedési rendszerek sebezhetőségére és a biztonsági intézkedések szükségességére hívta fel a figyelmet.

A megfelelő tervezés és a hulladékgazdálkodás fontosságára világított rá a Nápolyban és környékén a hulladékkezelési rendszer összeomlásával a Nápolyi hulladékválság.⁹ A szemétkérdés, vagyis a szemét lerakásának és kezelésének problémája éveken át sújtotta Nápolyt és környékét, amelynek mértéke elérte a 2400 tonnát. A lakossági hulladék súlyos közegészségügyi és környezeti problémákat okozott.

⁵ Szektoronként egy-egy, időrendi sorrendben

⁶ Sz.n.: 23 éve volt az a nap, amit az emberiség valószínűleg soha nem fog elfelejteni. Player, 2024. 09. 11.

⁷ Sz.n.: Amikor 50 millió ember maradt sötétben. Index, 2013. 08. 14.

⁸ Sz.n.: Terrortámadás volt a londoni metróban történt robbanás. Index, 2017. 09. 15.

⁹ Sz.n.: Nápolyban jól ismerik a pusztító látványt: ilyen, amikor nem viszik el a szemetet. Világgazdaság, 2022. 10. 06.

A Stuxnet számítógépvírus¹⁰ egy kiberfegyver volt, ami célzottan támadta az iráni nukleáris létesítményeket, olajvezeték-hálózatot, illetve ipari létesítményt, kihasználva az ipari vezérlőrendszerek sebezhetőségét, a besszállítói lánc védelmének hiányát. A Stuxnet volt az első olyan rosszindulatú program, amely nemcsak leblokkolja a számítógépeket, de fizikailag is kárt tudott okozni az ipari létesítményekben.

A vörösiszap-katasztrófa Magyarországon¹¹ a veszélyes hulladékok kezelésének és tárolásának biztonsági követelményeit hangsúlyozta ki az Ajka melletti tározó gátjának átszakadásával. Az esemény következtében nagy mennyiségű mérgező vörösiszap ömlött ki, ami súlyos környezeti károkat és emberi áldozatokat okozott.

A fukusimai nukleáris katasztrófa¹² 2011-ben történt. A természeti katasztrófa és az azt követő nukleáris baleset súlyos egészségügyi és környezeti problémákat okozott. Az eset a katasztrófavédelem és az egészségügyi infrastruktúra közötti interdependenciára hívta fel a figyelmet.

Flint városában, Michigan államban, az ivóvíz ólomszennyezése súlyos közegészségügyi incidenst okozott,¹³ amely a vízellátó rendszerek karbantartásának és a vízminőség ellenőrzésének fontosságára hívta fel a figyelmet.

A Malaysia Airlines MH17-es járatának Kelet-Ukrajna felett történő lelövése¹⁴ 298 ember halálát okozta. A polgári légi közlekedés sebezhetősége, a légtérvédelem hiányosságai okozták az incidenst.

2017. december 11-én egy öngyilkos merénylő robbantott a New York-i Port Authority buszterminál közelében¹⁵ több ember sérülését okozva. Ez az esemény ismételt felhívta a figyelmet a városi közlekedési rendszerek biztonsági kihívásaira.

A WannaCry kiberincidens¹⁶ különösen súlyosan érintette az egészségügyi szektort, többek között a brit NHS (Nemzeti Egészségügyi Szolgálat) rendszereit is. Az esemény hangsúlyozta a kiberbiztonság fontosságát a kritikus infrastruktúrában.

Fokvárosban a súlyos aszály következtében a vízkészletek kimerültek, ami a „Day Zero” fenyegetéséhez vezetett,¹⁷ amikor a város vízellátása teljesen megszűnt volna. Ez az incidens rávilágított a vízgazdálkodás és a fenntartható vízhasználat fontosságára.

¹⁰ Sz.n.: Erőműveket is megtámadott egy számítógépes vírus. Greenfo, 2010. 09. 25.

¹¹ Sz.n.: 10 éve történt a vörösiszap-katasztrófa. Katasztrófavédelem Központi Múzeuma, é.n.

¹² Sz.n.: A katasztrófa, aminek láttán elnémult a világ: 10 éve történt a fukusimai atomerőmű-baleset. infostart, 2021. 03. 11.

¹³ Sz.n.: Rezsit akartak csökkenteni, a fél város ólommérgezést kapott. Index, 2016. 02. 03.

¹⁴ Sz.n.: Lelőtt Malaj utasszállító: már több mint 166 millió Eurót költöttek a Hollandok a nyomozásra. MTI/iho, 2024. 03. 01.

¹⁵ Sz.n.: Robbantás volt egy manhattani pályaudvaron. origo.hu, 2017. 12. 11.

¹⁶ Sz.n.: Már felénk tart az új WannaCry? Magyarországra is megérkezhet az új zsarolóvírusos támadás. hvg.hu, 2023. 02. 13.

¹⁷ Sz.n.: Csak három hónapra elég a víz Fokvárosban. Index, 2018. 01. 11.

Egy orosz katonai repülőgépet lőttek le Szíria felett, ami 15 katona halálát okozta.¹⁸ Ez az incidens rámutatott a légtérvédelem és a légvédelmi rendszerek közötti koordináció fontosságára.

A Hableány nevű turistahajó összeütközött egy nagyobb hajóval és elsüllyedt, 28 ember halálát okozva.¹⁹ Ez az esemény felhívta a figyelmet a folyami hajózás biztonsági kihívásaira és a hajózási szabályok betartásának fontosságára.

A Covid19 világjárvány²⁰ súlyos terhelést rótt az egészségügyi rendszerekre világszerte. Az esemény rávilágított az egészségügyi infrastruktúra rugalmasságának és a járványügyi felkészültség fontosságára.

Nemzetközi és szövetségi kritikus infrastruktúrák szabályozási környezetének megjelenése és fejlődése²¹

Egyes létesítmények, rendszerek vagy szolgáltatások zavara, esetleges kiesése negatív hatást gyakorolhat a társadalmi és gazdasági stabilitásra. A kritikus infrastruktúra beazonosítását, a kormányzati – hadi, nemzetbiztonsági – és gazdasági kölcsönös függőségét, a sebezhetőségek gyors megszüntetését, az ártó szándékú cselekményektől való védelmét és beazonosításának szükségességét az Amerikai Egyesült Államok (a továbbiakban: USA) 1998-ban a 63. elnöki irányelvben fektette le.²² Az Irányelv kritikus infrastruktúráknak a gazdasági és a kormányzati létesítményeket tekintette.

Az első biztonsági stratégia

A 2001-es terrortámadások bekövetkezése tette első ízben szükségessé – társadalmi támogatás mellett – az Európai Unió (a továbbiakban: EU) jogalkotói számára – követve az USA-t – az egységes jogi szabályozás szükségességét a kritikus infrastruktúrák védelmére vonatkozóan. A terrortámadás és az azt követő láncreakció szolgált első ízben bizonyítékaul annak, hogy bizonyos szolgáltatások kormányzati érintettség nélkül is függenek egymástól, nem lehet egyesével védeni, komplexen, koherensen kell kezelni azt. A magánélet védelmét elősegítő intézkedésként az EU elfogadta az elektronikus hírközlési adatvédelmi irányelvet²³ a közlések titkosságára, a nem kívánt kommunikáció tiltására és a felhasználói jogok védelmére. Az EU felismerte továbbá, hogy ez nem csupán tagállami szinten szükséges, hanem közösségi szintű program létrejötte a célkitűzés. Ezt bizonyítandó, 2003-ban első lépésként fogadták el

¹⁸ Sz.n.: Oroszország: a szír légvédelem lőtte le a katonai gépet, de Izrael felelős érte. hvg.hu, 2018. 09. 18.

¹⁹ Sz.n.: Hajóbaleset történt a Dunán Budapesten – videóval. Tények.hu, 2024. 12. 23.

²⁰ Sz.n.: A SARS-CoV-2 (Covid-19) koronavírus. Dr. Weigert Higiéniai rendszerek, é.n.

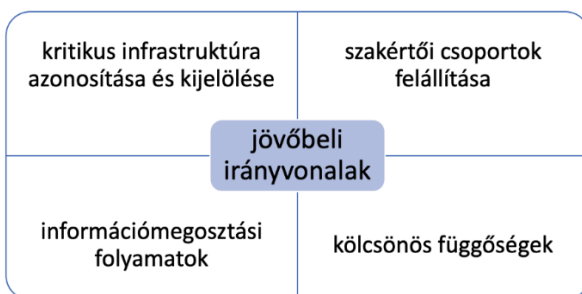
²¹ Időrendi sorrend szerint.

²² White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. Presidential Decision Directives, 1998. 06. 22.

²³ Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről ("Elektronikus hírközlési adatvédelmi irányelv"). Brüsszel, 2002. 07. 12.

az Európai Biztonsági Stratégiát.²⁴ Az EU történetében ez az első stratégia, amelyben az EU biztonsági érdekeinek figyelembevételével alapelvek és célok kerültek meghatározásra.

Az EU 2004 márciusában a stratégiai célkitűzések meghatározása mellett²⁵ az Európai Unió Tanácsának 460/2004/EK rendeletével²⁶ létrehozta az Európai Unió Kiberbiztonsági Ügynökségét (European Union Agency for Cybersecurity, a továbbiakban: ENISA). Az ENISA fő feladata volt,²⁷ hogy szorosan együttműködve a tagállamokkal, az Európai Bizottsággal és a piaci szereplőkkel, elősegítse az EU kiberbiztonsági kultúrájának fejlődését. Az Európai Tanács 2004 decemberében tartott ülésén jóváhagyták a Kritikus Infrastruktúrák Európai Programja²⁸ (European Programme for Critical Infrastructure Protection, a továbbiakban: EPCIP) megalkotására vonatkozó javaslatot. A javaslat keretében a terrorizmus elleni küzdelem főbb irányvonalai kerültek meghatározásra. Ez a program meghatározta a terrorizmus elleni küzdelem főbb, jövőbeli tendenciáit, amelyet a 2. ábra részletez.



2. ábra: A terrorizmus elleni küzdelem főbb, jövőbeli irányvonalai az EPCIP-ben
(saját szerkesztés)

A 2005. július 7-i londoni robbantások fokozták a terrorizmus elleni harc szükségességét. Az Európai Bizottság 2005 novemberében elfogadta és kiadta a kritikus infrastruktúrák védelméről szóló Zöld Könyvet.²⁹ A dokumentumban rögzítésre kerültek az EU akkori jövőbeli programjának alapelvei, céljai, meghatározásai, valamint a kapcsolódó és szükséges intézkedések. A Zöld Könyv középpontjába az alábbi főbb elemek kerültek: szubszidiaritás,³⁰ kiegészítő jelleg, együttműködés, titkosság, arányosság. További elemként jelent meg a kritikus infrastruktúrák azonosítását

²⁴ Európai Unió Tanácsa: Európai Biztonsági Stratégia; Brüsszel, 2009.

²⁵ Lásd: Európai Biztonsági Stratégia

²⁶ Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról. Brüsszel, 2004. 03. 13.

²⁷ Napjainkra feladatköre bővült, lásd kronologikus sorrend.

²⁸ European Programme for Critical Infrastructure Protection. EUR-Lex, 2010. 08. 17.

²⁹ Az Európai Közösségek Bizottsága: Zöld Könyv. A létfontosságú infrastruktúrák védelmére vonatkozó európai programról. Brüsszel, 2005. 11. 17.

³⁰ A szubszidiaritás az az elv, amely szerint minden döntést és végrehajtást a lehető legalacsonyabb szinten kell meghozni, ahol a legnagyobb hozzáértéssel rendelkeznek.

illetően az Európai Kritikus Infrastruktúrák (European Critical Infrastructure, a továbbiakban: ECI) és a Nemzeti Kritikus Infrastruktúrák (National Critical Infrastructure, a továbbiakban: NCI) halmaza, amelyek kiterjedése okán más-más biztonsági intézkedések kategóriáit kell, hogy tartalmazzák.

Az EU információs társadalomra irányuló stratégia³¹ 2006-ban került elfogadásra, amely az információs és kommunikációs technológiák (a továbbiakban: IKT), infrastruktúrák ellenálló képességének fokozására történő törekvést is tartalmazott. A kritikus informatikai infrastruktúrák ellenálló képességének növekedése érdekében a Közlemény a felkészülés, észlelés, reagálás, hatások enyhítése és a helyreállítás nemzetközi együttműködés IKT ágazati kritériumokat határozott meg a (kiber)biztonság fokozása érdekében.

Az első közösségi direktíva a 2008/114/EK Irányelv (Critical Infrastructures Protection, a továbbiakban: CIP)³² 2008. december 8-án került elfogadásra, amely az európai kritikus infrastruktúrák azonosításáról, kijelöléséről és védelmük javításának szükségességéről szól. A CIP célja egy átfogó uniós program – EPCIP – végrehajtásának biztosítása egy olyan mechanizmus által, amelyet a tagállamoknak implementálniuk kell a saját jogszabályi keretrendszerükbe. A CIP az európai kritikus infrastruktúrák azonosítására és kijelölésére egy átfogó, egységes rendszert ad az érintett ágazatok számára. A tagállamokat az implementációt túlmenően kötelezte a szabályozás két éven belüli végrehajtására, az energia- és közlekedési ágazatok kritikus infrastruktúráinak kiemelt védelmére, a sebezhető pontok és veszélyeztető tényezők felmérésére, az ágazati kritériumok³³ kidolgozására az ágazati szabályozások figyelembevételével, az uniós szinten meghatározott horizontális kritériumok³⁴ átvételére és alkalmazására, az általános azonosítási és kijelölési folyamat nemzeti szintű megvalósítására, a biztonsági összekötők kinevezésére, üzemeltetői biztonsági terv készítésére, valamint a kritikus infrastruktúrák figyelmeztető információs hálózatának (Critical Infrastructure Warning Information Network, a továbbiakban: CIWIN) felállítására.

A 2010-ben történt biztonsági események a biztonsági környezetek változásának lekövetését, azaz további szövetségi szabályozást tettek szükségessé a kiberbűnözés elleni harc erősítése érdekében. 2012-ben az EU a kritikus informatikai infrastruktúrák megerősítésére szolgáló nemzeti és uniós intézkedések keretében³⁵ felállított egy

³¹ A strategy for a Secure Information Society

³² A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. Brüsszel, 2008. 12. 08.

³³ A megzavarás vagy megsemmisítés jelentős hatással lenne legalább két tagállamra, és az egyéb típusú infrastruktúrákkal fennálló, ágazatokon átnyúló kölcsönös függőségből erednek.

³⁴ Veszteségek, gazdasági és társadalmi hatás kritériuma.

³⁵ Az Európai Parlament 2012. június 12-i állásfoglalása „A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: a globális kiberbiztonság felé” című dokumentumról (2011/2284(INI)). Strasbourg, 2012. 06. 12.

bizottságot, hogy dolgozzon ki egy átfogó stratégiát az internetbiztonság és a biztonságos és ellenálló kibertér létrehozására.

A második biztonsági stratégia

Az előkészítő munkát követően, 2013-ban közzétették az EU kiberbiztonsági stratégiáját³⁶ és az információs rendszerek elleni támadásokról szóló irányelvet.³⁷ Az irányelv újításokat vezetett be az egységes fellépés szükségessége érdekében, amelyet a 3. ábra szemléltet.



3. ábra: egységes fellépés szükségessége az Európai Parlament és a Tanács 2013/40/EU irányelve alapján
(saját szerkesztés)

Az EU első kiberbiztonsági stratégiája a nyílt, megbízható, biztonságos kibertér létrehozását szorgalmazta célkitűzéseként, és a további intézkedések bevezetésének szükségességét a reziliencia kérdésében. Felhívta a figyelmet továbbá az adatvédelem, valamint a hálózat- és információbiztonság – a későbbiekben kiberbiztonság – magas szintű kezelésének szükségességére.

2016-ban az EU kiberbiztonsági stratégiájának hatására a bizottságok közvetlenül hatályos adatvédelmi rendeletet³⁸ és tagállami jogba ültetendő hálózati és információs rendszerek biztonságának növelését célzó irányelvet³⁹ dolgoztak ki kettő éves hatályba lépési időszákkal. Az EU általános adatvédelmi rendelete az EU-ban lévő IKT-eszközökön

³⁶ EU cybersecurity strategy: an open, safe and secure cyberspace (2013/2606(RSP))

³⁷ Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. Brüsszel, 2013. 08. 14.

³⁸ Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). Brüsszel, 2016. 05. 04.

³⁹ Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv). Brüsszel, 2022. 12. 27.

lévő adatkezelésekre terjed ki az érintetti jogok⁴⁰ érvényesítése és érvényesíthetősége érdekében. Kezeli a beépített adatvédelmi alapelvek érvényesülésén keresztül az érintetti jogok – alapértelmezett adatvédelem – érvényesülését, a szervezetek részére adatvédelmi tisztviselő kinevezését határozza meg, adatvédelmi hatásvizsgálat elvégzését teszi kötelezővé, amennyiben az adatkezelés magas kockázattal jár az érintettek jogaira és szabadságaira nézve, valamint lehetővé teszi pénzbírság kiszabását az adatvédelmi szabályok megsértése esetén.

A hálózati és információs rendszerek biztonságáról szóló EU-irányelv biztonságot elősegítő célkitűzései voltak a biztonsági eseményekre reagáló csoportok (Computer Security Incident Response Team, a továbbiakban: CSIRT) létrehozása tagországi szinten; a tagországi CSIRT-ek jelentési kötelezettsége; a tagállamok kötelessége kapcsolattartó pont (Single Point of Contact, a továbbiakban: SPOC) kijelölése kapcsán; a biztonsági intézkedések és jelentési kötelezettségek a tagországi CSIRT-eknek és SPOC-oknak; tagországi kiberbiztonsági stratégia készítése, amely felkészültséget és reagálási képességet biztosíthat a kibertámadások kezelésére; valamint az EPCIP-ben meghatározott kritikus infrastruktúrák védelmének prioritizálása.

Az IKT-szolgáltatások elterjedésével, valamint a kibertámadások számának növekedésével a kiberbiztonság szabályozása szükségessé vált.⁴¹ A jogalkotó ezt a tanúsítási keret bevezetésével és az ENISA szerepének erősítésével – mint EU-s SPOC-központ – kezelte egy irányelven keresztül 2019-ben.⁴²

A harmadik biztonsági stratégia

2020-ban az EU az önkötelezett felülvizsgálat eredményeként új Európai Biztonsági Unió Stratégiát⁴³ adott ki a 2020-2025 évekre vonatkozóan. A stratégia négy pillére több fő cselekvési területre terjed ki,⁴⁴ amelyet a 4. ábra mutat.

⁴⁰ European Data Protection Board, 01/2022. sz. iránymutatás az érintettek jogairól – hozzáférési jog, 2.1. változat. edpb.com, 2023. 03. 28.

⁴¹ lásd: biztonsági események k) pont

⁴² Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Unió Kiberbiztonsági Ügynökségéről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (EGT-vonatkozású szöveg). Brüsszel, 2019. 04. 17.

⁴³ EU Security Union Strategy

⁴⁴ Európai biztonsági unió



4. ábra: a harmadik biztonsági stratégia cselekvési területei
(saját szerkesztés)

A biztonsági stratégia iránymutatásai mentén több albizottság is megalakult a kidolgozó munka és a kodifikáció végrehajtására, amelyek eredményeiről évenkénti eredményjelentést⁴⁵ tesz közzé. Ezen munka keretében 2022-ben első ízben az adatkormányzási rendelet⁴⁶ készült el. A rendelet többek között az adatok újrahasznosításának feltételeit, valamint biztonsági intézkedéseket vezetett be a nem személyes adatok EU-n kívüli áramlására.⁴⁷ A jogalkotás következő fázisában a digitális piacokra vonatkozó jogszabály⁴⁸ megalkotása történt. A versenyképesség és tisztességes eljárások mellett adatmegosztási kötelezettséget is meghatározott egyes digitális platformok részére. Az illegális online tartalmak elleni küzdelem, az átláthatóság és az elszámoltathatóság biztosítása a felhasználók védelme érdekében a digitális szolgáltatásokról szóló jogszabály⁴⁹ főbb elemeiként azonosíthatók.

A 2022. év vége a kritikus infrastruktúra és a kiberbiztonság szempontjából jelentős előírásokban történő változást hozott, mert megjelentek a pénzügyi ágazat digitális működési rezilienciájáról⁵⁰, az Unió egész területén egységesen magas szintű

⁴⁵ A Bizottság jelentése a biztonsági unió általános eredményeiről. Európai Bizottság sajtóközlemény, Brüsszel, 2024. 05. 15.

⁴⁶ Az Európai Parlament és a Tanács (EU) 2022/868 rendelete (2022. május 30.) az európai adatkormányzásról és az (EU) 2018/1724 rendelet módosításáról (adatkormányzási rendelet). Brüsszel, 2022. 06. 03.

⁴⁷ A rendelet hatályba lépéséig csak az EU Adatvédelmi rendelete (GDPR) a személyes adatok áramlását kezelte.

⁴⁸ Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály. Brüsszel, 2022. 10. 12.

⁴⁹ Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). Brüsszel, 2022. 10. 27.

⁵⁰ Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a

kiberbiztonságot biztosító intézkedésekről⁵¹ és a kritikus szervezetek rezilienciájáról⁵² szóló jogszabályok. A közzétételük és hatályba lépésük is megegyező, ezzel is elősegítve és támogatva a jogszabályok témakörében és előírásaiban egységes kezelést a biztonság és ellenálló képesség növelése érdekében.

A pénzügyi ágazat digitális működési rezilienciájáról szóló rendelet (Digital Operational Resilience Act, a továbbiakban: DORA) korunk (kiber)biztonsági kockázatainak a rugalmas ellenállóképességét hivatott szabályozni a pénzügyi szektorban. A DORA meghatározza azt, hogy a pénzügyi szervezeteknek IKT kockázatkezelési intézkedéseket kell bevezetniük, az IKT-incidenseket jelenteni kell a tagországi CSIRT-eknek és SPOC-oknak, a digitális működési ellenállóképességüket (védelmi megoldások, folytonossági tervek) rendszeresen tesztelniük kell, valamint az IKT-eszközök beszállítói láncának felügyeletét és ellenőrzését (biztonsági tesztelés, megfelelés) el kell végezniük.

Az EU egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről szóló rendelet (a továbbiakban: NIS2) a kiberfenyegetettség kezelését célzó intézkedések keretében azonosította a kiemelten kritikus és az egyéb kritikus ágazatokat (5. ábra).

kiemelten kritikus ágazatok	energia	egyéb kritikus ágazatok	postai és futárszolgáltatások
	szállítás		hulladékgazdálkodás
	közlekedési infrastruktúrát üzemeltető vagy biztosító vállalkozások		vegyszerek gyártása, -előállítása és -forgalmazása
	banki és pénzügyi szolgáltatások		élelmiszer előállítás, feldolgozás, forgalmazás
	egészségügy		meghatározott termékek gyártói
	ivóvíz		digitális szolgáltatások
	szennyvíz		kutatóhelyek
	digitális infrastruktúra szolgáltatók		
	közigazgatás		
	kihelyezett IKT szolgáltatások		
	világűr		
	űripar		

5. ábra: a kiemelten kritikus és az egyéb kritikus ágazatokat a NIS2 szerint (saját szerkesztés)

A NIS2 a kiemelten kritikus ágazatokra szigorúbb – zavarok megelőzésére, kezelésére, helyreállítására – kockázatkezelési intézkedéseket és incidensjelentési rendet határoz meg, mint az egyéb kritikus ágazatok részére. A kritikus szervezetek rezilienciájának

648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról. Brüsszel, 2022. 12. 27.

⁵¹ Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv). Brüsszel, 2022. 12. 27.

⁵² Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről. Brüsszel, 2022. 12. 27.

növelésére tagállami kötelezettségként a rendelet nemzeti stratégiák kidolgozását és tagországi CSIRT-ek – SPOC – létrehozását teszi kötelezővé, amelyekben az együttműködés kötelezettségét az ENISA-val érvényesíteni kell.

A kritikus szervezetek rezilienciájáról szóló irányelv (a továbbiakban: CER) 2023. január 3-án lépett hatályba, és rendelkezéseit a tagállamoknak 2024. október 18-tól kell a NIS2-vel együtt kötelezően alkalmazni. Az irányelv rögzíti, hogy a kritikus szervezetek fizikai biztonsága és kiberbiztonsága közötti kapcsolatot a tagállamok kötelezettsége kialakítani és biztosítani, azzal, hogy a CER-irányelv és a NIS2 végrehajtását koordináltan szükséges megvalósítani. A CER-irányelv célja, hogy az alapvető szolgáltatást nyújtó kritikus szervezetek rezilienciáját fokozza annak érdekében, hogy az alapvető szolgáltatásokat – mint a társadalmi funkciók és gazdasági tevékenységek fenntartásához nélkülözhetetlen szolgáltatások – az unió belső piacán egységes és elégséges szinten biztosítsák a szolgáltatást nyújtó szervezetek. A CER rögzíti a kritikus szervezet, reziliencia, kritikus infrastruktúra és az alapvető szolgáltatás fogalm meghatározásokat, azokat a kötelezettségeket a kritikus szervezetek számára, amelyek teljesítésével, végrehajtásával rezilienciájukat és szolgáltatási szintjüket tudják növelni. A CER szabályozza továbbá, hogy a kritikus szervezeteknek kockázatokkal arányos technikai, biztonsági és szervezeti intézkedéseket kell hozniuk, amelyekkel megelőzik, reagálnak, enyhítik vagy a helyreállítását támogatják a biztonsági eseményeknek. A CER szerint minden tagállamnak a kritikus szervezetek rezilienciájának fokozására 2026. január 17-ig stratégiát kell készíteni, lefedve az alábbi ágazatokat: energia, közlekedés, banki szolgáltatások, pénzügyi, piaci infrastruktúra, egészségügy, ivóvíz, szennyvíz, digitális infrastruktúra, közigazgatás, világűr, élelmiszer-előállítás, -feldolgozás és -forgalmazás.⁵³

A jogalkotó 2023-ban is aktívan dolgozott az Európai Biztonsági Unió Stratégiában meghatározott célkitűzések eléréséhez szükséges jogi aktusok kidolgozásában. Kiadásra került az Adatkormányzási rendelet⁵⁴ párjaként értelmezett Adatrendelet.⁵⁵ A rendelet a magánszféra adatainak bevonását a közzszférába, valamint a magánszféra egymás közötti adatmegosztását szabályozza, különösen a közösen generált adatok esetén. Elősegíti továbbá az adatokat generáló, hálózatra csatlakoztatható eszközök felhasználói számára, hogy hozzáférjenek adataikhoz, és megosszák ezeket az adatokat harmadik féllel.

⁵³ Lásd: NIS2 kiemelten kritikus ágazatok

⁵⁴ Az Európai Parlament és a Tanács (EU) 2022/868 rendelete (2022. május 30.) az európai adatkormányzásról és az (EU) 2018/1724 rendelet módosításáról (adatkormányzási rendelet). Brüsszel, 2022. 06. 03.

⁵⁵ az Európai Parlament és a Tanács (EU) 2023/2854 rendelete (2023. december 13.) a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról, valamint az (EU) 2017/2394 rendelet és az (EU) 2020/1828 irányelv módosításáról (adatrendelet)

A kiemelten kritikus ágazatok és a digitalizáció bővülésével az EU elkészítette az elektronikus azonosításról és a bizalmi szolgáltatásokról szóló rendeletet,⁵⁶ amely a digitális személyazonosság hatékonyságának növelését és a biztonságos és interoperábilis digitális aláírások keretének meghatározását tartalmazza.

A mesterséges intelligencia (a továbbiakban: MI) rohamos térhódítása, elterjedése és fejlődése szabályozási keret bevezetését tette szükségessé. Erre az EU az MI-ről szóló rendelet⁵⁷ fogadott el, amelyben az MI-rendszerek biztonságos, etikus és megbízható fejlesztését és használatát kezelte. Az MI-rendszerek használatára és kezelésére kockázati besorolást határozott meg:⁵⁸

- a) minimális vagy semmilyen kockázat: ezek az MI-rendszerek szabadon használhatók;
- b) csekély kockázat: átláthatósági kötelezettségek az alkalmazására vonatkozóan;
- c) nagy kockázat: tesztelési, átláthatósági és emberi felügyeleti szabályoknak kell megfelelniük. Ilyen rendszerek a betegségek diagnosztizálásában, az önvezető járművekben, valamint a bűncselekményekben vagy bűnügyi nyomozásokban részt vevő személyek biometrikus azonosításában használt MI-rendszerek;
- d) elfogadhatatlan kockázat: azokat az MI-rendszereket, amelyek veszélyt jelentenek az emberek biztonságára, jogaira vagy megélhetésére, tilos használni az EU-ban. Ezek közé tartozik a kognitív viselkedési manipuláció, a prediktív rendszet, az érzelemfelismerés a munkahelyen és az oktatási intézményekben, valamint a társadalmi pontozás.

Az internetre csatlakoztatott termékek (Internet on device, Internet on technic) számának növekedésével a változó fenyegetések kezelésére⁵⁹ az EU rendeletben megfogalmazott kötelező kiberbiztonsági követelményeket vezetett be a csatlakoztatott digitális elemeket tartalmazó hardver- és szoftvertermékekre vonatkozóan.⁶⁰ A rendelet a kiberbiztonsági követelmények egységesítésére törekszik a gyártói felelősségek növelésével az eszközöket használók kötelező és szélesebb körű tájékoztatása mellett.

⁵⁶ Az Európai Parlament és a Tanács (EU) 2024/1183 rendelete (2024. április 11.) a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról. Brüsszel, 2024. 04. 30.

⁵⁷ Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet). Brüsszel, 2024. 07. 12.

⁵⁸ A mesterséges intelligenciáról szóló rendelet. Európai Tanács, é.n.

⁵⁹ Lásd: Európai Biztonsági Unió Stratégia 2020-2025 évre

⁶⁰ Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról (a kiberrezilienciáról szóló rendelet). Brüsszel, 2024. 11. 20.

Összegzés

Korunk biztonsági kihívásai szükséges mértékű kezelésének kialakulásához a nemzetközi biztonsági térben bekövetkezett biztonsági események kihatásait és összefüggéseit figyelhetjük meg. A biztonsági események hatására a védendő szektorok és tevékenységek száma is jelentős változáson esett át.

Az emberi szükségleteink védelméhez – beleértve az információs társadalmi szükségleteink kielégítését is – elengedhetetlen a megfelelő intézkedések kidolgozása, egymásra épülve stratégiai, majd rendeleti szinten. A biztonsági stratégiák iránymutatásként szolgáló célkitűzéseket határoztak és határoznak meg az EU-s joganyagok szabályozási kereteinek. A stratégiák összeállításánál az aktuális időszak technikai fejlettségi színvonala és a biztonsági események hatásai is beazonosíthatók. A 2003-as Európai Biztonsági Stratégia⁶¹ hatására beazonosításra került az, hogy egyes szolgáltatások nélkülözhetetlenek az emberi lét fenntartásához, ezért kiemelten szakértők bevonásával, információmegosztáson alapulva kell kezelnünk azt. Ezen kritikusnak minősített szolgáltatások kölcsönös függőségét a szervezett bűnözés is felismerte. A nemzetközi együttműködés fokozásának szükségességét a 2013-as EU kiberbiztonsági stratégia⁶² kezelte. A hibrid fenyegetések és a kiberbűnözés megjelenésével a védelmi tevékenységek diverzifikálásával a 2020-as Európai Biztonsági Unió Stratégia⁶³ foglalkozott. A stratégiák a jövőbeni irányvonalak, az egységes fellépés és a cselekvési területek meghatározásait szorgalmazták szövetségi szinten azért, mert a veszélyeztető tényezők megjelenése határokon átnyúló ellenállóképességet követel meg, és kölcsönösen interdependens módon függővé válnak egymástól az egyes szolgáltatások.⁶⁴

Az egyre komplexebb és egymásra épülő tevékenységek, a beszállítói függőségek indukálták annak a változásnak a szükségességét, hogy nem egy adott tevékenység, hanem az azt végző és kiszolgáló szervezet került beazonosításra. Ez alapján kritikus és egyéb kritikus szervezetek kerültek azonosításra az általuk végzett ágazati specifikumtól függően. Így biztosítva szervezeti szinten a biztonsági előírások érvényre jutási lehetőségének jogi előírási köteleességét.

A szabályozás eredményeként kialakult napjainkra egy olyan szabályozási keretrendszer, amelyet a nemzetközi biztonsági környezet, az abból levont tanulságok és tapasztalatok alakítottak és formáltak. A szabályozás leköveti a technológiai fejlődésből adódó prognosztizált veszélyforrások beazonosíthatóságának és interoperabilis kezelésének lehetőségét.

⁶¹ Európai Biztonsági Stratégia

⁶² EU cybersecurity strategy: an open, safe and secure cyberspace (2013/2606(RSP))

⁶³ EU Security Union Strategy

⁶⁴ European Union Agency for Cybersecurity (2015) Critical Information Infrastructures Protection approaches in EU. 1. o.

Felhasznált irodalom:

A Bizottság jelentése a biztonsági unió általános eredményeiről. Európai Bizottság sajtóközlemény, Brüsszel, 2024. 05. 15. Elérhető:

https://ec.europa.eu/commission/presscorner/detail/hu/ip_24_2565 (Letöltés ideje: 2024. 12. 11.)

A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – A biztonságos információs társadalomra irányuló stratégia: „párbeszéd, partnerség, felvértezés és felelősségvállalás”. Brüsszel, 2006. 05. 31. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A52006DC0251> (Letöltés ideje: 2024. 12. 11.)

A mesterséges intelligenciáról szóló rendelet. Európai Tanács, é.n. Elérhető: <https://www.consilium.europa.eu/hu/policies/artificial-intelligence/> (Letöltés ideje: 2024. 12. 11.)

A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. Brüsszel, 2008. 12. 08. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32008L0114> (Letöltés ideje: 2024. 12. 11.)

Az Európai Közösségek Bizottsága: Zöld Könyv. A létfontosságú infrastruktúrák védelmére vonatkozó európai programról. Brüsszel, 2005. 11. 17. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX%3A52005DC0576> (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament 2012. június 12-i állásfoglalása „A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: a globális kiberbiztonság felé” című dokumentumról (2011/2284(INI)). Strasbourg, 2012. 06. 12. Elérhető: https://www.europarl.europa.eu/doceo/document/TA-7-2012-0237_HU.html#def_1_2 (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. Brüsszel, 2016. 07. 06. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A32016L1148> (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). Brüsszel, 2016. 05. 04. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32016R0679> (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Unió Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályaon kívül helyezéséről (kiberbiztonsági jogszabály) (EGT-vonatkozású szöveg). Brüsszel, 2019. 04. 17. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32019R0881> (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály). Brüsszel, 2022. 10. 12. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022R1925> (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). Brüsszel, 2022. 10. 27. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022R2065> (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról. Brüsszel, 2022. 12. 27. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022R2554> (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályaon kívül helyezéséről (NIS 2 irányelv). Brüsszel, 2022. 12. 27. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32022L2555> (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályaon kívül helyezéséről. Brüsszel, 2022. 12. 27. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022L2557> (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács (EU) 2022/868 rendelete (2022. május 30.) az európai adatkormányzásról és az (EU) 2018/1724 rendelet módosításáról (adatkormányzási rendelet). Brüsszel, 2022. 06. 03. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32022R0868> (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete (2023. december 13.) a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról, valamint az (EU) 2017/2394 rendelet és az (EU) 2020/1828 irányelv módosításáról (adatrendelet). Brüsszel, 2023. 12. 22. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:L_202302854 (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács (EU) 2024/1183 rendelete (2024. április 11.) a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról. Brüsszel, 2024. 04. 30. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:L_202401183 (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet). Brüsszel, 2024. 07. 12. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:L_202401689 (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról (a kiberezilienciáról szóló rendelet). Brüsszel, 2024. 11. 20. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:L_202402847 (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről ("Elektronikus hírközlési adatvédelmi irányelv"). Brüsszel, 2022. 07. 12. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32002L0058> (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. Brüsszel, 2013. 08. 14. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32013L0040> (Letöltés ideje: 2024. 12. 11.)

Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról. Brüsszel, 2004. 03. 13. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32004R0460> (Letöltés ideje: 2024. 12. 11.)

EU cybersecurity strategy: an open, safe and secure cyberspace (2013/2606(RSP)); Elérhető: https://www.europarl.europa.eu/doceo/document/TA-7-2013-0376_EN.pdf (Letöltés ideje: 2024. 12. 11.)

EU Security Union Strategy; Brüsszel, 2020. 07. 24. Elérhető: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52020DC0605> (Letöltés ideje: 2024. 12. 11.)

Európai Bizottság: Európai biztonsági unió. Brüsszel, é.n. Elérhető: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_hu (Letöltés ideje: 2024. 12. 11.)

Európai Unió Tanácsa: Európai Biztonsági Stratégia; Brüsszel, 2009. DOI: 10.2860/15719

European Programme for Critical Infrastructure Protection. EUR-Lex, 2010. 08. 17.

Elérhető: <https://eur-lex.europa.eu/EN/legal-content/summary/european-programme-for-critical-infrastructure-protection.html> (Letöltés ideje: 2024. 12. 11.)

European Union Agency for Cybersecurity (2015) Critical Information Infrastructures Protection approaches in EU. Elérhető: <https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf> (Letöltés ideje: 2024. 12. 11.)

European Data Protection Board, 01/2022. sz. iránymutatás az érintettek jogairól – hozzáférési jog, 2.1. változat. edpb.com, 2023. 03. 28. Elérhető: https://www.edpb.europa.eu/system/files/2024-04/edpb_guidelines_202201_data_subject_rights_access_v2_hu.pdf (Letöltés ideje: 2024. 12. 11.)

KARIMIPOUR, Hadis – SRIKANTHA, Pirathayini – FARAG, Hany – WEI-KOCSIS, Jin: *Security of Cyber-Physical Systems – Vulnerability and Impact*. 2020. 01. DOI:10.1007/978-3-030-45541-5

SHIMODA, Atsushi: Study on Organizational Response Management to System Failures. IEEE, 2022. 08. 02. DOI: 10.1109/IIAIAAI55812.2022.00114

Sz.n.: 10 éve történt a vörösiszap-katasztrófa. Katasztrófavédelem Központi Múzeuma, é.n. Elérhető: <https://muzeum.katasztrofavedelem.hu/35837/10-eve-tortent-a-vorosizsap-katasztrofa> (Letöltés ideje: 2024. 12. 11.)

Sz.n.: 23 éve volt az a nap, amit az emberiség valószínűleg soha nem fog elfelejteni. Player, 2024. 09. 11. Elérhető: <https://player.hu/tech-3/2001-szeptember-11> (Letöltés ideje: 2024. 12. 11.)

Sz.n.: A katasztrófa, aminek láttán elnémult a világ: 10 éve történt a fukusimai atomerőmű-baleset. infostart, 2021. 03. 11. Elérhető: <https://infostart.hu/kulfold/2021/03/11/a-katasztrofa-aminek-lattan-elnemult-a-vilag-10-eve-tortent-a-fukusimai-atomeromu-baleset> (Letöltés ideje: 2024. 12. 11.)

Sz.n.: A SARS-CoV-2 (Covid-19) koronavírus. Dr. Weigert Higiéniai rendszerek, é.n. Elérhető: <https://www.drweigert.com/hu/a-sars-cov-2-covid-19-koronavirus> (Letöltés ideje: 2024. 12. 11.)

Sz.n.: Amikor 50 millió ember maradt sötétben. Index, 2013. 08. 14. Elérhető: https://index.hu/tech/2013/08/14/otvenmillioan_maradtak_aram_nelkul/ (Letöltés ideje: 2024. 12. 11.)

Sz.n.: Csak három hónapra elég a víz Fokvárosban. Index, 2018. 01. 11. Elérhető: https://index.hu/tudomany/2018/01/11/csak_harom_honapra_eleg_vize_van_fokva_rosnak/ (Letöltés ideje: 2024. 12. 11.)

Sz.n.: Erőműveket is megtámadott egy számítógépes vírus. Greenfo, 2010. 09. 25. Elérhető: https://greenfo.hu/hir/eromuveket-is-megtamadott-egy-szamitogepes-virus_1285407477/ (Letöltés ideje: 2024. 12. 11.)

Sz.n.: Hajóbaleset történt a Dunán Budapesten – videóval. Tények.hu, 2024. 12. 23. Elérhető: <https://tenyek.hu/cikkek/hajobaleset-tortent-a-dunan-budapesten-videoval> (Letöltés ideje: 2024. 12. 11.)

Sz.n.: Infrastruktúra. Közszolgálati Online Lexikon, é.n. Elérhető: <https://lexikon.uni-nke.hu/szocikk/infrastruktura/> (Letöltés ideje: 2024. 12. 11.)

Sz.n.: Ipar 4.0. – Negyedik Ipari Forradalom. Pannon Egyetem Mérnöki Kar, 2023. 08. 14. Elérhető: <https://mk.uni-pannon.hu/index.php/home/hirek-hu/2899-ipar-4-0-negyedik-ipari-forradalom> (Letöltés ideje: 2024. 12. 11.)

Sz.n.: Lelőtt Malaj utasszállító: már több mint 166 millió Eurót költöttek a Hollandok a nyomozásra. MTI/iho, 2024. 03. 01. Elérhető: <https://iho.hu/hirek/lelott-malaj-utasszallito-mar-tobb-mint-166-millio-eurot-koltottek-a-hollandok-a-nyomozasra-240301> (Letöltés ideje: 2024. 12. 11.)

Sz.n.: Már felénk tart az új WannaCry? Magyarországra is megérkezhet az új zsarolóvírusos támadás. hvg.hu, 2023. 02. 13. Elérhető: https://hvg.hu/tudomany/20230209_zsarolovirus_tamadas_hackerek_sebezhetoseg_szerverek_kiberbiztonsag_wannacry (Letöltés ideje: 2024. 12. 11.)

Sz.n.: Nápolyban jól ismerik a pusztító látványt: ilyen, amikor nem viszik el a szemetet. Világgazdaság, 2022. 10. 06. Elérhető: <https://www.vg.hu/kozelet/2022/10/napolyban-jol-ismerik-a-pusztito-latvanyt-ilyen-amikor-nem-viszik-el-a-szemetet> (Letöltés ideje: 2024. 12. 11.)

Sz.n.: Oroszország: a szír légvédelem lötte le a katonai gépet, de Izrael felelős érte. hvg.hu, 2018. 09. 18. Elérhető: https://hvg.hu/vilag/20180918_Oroszorszag_a_szir_legvedelem_lotte_le_a_katonai_gepet_de_Izrael_felelos_erte (Letöltés ideje: 2024. 12. 11.)

Sz.n.: Rezsit akartak csökkenteni, a fél város ólommérgezését kapott. Index, 2016. 02. 03. Elérhető: https://index.hu/tudomany/egeszseg/2016/02/03/flint_olommergezes_vizvezetekre_ndszer_rezsicsokkentek/ (Letöltés ideje: 2024. 12. 11.)

Sz.n.: Robbantás volt egy manhattani pályaudvaron. origo.hu, 2017. 12. 11. Elérhető: <https://www.origo.hu/nagyvilag/2017/12/robbanas-volt-manhattanban>

Sz.n.: Terrortámadás volt a londoni metróban történt robbanás. Index, 2017. 09. 15. Elérhető: https://index.hu/kulfold/2017/09/15/robbanas_tortent_a_londoni_metroban/ (Letöltés ideje: 2024. 12. 11.)

White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. Presidential Decision Directives, 1998. 06. 22. Elérhető: <https://irp.fas.org/offdocs/paper598.htm> (Letöltés ideje: 2024. 12. 11.)

A BŰNÜLDÖZÉSI CÉLÚ TITKOS INFORMÁCIÓSZERZÉS ÉS A NEMZETBIZTONSÁGI SZOLGÁLATOK KAPCSOLATA MAGYARORSZÁGON

A bűnüldözési célzatú titkos információszerzés a modern magyar büntetőeljárás bizonyítási rendszerét már régóta támogató jogintézmény. A leplezett eszközök alkalmazása révén a büntetőügyben eljáró hatóságok – külső szakmai támogatással – olyan releváns információkhoz juthatnak, melyek érdemi segítséget jelentenek a tényállás felderítésében, ezáltal pedig segíthetik az anyagi igazságra törekvés ideálját. Ugyanakkor a titkos bizonyítékok beszerzése olyan hatósági cselekményeken keresztül történik, melyek alapvető jogokat érintenek, így a nyílt eljárás garanciái sem érvényesíthetők automatikusan. A tanulmány célja ezért a leplezett eszközökre vonatkozó kodifikációs előzmények bemutatása, valamint a nemzetbiztonsági szolgálatok szerepének értékelése a bűnüldözési célzatú titkos információszerzés során.

Kulcsszavak: *leplezett eszközök, nemzetbiztonsági szolgálatok, emberi jogok, büntető eljárásjog, a legalitás elve*

THE RELATIONSHIP BETWEEN THE COVERT INVESTIGATION AND NATIONAL SECURITY SERVICES IN HUNGARY

The gathering of secret information for law enforcement purposes has been a legal institution supporting the system of taking evidence in modern Hungarian criminal proceedings for a long time. Through the use of covert means, the authorities involved in investigating a criminal case can – with the support of external professionals – obtain relevant information that can be of significant assistance for the investigation and help to promote the ideal of the pursuit of material truth. At the same time, the collection of secret evidence is carried out through official acts that affect fundamental rights of the citizens, so the guarantees of an open procedure cannot be automatically enforced. The aim of this study is to present the history of codification of covert means in Hungary and to assess the role of national security services in the process of collection of covert information for law enforcement purposes.

Keywords: *covert means, national security services, human rights, criminal procedure law, the principle of legality*

Bevezetés, kodifikációs indokok

Magyarországon a bűnüldözési célokat szolgáló titkos információszerzés viszonylag régóta a jogrendszer részét képezi, a Hága-Program elfogadása óta pedig az

¹ ORCID-azonosító: 0000-0002-3547-4252 MTMT-azonosító: 10033153

ún. „információ-vezérelt rendészet” uniós szinten megfogalmazott elvárás lett,² ennek ellenére azonban annak szabályrendszere – egészen a 2017. évi XC. tv. (a továbbiakban: Be.) hatályba lépéséig – erősen fragmentált volt. A szabályozás kialakítása egyértelműen a rendszerváltás utáni időszakra tehető, és alapvetően fokozatos fejlődést mutatott. Első ízben a titkos információgyűjtéssel kapcsolatos szabályokat az 1990. évi X. tv. szabályozta. A kezdetleges szabályozás nem biztosította a bírósági kontrollt, s bár az ügyészség tudhatott az igénybevétel tényéről, annak jogszerűségének ellenőrzése körében gyakorlatilag hatáskörrel nem rendelkezett.

A magyar jog ezt követően sokáig külön kezelte a büntetőeljáráshoz kapcsolódó titkos adatszerzés, valamint a büntetőeljáráson kívüli, azonban a büntetőeljárásban is felhasználható bizonyítékot közvetíteni képes titkos információgyűjtés intézményét. Utóbbit jellemzően ágazati törvények rendezték, hiszen 11 szerv kapott arra lehetőséget,³ hogy titkosszolgálati eszközöket alkalmazzon feladatai ellátása során. Ennek eredményeként pedig ágazati törvények szerinti titkos információgyűjtés eredményét akár bizonyítási eszközként is fel lehetett használni egy későbbi büntetőeljárásban, a korábbi eljárási törvény csak a felhasználás feltételrendszerét szabályozta.⁴ Természetesen a régi Be. törekedett a két információszerzési forma közötti átmenet megteremtésére is azokban az esetekben, ha az ágazati törvények alapján bírói, vagy az igazságügyért felelős miniszter engedélyéhez kötött végzett titkos információgyűjtés eredménye alapján a nyomozás elrendelésére került sor. Utóbbi esetben ugyanis amennyiben a korábbi információgyűjtés folytatása volt indokolt, azt kizárólag a régi Be. titkos adatszerzésre vonatkozó szabályai alapján lehetett folytatni – hiszen ebben az esetben a nyomozás elrendelése okán a hatóságok titkosszolgálati munkájukat immáron folyó büntetőeljárás hatálya alatt végezték.⁵

A bűnüldözési célzatú leplezett eszközökhöz kapcsolódó egységes, eljárási törvényben szabályozott keretrendszer hiánya ezért diszkrepanciához vezetett, emellett a tisztességes eljáráshoz való jog alkalmi sérülését is eredményezhette. Nem választódott el egymástól egyértelműen a leplezett eszközök alkalmazása során a

² JANCsó Gábor: Leplezett eszközök alkalmazása: titkos információgyűjtés az új büntetőeljárási törvényben. *Acta Humana*, 2018/1. 23. o.

³ BAKONYI Mária: A leplezett eszközök új büntetőeljárási szabályozásának néhány kérdése *Magyar Jog*, 2018/7-8., 419. o.

⁴ Így a felhasználás feltétele volt, hogy a régi Be. szerinti titkos adatszerzés feltételei az információgyűjtéssel érintett bűncselekmény esetében is fennálljanak, valamint hogy az azt engedélyező szerv a legalitás elve alapján a nyomozás elrendelése iránt a szükséges intézkedéseket nyomban megtette.

⁵ A régi Be. 200.§ (3) – (4) bekezdése alapján a titkos adatszerzésre vonatkozó rendelkezések nem érintették „a nyomozás elrendelését megelőzően a bírói, illetve az igazságügyért felelős miniszter engedélyéhez kötött titkos információgyűjtést; e tevékenységet a külön törvényekben meghatározottak szerint az erre feljogosított szervek a rájuk irányadó szabályok alapján végzik. Ha a nyomozás elrendelését megelőzően külön törvény alapján a bírói, illetőleg az igazságügyért felelős miniszter által engedélyezett titkos információgyűjtés végrehajtása során az ügyben a nyomozás elrendelik, a titkos információgyűjtést a továbbiakban csak e törvény szerint, mint titkos adatszerzést lehet folytatni.”

bűnüldözési, a nemzetbiztonsági és a rendészeti célú felderítés, holott az elsőre vonatkozó szabályok tartoznak csak a büntető eljárás jogi terrénumához.⁶

Ez különösen azért hangsúlyos, mert a leplezett eszközök az egyén alapvető jogainak lényeges korlátozását jelentik, különösen a magánélethez, a magánlakás tiszteltben tartásához, az információs önrendelkezési joghoz, valamint a személyes adatok védelméhez kapcsolódó jogosítványokat tekintve. Emellett pedig a büntetőeljárásban felhasznált „titkos bizonyítékok” olyan eljárásokban kerülnek beszerzésre, melyek során nem érvényesülnek a nyílt eljárások szabályai, garanciái – titkos a bizonyítás elrendelése és foganatosítása, és sok esetben titkos maradhat annak eredménye is.⁷ Ezért a Be. kodifikációja során a jogalkotó egyértelmű szándéka volt, hogy megszüntesse ezt a töredezettséget, és a bűnüldözési célzatú felderítéshez kapcsolódó leplezett eszközök alkalmazását a büntetőeljárás jogintézményének tekintve, azt immáron a Be-ben szabályozza. Ez az egységes, áttekinthető és megismerhető szabályozás áll összhangban a jogállamiság elvével, amely elvnek az Emberi Jogok Európai Bírósága (a továbbiakban: EJEB) is relevanciát tulajdonít esetjogi gyakorlatában, mint ahogyan azon megállapításnak is, hogy a leplezett eszközökkel érintett emberi jogok csak annyiban korlátozhatók, amennyiben a demokratikus intézményrendszer védelméhez azok feltétlenül szükségesek.⁸

Jelen tanulmány célja a leplezett eszközökre vonatkozó kodifikációs előzmények bemutatása, valamint a nemzetbiztonsági szolgálatok szerepének értékelése a bűnüldözési célzatú titkos információszerezés során. Ennek megfelelően az egyéb állami szervek, hatóságok közreműködésével jelen írásban nem foglalkozunk.

A kodifikációt meghatározó emberi jogi, valamint alkotmányos elvárások

Az EJEB évtizedes⁹ joggyakorlatot alakított ki a leplezett eszközök alkalmazásával összefüggő emberi jogi jogsértésekkel kapcsolatos keresetek megítélése során. Alapvetően három emberi jog sérelmére vonatkozó érvelés jelenik meg a bíróság gyakorlatában: a magánélet és a családi élet tiszteltben tartásához való jog, a tisztességes eljáráshoz való jog, főként a bűnüldözési provokáció vonatkozásában,¹⁰

⁶ FINSZTER Géza: *A rendészet elmélete*. KJK KERSZÖV Jogi és Üzleti Kiadó Kft, Budapest, 2003. 37. o.

⁷ BARTKÓ Róbert – ELEK Balázs – FANTOLY Zsanett – HERKE Csongor: *A büntető eljárásjog tankönyve*. ORAC Kiadó Kft, Budapest, 2024. 179. o.

⁸ Case of Malone vs The United Kingdom ECHR Application no. 8691/79; Case of Huvig vs France ECHR Application no. 11105/84; Case of Kruslin vs France ECHR Application no. 11801/85, Case of Klass and Others vs Germany ECHR Application no. 5029/71, Case of Szabó and Vissy vs Hungary ECHR Application no. 37138/14.

⁹ Kis László: Leplezett eszközökkel kapcsolatos bizonyítási tilalmak az európai és a hazai joggyakorlatban – a kölcsönös bizalom elve a tagállami bíróságok és az európai bíróságok párbeszédében. *Miskolci Jogi Szemle*, 2019/2. 39. o.

¹⁰ Kiss 2019, 39.

valamint a hatékony jogorvoslathoz való jog.¹¹ Minthogy pedig a leplezett eszközök alapvető jogot korlátoznak, ugyanakkor azokból bizonyítási eszközök származhatnak, jogszerűségüket mindig az elrendelés – végrehajtás – felhasználhatóság tengelyében vizsgálja maga az EJEB is. A Be. is ebben a felosztásban szabályozza az egyes rendelkezéseket. Az EJEB elvárja,¹² hogy ezen eszközök alkalmazása során a jogállamiság elvéből levezethető megismerhetőség, előreláthatóság, törvényesség követelményei érvényesüljenek az egyezményben részes államok jogrendszerében, a konkrét szabályozás pedig legyen összhangban a szükségesség-arányosság-célszerűség¹³ mércéjével. Erre a magyar jogirodalomban Tremmel Flórián is rámutatott, hangsúlyozva annak fontosságát, hogy törvényi szintű szabálynak kell garantálnia, hogy: (a) kivel szemben rendelhető el a titkos bizonyítás; (b) mely cselekmények alapján van helye titkos bizonyítás elrendelésének; (c) a titkos bizonyítás eredménye milyen úton használható fel az eljárásban; (d) milyen garanciái vannak annak, hogy a titkos bizonyítás eredménye minden manipulációtól mentesen jusson el az azt értékelő hatóságokig; valamint, hogy (e) milyen módon kerülhetnek ezen bizonyítékok megsemmisítésre, amennyiben azokra nincs szükség, vagy nem elégségesek a bűnösség bizonyítására.¹⁴ A Be. által követett új koncepció a bűnüldözési célzatú leplezett eszközök alkalmazását egyértelműen a büntetőeljáráshoz kapcsolatosan szabályozza, elkülönítve azt a rendészeti és nemzetbiztonsági szervek ágazati jogszabályok szerinti titkos információszerzésétől.¹⁵

A nemzetközi egyezményekből fakadó emberi jogi kötelek mellett a Be. leplezett eszközökre vonatkozó szabályainak meghatározása során figyelemmel kellett lenni a jogalkotással szemben támasztott alkotmányos elvárásokra is, amely összhangban az EJEB gyakorlatával, a jogállamiságból levezethető jogbiztonság elve, valamint az emberi méltósághoz való jogra visszavezethető magánszférához való jog szükséges és arányos mértékű korlátozásának követelménye érvényesülését várta el a magyar jogalkotástól. Korábbi határozataiban az Alkotmánybíróság rámutatott, hogy bár a büntető igény érvényesítésének alapvető feltétele tárgyi oldalon a bűncselekmény, alanyi oldalon pedig az elkövető felderítése, egy jogállamban maga a bűnüldözés is kizárólag jogállami keretek között folyhat. Ez pedig a jogállami garanciák tényleges érvényre juttatásában ölthet testet, azok mellőzésére még célszerűségi vagy

¹¹ BAKONYI Mária: A leplezett eszközök megítélése az EJEB joggyakorlatában. *Ügyészek Lapja*, 2019/1. 87. o.

¹² Case of Kopp vs Switzerland 13/1197/797/1000; Case of Lüdi vs Switzerland Application no. 12433/86; Case of Van Mechelen and Others vs The Netherlands 55/1996/674/861-864.

¹³ CZEBE András: Fegyverek egyenlősége a digitális forradalom korában: a leplezett eszközök alkalmazásával összegyűjtött elektronikus adatok garanciális kérdései. *Kúria Döntése: Bírósági Határozatok. A Kúria Lapja*, 2022/1. 143. o.

¹⁴ Ezzel kapcsolatban lásd: TREMMEL Flórián: „Örökzöld kérdések” és új kihívások a büntető bizonyításban. *Sapientia sat. Ünnepi kötet dr. Cséka Ervin professor 90. születésnapjára*, Szegedi Tudományegyetem Állam-és Jogtudományi Kar, Acta Universitatis Szegediensis, 2012. 489-497. o.

¹⁵ JANCsó Gábor: A leplezett eszközök alkalmazása új rendszerének első évei és a Be. első novellája. *Rendőrségi Tanulmányok*, 2021/1. 43. o.

igazságossági szempontok sem adhatnak alapot.¹⁶ „A jogállamiság, valamint az alkotmányos büntetőjog követelményei megkívánják, hogy az állam a büntető hatalmát olyan szabályok szerint gyakorolja, amelyek egyensúlyt teremtenek az egyéneket az állammal szemben védő garanciális rendelkezések, ezen belül elsősorban a büntetőeljárás alá vont személy alkotmányos jogainak védelme és a büntető igazságszolgáltatás megfelelő működésével kapcsolatos társadalmi elvárások között”.¹⁷ Így alkotmányos elvárás, hogy a jogalkotó ezen keretek között találja meg azokat a megoldásokat, amelyek a legalitás elvét még hatékonyan képesek érvényre juttatni.¹⁸

A leplezett eszközök alkalmazásának kodifikált alapelvei

Az EJEB gyakorlatával összhangban a Be. deklarálja egyfajta minimum szabályként *a törvényesség és a törvényhez kötöttség elvét*. Minthogy jogalkotói cél volt a bűnüldözési célú titkos felderítés Be.-ben történő egységes szabályozása, így leplezett eszközt bűnüldözési céllal kizárólag a törvényben meghatározott formákban és feltételek mellett lehet alkalmazni. Megjegyzendő azonban – és ezzel a tanulmány későbbi részében még foglalkozni fogunk –, hogy az elv előírása nem érinti a nemzetbiztonsági szolgálatok, valamint a Terrorrelhárítási Központ külön törvény szerinti titkos információgyűjtési tevékenységét. Azaz a két szakszolgálatnak a jelenlegi eljárási keretrendszerben is engedélyezett a külön ágazati törvény szerinti titkos információgyűjtés folytatása.¹⁹

A törvényesség elvének mintegy kiegészítéseként a Be. rögzíti a *hatósági kontroll elvét*, amely a leplezett eszközök differenciálása során nyer értelmet. A törvény ugyanis különbséget tesz engedélyhez nem kötött,²⁰ az ügyészi,²¹ valamint a bírói engedélyhez

¹⁶ Lásd 9/1992. (I.30.) AB határozat indokolását.

¹⁷ 42/2005. (XI.14.) AB határozat indokolása.

¹⁸ Bár az Alaptörvény negyedik módosítása révén a korábbi, Alaptörvény hatályba lépését megelőzően meghozott alkotmánybírói határozatok hatályukat veszítették, mégis, mivel a jogállamiság elve az Alaptörvénynek is kiindulási pillérét képezi, a fent hivatkozott alkotmányos összefüggések és érvelések jelen alkotmányos környezetben is irányadók. Lásd ezzel kapcsolatban a 13/2013. (VI.17.) AB határozat indokolását.

¹⁹ A Be. 214.§ (2)-(3) bekezdése alapján: „Leplezett eszközöket az erre feljogosított szervek a rájuk vonatkozó jogszabályokban meghatározott bűnüldözési feladataik végrehajtása céljából kizárólag az e törvényben meghatározott szabályok alapján alkalmazhatnak.” *Ez a szabály ugyanakkor „nem érinti nemzetbiztonsági szolgálatok és a rendőrség terrorizmust elhárító szerve által a nemzetbiztonsági szolgálatokról szóló törvény alapján bűnüldözési feladataik végrehajtása céljából folytatott titkos információgyűjtést.”*

²⁰ Ezek a következők: titkosan együttműködő személy igénybe vétele; csapda állítása; a sértett vagy más személy helyettesítése; rejtett figyelés; az érintett személy hatósági megtevesztése.

²¹ Ügyészi engedélyhez kötött leplezett eszközök: fizetési műveletek megfigyelése; a büntetőjogi felelősségre vonás elkerülésének kilátásba helyezése; megfigyelés; álvásárlás; fedett nyomozó alkalmazása; fedőkirat, fedőintézmény, fedőadat felhasználása.

kötött leplezett eszközök²² között, amelyek részletes ismertetése jelen tanulmányban terjedelmi okok miatt nem lehetséges, de annak nem is kitűzött célja. A rendszerbe foglalás a fokozatosság mentén történt, hiszen minél nagyobb beavatkozást eredményez egy leplezett eszköz alkalmazása az egyén magánszféréjába, annál inkább „magasabb” szintű fórum közreműködése tudja a jogi garanciákat közvetíteni. Ugyanakkor változatlanul probléma – és ez a magyar jogrendszer évtizedes „adóssága” –, hogy egyedül az ügyészségi rendszer az, ahol ez a hatósági kontroll „rendszeren belül” érvényesül, azaz az ügyészség által alkalmazott leplezett eszköz törvényessége felett nem egy külső szerv, hanem a felettes ügyészség gyakorolja a felügyeletet. Holott erre a Be.-ben a bíróság is kijelölhető lett volna.

Szintén hangsúlyos alapelv a *szubszidiaritás elve*, amely szerint leplezett eszköz alkalmazása akkor lehetséges, ha más, hagyományos nyomozati módszerrel az adott információ vagy bizonyíték nem lenne beszerezhető. Ebből tehát az is következik, hogy bűnfelderítést elsődlegesen a rendes nyomozati eszközök igénybevételével van lehetőség lefolytatni, ezekhez képest a leplezett eszközök kivételesnek tekinthetők.

A Be. megjeleníti az EJEB és az Alkotmánybíróság által is elvárt *szükségességi, arányossági elvet*,²³ valamint a *célhoz kötöttség elvét* is. Ennek alapján leplezett eszközt alkalmazni csak akkor lehetséges, ha az a büntetőeljárás céljainak eléréséhez szükséges, és csak a célokkal arányos mértékben és ideig eredményezhetik az alapvető jog korlátozását. Az időbeli korlátok alapvetően az ügyészi és a bírói engedélyes leplezett eszközök esetében érvényesülnek.

Legalitás elve vs. leplezett eszközök

Kétségtől megállapítható, hogy a Be. jelentős előrelépést hozott a bűnüldözési célzatú titkos információszerezés területén, megszüntetve a korábbi töredezett és kevésbé átlátható szabályozási rendszert. A jogalkotás azonban nem volt tökéletes, hiszen a legalitás elvének kiszélesített értelmezésével a leplezett eszközök alkalmazásának lehetősége is kiszélesedett a büntetőeljárás vonatkozásában. Kiindulási pont, hogy bűnüldözési célzatú titkos információgyűjtés alapja a bűncselekmény elkövetésének gyanúja kell, hogy legyen. Ezen gyanú hiányában klasszikus értelemben büntetőeljárás sem folytatható. Ugyanakkor a Be. az alábbiakban említésre kerülő előkészítő eljárás beemelésével a nyomozás megindítását megelőző időszakra is szabályozott környezetet teremtett a leplezett eszközök alkalmazásának, akár ilyen egyszerű gyanú hiányában is, mindezt pedig úgy, hogy elrendelése esetén az előkészítő eljárást tulajdonképpen a büntetőeljárás részévé tette.²⁴ Ezzel lehetővé téve, hogy alapvetően nyomozati jogkörrel nem

²² Ezek az alábbiak: információs rendszer titkos megfigyelése; titkos kutatás; hely titkos megfigyelése; küldemény titkos megismerése; lehallgatás.

²³ Ennek fontosságát hangsúlyozta éppen a titkos információgyűjtés témakörében született 2/2007. (I.24.) AB határozatában is a magyar Alkotmánybíróság.

²⁴ Lásd a Be. 339.§ (1) bekezdését, mely a következők szerint fogalmaz: „A büntetőeljárás az e Részben meghatározott feltételek esetén előkészítő eljárással kezdődik.”

rendelkező, büntetőeljáráson kívüli hatóságoknak is legyen lehetőségük a büntetőeljáráshoz kapcsoltn leplezett eszközöket alkalmazni.

Ennek törvényi alapját részben az alanyokat szabályozó fejezetében teremti meg a Be. azzal, hogy a 36.§ (1) bekezdésében elvi éllel rögzíti, hogy az előkészítő eljárásban a leplezett eszközök alkalmazása során a Be. által arra feljogosított szervek is eljárhatnak. Részben pedig a Be. 339.§ (3) bekezdésében, amely a Nemzeti Védelmi Szolgálatot, valamint a Terrorelhárítási Központot is feljogosítja előkészítő eljárás lefolytatására.

Bár a Be. rögzíti, hogy az arra külön ágazati törvényekben feljogosított szervek bűnüldözési feladataik végrehajtása céljából a Be. szabályai szerint vehetnek igénybe leplezett eszközöket – ezzel tehát a jogalkotó a Be. rendelkezéseit összekapcsolta az ágazati törvényekkel –, probléma lehet, hogy a nemzetbiztonsági szolgálatok, valamint a Terrorelhárítási Központ, akik alapvetően nemzetbiztonsági és terrorelhárítási célzattal folytathatnak felderítő tevékenységet, a saját ágazati törvényükben foglaltak szerint jogosultak a Be. 214.§ (3) bekezdése alapján bűnüldözési célzatú titkos információgyűjtést végezni.²⁵ Ez a szabály így a Be. és az egyéb ágazati törvények közötti kettősséget fenntartja, biztosítva a hatóságoknak a titkos művelet révén történő bizonyítékbeszerzést. A Be. bár az így beszerzett bizonyítási eszközök felhasználására vonatkozó törvényi feltételeket rögzíti, az említett szervek eljárásában az eltérő célú felderítési funkciók mégis összemósódhatnak egymással.

Szintén problematikus a Terrorelhárítási Központ és a Nemzeti Védelmi Szolgálat leplezett eszközök alkalmazásával összefüggésben telepített eljárási jogköre az ún. előkészítő eljárásban. Az előkészítő eljárás a magyar jogrendszer új eljárási jogintézménye. Funkciója abban áll, hogy a nyomozást megelőzően lehetőség legyen arra, hogy a nyomozás megindításához a legalitási elv alapján szükséges egyszerű gyanú vizsgálata körében további eljárási cselekményeket, bizonyítást foganatosítsanak a hatóságok. Mivel az előkészítő eljárás nem „nyílt eljárást”, domináns a leplezett eszközök igénybevétele ebben a fázisban. Ebben az optikában pedig kétséges, hogy nyomozó hatóságnak nem tekinthető szervek (Nemzeti Védelmi Szolgálat, Terrorelhárítási Központ) a nyomozás elrendelése tárgyában való döntés meghozatala érdekében titkosszolgálati eszközök felhasználásával bizonyítási eszközöket szerezhetnek be a büntetőeljárás számára, büntetőeljárás keretei között. Változatlanul fontos hangsúlyozni, hogy a felderítés belső védelmi, terrorelhárítási, rendészeti, nemzetbiztonsági és természetesen a témánk szempontjából fontos bűnüldözési célokat is szolgálhat.²⁶ Ezek között pedig a határvonalak nem mosódhatnak el.

²⁵ A hivatkozott törvényi rendelkezés szerint a fentiekben rögzített törvényi kritérium nem érinti a nemzetbiztonsági szolgálatok és a rendőrség terrorizmust elhárító szerve által a nemzetbiztonsági szolgálatokról szóló törvény alapján bűnüldözési feladataik végrehajtása céljából folytatott titkos információgyűjtést.

²⁶ FINSZTER Géza: Szabályozott felderítés – titkosított büntetőeljárás. *Miskolci Jogi Szemle*, 2019/1. 281. o.

A nemzetbiztonsági szolgálatok szerepe és helyzete a bűnüldözési célzatú titkos információgyűjtésben

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. tv. (a továbbiakban: Nbtv.) részletes szabályrendszert tartalmaz mind az engedélyhez nem kötött, mind pedig az engedélyhez kötött titkos információgyűjtéssel kapcsolatban. Az Nbtv. által meghatározott normatív keretrendszer a Be. hatályba lépését megelőzően csak kisebb mértékben változott, ugyanakkor a bűnüldözési célzatú titkos információszerzés eljárási törvényben való megjelenésével a jogalkotó szükségképpen nyúlt hozzá az ágazati szabályozókhoz is. A bűnüldözési célzatú információszerzés leválasztása a konkrét bűncselekmény gyanújához nem kapcsolódó titkosszolgálati eszközök alkalmazásától jelentős előrelépés. Az ágazati jogszabályokban a Be. hatályba lépésével átvezetett módosításokat három jogpolitikai cél határozta meg: „egyrészt a bűnüldözési célzatú titkos információgyűjtés elválasztása a rendészeti, vagy nemzetbiztonsági célú titkos információgyűjtéstől”, másrészt a Be. által szabályozott normatív keretek ágazati törvényekbe történő átültetése, harmadrészt pedig a diszcrepancia felszámolása.²⁷ Ezzel – többek között – a jogalkotó célja volt az is, hogy a nemzetbiztonsági szolgálatokkal²⁸ szemben megfogalmazott állampolgári bizalmatlanságot²⁹ oldani tudja. Azaz a 2018-as rendszerszintű átalakítással ágazati jogszabályok – azaz a Be-n kívüli normák – alapján tisztán bűnüldözési célzatú titkos információgyűjtés nem folytatható, amely alól kizárólag az Nbtv., és az ott megjelölt nemzetbiztonsági érdek került kiemelésre. Azaz bűnüldözési célzatú titkos bizonyítékbeszerzést már annak kezdetétől fogva büntetőeljárás keretei között (vagy előkészítő eljárásban vagy nyomozásban) szükséges folytatni, korlátozott lehetőségek mellett azonban bűnüldözést támogató, illetve bűnmegelőző célzattal az ágazati törvények is lehetővé teszik továbbra is a titkos információgyűjtést.³⁰

Ugyanakkor ahhoz, hogy értékelni tudjuk a fenti módosításokat kifejezetten a nemzetbiztonsági szolgálatok vonatkozásában, első lépésként azt kell detektálnunk, hogy e hatóságok milyen feladatkörben tudnak kapcsolódni egy büntetőeljáráshoz, adott esetben egy büntetőeljárás megindításához milyen módon járulhatnak hozzá adatszerző tevékenységükkel.

Kiindulási pontunk az, hogy ahhoz, hogy a büntetőeljárás „gépezete” beinduljon, információra, adatra van szükség, amely körvonalazza egy vagy több lehetséges bűncselekmény megvalósulását, vagy legalább arra elégséges, hogy a hatóság annak

²⁷ Solti István: A magyar nemzetbiztonsági szolgálatok esete a jogállami szabályozással. *Belügyi Szemle*, 2022/1. 93. o.

²⁸ Az Nbtv. 1.§-a alapján ezen szolgálatok közé tartozik: az Információs Hivatal, az Alkotmányvédelmi Hivatal, a Katonai Nemzetbiztonsági Szolgálat, a Nemzetbiztonsági Szakszolgálat, valamint a Nemzeti Információs Központ.

²⁹ Ennek ingoványos voltáról lásd bővebben: Vadász Pál – Zódi Zsolt: A nemzetbiztonsági szolgálatok és rendvédelmi szervek információkereséshez kapcsolódó számon kérhetősége. *Jogtudományi Közlöny*, 2020/11. 518-527. o.

³⁰ Ezekről bővebben lásd: Nyeste Péter – Szendrei Ferenc: *A bűnügyi hírszerzés kézikönyve*. Ludovika Egyetemi Kiadó, Budapest, 2019.

alapján előkészítő eljárást rendeljen el annak érdekében, hogy az egyszerű gyanú kérdésében megalapozott döntést tudjon hozni. Ez az információ természetesen a hatóság birtokába tud kerülni normál működése során is, azonban az esetek többségében kívülről érkezik jelzés, feljelentés formájában. A nemzetbiztonsági szolgálatok törvényi feladata az információk beszerzése és értékelése, így ezen hatóságok szerepe első lépésként ezen „indító információ” megszerzésében érhető tetten.³¹ A bűnügyi hírszerzés ugyanakkor több ágú tevékenység, hiszen stratégiai és taktikai funkciója mellett nyomozást támogató szerepe is van. Témánk szempontjából főként ez utóbbinak van relevanciája,³² hiszen ez utóbbi tud szervesen is kapcsolódni büntetőeljáráshoz. A nyomozást támogató bűnügyi hírszerzés központi kiindulási pontja az elemző munka a nyomozás eredményességének támogatása érdekében. Feladata konkrét, illetve egyedi bűncselekményekre vonatkozó adatok, információk elemzése révén a nyomozati munka információigényének kiszolgálása akár konkrét bizonyítási eszközök útján.³³

Ugyanakkor a szolgálatok nemcsak az információ közvetlen megszerzésében működhetnek közre, hanem az információ megszerzéséhez közvetve támogatást is nyújthatnak (bűnüldözést támogató funkció). Kiemelt szerepe van ebben a tekintetben a Nemzetbiztonsági Szakszolgálatnak, amely hatóság az Nbtv. 8.§ (1) bek. a)-b) pontjai alapján saját eszközeivel és módszereivel – megkeresés alapján – végez támogató szolgáltatást titkos információgyűjtés, illetve a Be. szerinti leplezett eszközök végrehajtásához, illetve az ezen titkos bizonyítást végző hatóságok számára különleges technikai eszközöket, illetve anyagokat szolgáltathat. Azaz, bár a Be. külön nem nevesíti, de a hatályos eljárási jogunk szerinti leplezett eszközök foganatosítása során a Nemzetbiztonsági Szakszolgálat is fontos, a titkos bizonyíték megszerzését segítő, azt

³¹ Az Nbtv. 4.§ c) pontja alapján az *Információs Hivatal* információkat gyűjt a nemzetbiztonságot veszélyeztető külföldi szervezett bűnözéssel összefüggésben, különösen a transznacionális jellegű deliktumok esetében. Ilyen lehet például a terrorcselekmény, illegális kábítószer- illetve fegyverkereskedelem, tömegpusztításra alkalmas, vagy arra szolgáló eszközök, berendezések, ezek alkotóelemeinek illegális nemzetközi kereskedelme. Az *Alkotmányvédelmi Hivatal* esetében a büntetőeljáráshoz való kapcsolódás már erősebben tetten érhető a feladatkörök szintjén is, hiszen az Nbtv. 5.§ j) pontja alapján az ott taxatív felsorolt bűncselekményekre vonatkozó információgyűjtés a Hivatal egyik alapvető feladata. Ez elsősorban saját állományi körben, valamint a Kormány és a Kormány tagjainak irányítása, felügyelete alatt álló költségvetési szervek tekintetében irányadó. A büntetőeljárást esetlegesen megalapozó információgyűjtés terén a *Katonai Nemzetbiztonsági Szolgálat*nak is fontos szerepe van, hiszen az Nbtv. 6.§ g)-i), valamint n) pontjai alapján ilyen feladatokat lát el a nemzetbiztonságot veszélyeztető terroriszervezetek és terrorcselekmények, illetve az illegális kábítószer-, és fegyverkereskedelem felderítése, valamint a honvédelmi érdekeket sértő kibertámadások, kiberbűncselekmény elhárítása érdekében. Emellett pedig működési területén információt szerez az Nbtv. 6.§ na)-nb) pontjában taxatív felsorolt bűncselekmények felderítésének támogatása érdekében.

³² Itt szükséges azonban megjegyezni, hogy a taktikai bűnügyi hírszerzés is rendelkezik büntetőeljárási kapcsolódással, hiszen a hírszerzés ezen szegmensében konkrét bűncselekmény(ek) azonnali megelőzése, kezelése, megoldása a prioritás.

³³ NYESTE Péter – NAGY Ivett: A bűnügyi hírszerzés az elméletben és a gyakorlatban. *Rendőrségi Tanulmányok*, 2021/1. 7. o.

támogató szerepkörben tud megjelenni a leplezett eszközt foganatosító hatóság megkeresése alapján.

A későbbi nyomozati munka információszükségletének kiszolgálása mellett a szolgálatok felderítő funkciója is releváns, azonban ezen tevékenységüket kizárólag a nyomozás elrendelését megelőző időszakban gyakorolhatják.³⁴ Ez a határvonal érthető, hiszen a nemzetbiztonsági szolgálatokat a Be. nem ruházza fel nyomozati jogkörrel, így klasszikus nyomozati tevékenységet sem végezhetnek, ugyanakkor bűnüldözési célzatú titkos felderítést éppen a Be. 214.§ (3) bekezdésében rögzített felhatalmazás alapján igen. Ez a felderítő funkció a későbbi nyomozás információigényét akár bizonyítási eszközök beszerzése és rendelkezésre bocsátása révén is támogathatja, amellyel a jogalkotó a titkos bizonyítást ebben az esetben – még ha bűnüldözési célzatú is – kvázi kiemelte a büntetőeljárás normarendszer kereteiből. Ezzel pedig „előbbre hozta” az előző pontban a legalitással összefüggésben jelzett dogmatikai problémafelvetés lehetőségét. Ugyanis elképzelhető, hogy az Nbtv. alapján végzett „felderítést célzó titkos bizonyítékbeszerző” tevékenység még az ún. előkészítő eljáráshoz sem kapcsolódik, hiszen az Nbtv. szerinti szolgálatok a Be. alanyainak rendszerében nem kerülnek említésre. Így az eljárási törvény az előkészítő eljárással összefüggésben sem ruházza fel e szerveket „felderítő funkcióval”. Azaz az Nbtv., valamint a fentiekben hivatkozott normatív felhatalmazás a szolgálatok számára bűnüldözési célzatú titkos bizonyítást tesz lehetővé az előkészítő eljárás megindítását megelőzően is. A „nyomozás elrendelését megelőzően” időbeli kitétel is csak ezt erősíti. Ennek alapján tehát kijelenthető, hogy az Nbtv. nemzetbiztonsági érdekből a szolgálatok által végzett titkos felderítő tevékenységet büntetőeljáráshoz nem kapcsoltan is biztosítja, így a jogalkotói indokolásban is hangsúlyozott „elválasztás” nem teljesült teljeskörűen. Ez pedig éppen a Be. koncepcionális átalakulása okán megfontolandó kérdés a jövőben.

Mint ahogy az egyes nemzetbiztonsági szolgálatok a fentiek szerint jogosultak titkos információgyűjtést végezni – azonban nem nyomozati funkció mellett, hanem a törvényben rögzített egyes feladataik ellátása körében és érdekében –, az Nbtv. ennek részletes szabályrendszerét is tartalmazza. A titkos bizonyítást, felderítő feladatokat az arra kijelölt szolgálatok maguk, vagy más szolgálat közreműködése révén hajtják végre, ugyanakkor technikai támogatás érdekében a Nemzetbiztonsági Szakszolgálatot is igénybe vehetik. Ez fakad a Szakszolgálat fentiekben leírt „bűnüldözést támogató funkciójából”. Ez esetben természetesen a jogszerűségért való felelősség is osztott, hiszen az alkalmazást megrendelő szolgálat tartozik felelősséggel az alkalmazás, míg a Szakszolgálat a végrehajtás jogszerűségéért. Az említett titkos információgyűjtési

³⁴ Az Nbtv. alapján mind az Alkotmányvédelmi Hivatal, mind pedig a Katonai Nemzetbiztonsági Szolgálat végezhet ilyen felderítő tevékenységet a törvény által tételesen felsorolt bűncselekmények tekintetében működési területüket érintően. Ez a tevékenység egyes bűncselekmények esetében nem konkrét személyi körhöz kapcsolatosan (pl. állam elleni bűncselekmények, emberiség elleni bűncselekmények), míg mások esetében (pl. vesztegetés) csak bizonyos az Nbtv. 5/A.§ (1) bekezdése szerinti szervekkel összefüggésben, vagy az adott szolgálatok egyes törvényben meghatározott feladatainak ellátásával összefüggésben végezhető.

formák alapvetően differenciáltak a törvényben aszerint, hogy külső (bírói) engedélyhez kötöttek-e, vagy sem.³⁵ Fontos ugyanakkor kiemelni, hogy a Be. által követett koncepcionális optikai váltás a bűnüldözési célzatú titkos információgyűjtést a büntető eljárási jog hatálya alá helyezte, ezzel biztosítva, hogy az abban érintett szervek immáron a büntetőeljárási törvény által teremtett garanciális keretek között végezzék e tevékenységüket.³⁶ Ennek a paradigmaváltásnak köszönhető, hogy számos ágazati jogszabály, így a rendőrségről, valamint a Nemzeti Adó- és Vámhivatalról szóló törvény is módosításra került. Ugyanakkor a korábbiakban is már említett, deklarált eljárási szabályból fakadóan az Nbtv. nem tartozott e jogszabályok közé, ugyanis itt csak a Be. által bevezetett terminológiai változások kerültek átvezetésre. Ezt pedig éppen azért fontos hangsúlyozni, mert bizonyos információgyűjtési formák bírói kontrollja tekintetében tapasztalhatók eltérések azok nemzetbiztonsági és büntetőeljárási jogi formája között. Így fontos kiemelni, hogy addig, amíg a Be. által szabályozott lehallgatás, titkos megfigyelés, illetve a küldemény titkos megfigyelése minden körülmények között bírói engedélyes tevékenység, addig a nemzetbiztonsági szolgálatok bizonyos terjedelemben ezeket külső engedély nélkül is végezhetik³⁷. Ez nehezen indokolható jogállami különbségtétel. Hiszen mindkét esetben arról van szó, hogy az egyes titkos bizonyítékszerzési formák bűnüldözési célokat szolgálnak, szolgálhatnak. Azaz a Be.-hez hasonló egységes szemlélet jogalkotói ignorálása nem volt indokolt ezen a területen, főként úgy nem, hogy a Be. egyes jogintézményei – pl. az ügyészengedélyes megállapodás³⁸ – szó szerint, azaz változtatás nélkül – éppen

³⁵ Jelen tanulmánynak alapvetően nem célja ezen eszközök tételes bemutatása, ugyanakkor a teljesség igényével szükséges azokat megemlíteni. Az Nbtv. 54.§ (1) bekezdése alapján külső engedélyhez nem kötött eszközök a következők: felvilágosítás kérése, leplezett jelleg melletti információgyűjtés, titkos kapcsolat létesítése, csapda állítása, információs rendszer létrehozása és alkalmazása, fedőokmány és fedőadat,-okirat kiállítása, használata, fedőintézmény alkalmazása, titkos megfigyelés, bírói engedélyes eseteken kívüli titkos lehallgatás és a tartalom-rögzítése, valamint elektronikus hírközlő hálózatokon továbbított adatok körének megállapításához és azonosításához szükséges adatgyűjtés. Külső (bírói) engedélyhez kötött titkos eszközök az Nbtv. 56.§-alapján: titkos kutatás és titkos megfigyelés és az észlelteknél technikai úton történő rögzítése az „érzékeny helyszíneken”, postai vagy egyéb zárt küldemény tartalmának megismerése és rögzítése, információs rendszerekben kezelt adatok titkos megismerése, titkos megfigyelési eszközök elrejtése, valamint információs rendszerekbe történő beavatkozás kiberfenyegetés elhárítása céljából.

³⁶ Lásd a 2017. évi XCIII. tv. Általános Indokolását.

³⁷ A nemzetbiztonsági szolgálatok a feladataikat érintő személyeket és az azokhoz kapcsolódó lakást, egyéb helyiséget, bekerített helyet, nyilvános helyet, vagy járművet titkosan megfigyelhetnek, az észlelteket rögzíthetik, bizonyos „fokozott védeltséget élvező helyszínek” kivételével bírói engedély nélkül végezhetnek lehallgatást, elektronikus hírközlő csatornák tartalmát ismerhetik meg.

³⁸ Ennek lényege abban áll, hogy ügyési engedély mellett a nemzetbiztonsági szolgálatok megállapodást köthetnek az együttműködő terheltekkel, amennyiben azok nemzetbiztonsági célzatú együttműködése jelentősebb érdek, mint az általuk elkövetett bűncselekmény miatti felelősségre vonáshoz kapcsolódó állami érdek. Az együttműködés eredményeként – a büntető eljárási normarendszerhez hasonlóan – a terhelttel szemben nem indul az általa elkövetett bűncselekmény miatt büntetőeljárás, vagy a már megindult eljárás került megszüntetésre. A Be. rendelkezéseivel egyezően az Nbtv. alapján sem köthető megállapodás olyan elkövetővel, aki szándékos életellenes, vagy súlyosabb következményekkel (maradandó fogyatékoság, súlyos egészségromlás) járó szándékos testi épséget vagy egészséget sértő bűncselekményt követett el.

a kodifikációs célként megjelölt koherencia biztosítása érdekében – kerültek a Be.-ből átvételre az Nbtv.-be.

Összegzés

A bűnüldözési célzatú titkos információgyűjtés hazai fejlődéstörténete jól példázza, hogy a kezdeti, fragmentált, eljárásjogi garanciákkal kellően át nem szótt rendszer „profiltisztítása” a Be. kodifikációs munkálatai során hogyan valósult meg. Azon jogalkotói cél, amely arra irányult, hogy a bűnüldözési célzatú titkos bizonyítás immáron a büntetőeljárás szabályrendszeréhez kapcsolatosan, az abban érvényesülő garanciák mentén valósuljon meg, egyértelmű jogállami elvárás volt, és jogalkotás hosszú évekre visszamenő adóssága is egyben. A Be. leplezett eszközökkel kapcsolatos, valamint a titkos információgyűjtés és a büntetőeljárás viszonyrendszerét szabályozó normatív rendelkezései immáron kellő háttérrel biztosítanak a fenti kodifikációs cél biztosításához.

Azonban, mint az kiolvasható a tanulmányból is, éppen a nemzetbiztonsági szolgálatok rendszerében kerültek meghagyásra olyan rendelkezések, amelyek a fenti „profiltisztítás” ellenére anomáliákat okoznak az egységesítő szemlélet terén. Ehhez a Be. 214.§ (3) bekezdésében foglalt jogalkotói „felhatalmazás” erős támogatás is, amelynek hosszú távú fenntartása éppen a fent említett jogalkotási célkitűzés következetes érvényesítése érdekében átgondolandó. A tanulmányban jelzett felvetések, így a nemzetbiztonsági szolgálatok azon törvényi jogköre, hogy egyes, a büntetőeljárás szabályrendszerben is bírói engedélyhez kötött titkos bizonyítékszerzési tevékenységeket bizonyos esetekben külső engedély nélkül is végezhetnek, illetve a szolgálatok azon hatásköre, hogy meghatározott bűncselekményekhez telepített, a nyomozást megelőzően érvényesülő felderítő hatáskörrel rendelkeznek, azért kerültek külön is kiemelésre, mert ezeken a területeken sérülni látszik a titkos bizonyítás szabályrendszerében érvényesíteni kívánt koherencia. Az jól látható, hogy a kodifikátor határozott célja volt, hogy az egyes nemzetbiztonsági szolgálatoknak biztosítsa a későbbi nyomozást támogató felderítési funkciót, ugyanakkor annak időbeli hatályának meghatározása további tudományos kérdések felvetéséhez vezet. Ezen feladatkör „nyomozást megelőző” jellege ugyanis nem egyértelműen kapcsolja e titkosszolgálati eszközök alkalmazhatóságának lehetőségét az annak alapját képező információk minőségéhez. Az a Be. 339.§ (2)-(3) bekezdése alapján ugyanis egyértelműnek látszik, hogy a szolgálatokat a Be. nem jelöli ki olyan szervként, akik előkészítő eljárást folytathatnak, ugyanakkor felderítő tevékenységük keretei között bizonyítási eszközöket tudnak a későbbi büntetőeljárás számára beszerezni.

Összességében ugyanakkor megállapítható, hogy a bűnüldözési célzatú titkos információgyűjtés leválasztása az egyéb titkos bizonyítékbeszerző eljárásokról és annak büntetőeljárásba történő integrálása immáron nemcsak célkitűzésként, de expressis verbis a norma szintjén is megjelenik hatályos jogrendszerünkben, amely az

abban érintett szerveket segíteni tudja nemcsak a hatékonyság, de az eredményesség³⁹ fokozásában is.

Felhasznált irodalom:

BAKONYI Mária: A leplezett eszközök új büntetőeljárési szabályozásának néhány kérdése. *Magyar Jog*, 2018/7-8. ISSN: 0025-0147

BAKONYI Mária: A leplezett eszközök megítélése az EJEJ joggyakorlatában. *Ügyészek Lapja*, 2019/1. ISSN: 1217-7059

BARTKÓ Róbert – ELEK Balázs – FANTOLY Zsanett – HERKE Csongor: *A büntető eljárásjog tankönyve*. ORAC Kiadó Kft, Budapest, 2024. ISBN: 978 963 258 633 5

CZEBE András: Fegyverek egyenlősége a digitális forradalom korában: a leplezett eszközök alkalmazásával összegyűjtött elektronikus adatok garanciális kérdései. *Kúria Döntése: Bírósági Határozatok. A Kúria Lapja*, 2022/1. ISSN: 2786-3964

FINSZTER Géza: *A rendészet elmélete*. KJK KERSZÖV Jogi és Üzleti Kiadó Kft, Budapest, 2003. ISBN: 9632247019

FINSZTER Géza: Szabályozott felderítés – titkosított büntetőeljárás. *Miskolci Jogi Szemle*, 2019/1. ISSN: 1788-0386

GYŐRI Attila – SZENDREI Ferenc: A leplezett eszközök alkalmazásának tapasztalatai a jogintézmény bevezetésétől napjainkig. *Rendőrségi Tanulmányok*, 2021/1. ISSN: 2630-8002

JANCSÓ Gábor: Leplezett eszközök alkalmazása: titkos információgyűjtés az új büntetőeljárési törvényben. *Acta Humana*, 2018/1. ISSN: 0866-6628

JANCSÓ Gábor: A leplezett eszközök alkalmazása új rendszerének első éveit és a Be. első novellája. *Rendőrségi Tanulmányok*, 2021/1. ISSN: 2630-8002

KIS László: Leplezett eszközökkel kapcsolatos bizonyítási tilalmak az európai és a hazai joggyakorlatban – a kölcsönös bizalom elve a tagállami bíróságok és az európai bíróságok párbeszédében. *Miskolci Jogi Szemle*, 2019/2. ISSN 1788-0386

NYESTE Péter – Szendrei Ferenc: *A bűnügyi hírszerzés kézikönyve*. Ludovika Egyetemi Kiadó, Budapest, 2019. ISBN 9786155945793

NYESTE Péter – NAGY Ivett: A bűnügyi hírszerzés az elméletben és a gyakorlatban. *Rendőrségi Tanulmányok*, 2021/1. ISSN 2630-8002

SOLTI István: A magyar nemzetbiztonsági szolgálatok esete a jogállami szabályozással. *Belügyi Szemle*, 2022/1. ISSN 2062-9494

³⁹ Az elsődleges tapasztalatok tekintetében lásd: Győri Attila – Szendrei Ferenc (2021): A leplezett eszközök alkalmazásának tapasztalatai a jogintézmény bevezetésétől napjainkig. *Rendőrségi Tanulmányok*, 2021/1. 72-92. o.

TREMMELE Flórián: „Örökzöld kérdések” és új kihívások a büntető bizonyításban. *Sapientia. Ünnepi kötet dr. Cséka Ervin professor 90. születésnapjára*, Szegedi Tudományegyetem Állam-és Jogtudományi Kar, Acta Universitatis Szegediensis 2012. 489-497.

VADÁSZ Pál – ZÓDI Zsolt: A nemzetbiztonsági szolgálatok és rendvédelmi szervek információkereséshez kapcsolódó számon kérhetősége. *Jogtudományi Közlöny*, 2020/11. ISSN 0021-7166

SZERZŐINK

Dr. Bányász Péter	PhD, a Nemzeti Közszerológati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar Kiberbiztonsági Tanszék egyetemi docense
Bányász-Váczi Kincső Boróka	a Nemzeti Közszerológati Egyetem Nemeskürty István Tanárképző Kar munkatársa
Dr. habil. Bartkó Róbert	PhD, a Széchenyi István Egyetem DF ÁJK Büntetőjogi Tanszék tanszékvezető egyetemi docense
Földes Tibor	főhadnagy, az MH Légi Műveleti Vezetési és Irányítási Központ beosztott tisztje
Griffiths Dániel	az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusza
Knapp Gábor	alezredes, a KNBSZ munkatársa, a Nemzeti Közszerológati Egyetem Hadtudományi Doktori Iskola doktorandusza
Kotsis Levente	az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusza
Dr. Magyar Sándor	ezredes, PhD, a KNBSZ munkatársa, az NKE Katonai Nemzetbiztonsági Tanszék vezetője, egyetemi docens
Neuspiller Ferenc	az Eötvös Lóránd Tudományegyetem Biztonságtudományi Doktori Iskola doktorandusza
Pál Anita Brigitta	az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusza
Dr. Pál István	PhD, az Eötvös Lóránd Tudományegyetem Bölcsészettudományi Kar egyetemi adjunktusa
Pozderka Gábor	ezredes, a Honvéd Vezérkar munkatársa, a Nemzeti Közszerológati Egyetem Hadtudományi és Honvéd Tisztképző Kar Katonai Műszaki Doktori Iskola doktorandusza

E SZÁMUNKAT LEKTORÁLTÁK

Dr. Farkas Ádám	alezredes, PhD, a KNBSZ munkatársa, a Széchenyi István Egyetem Deák Ferenc ÁJK és a Nemzeti Közszolgálati Egyetem HHK tudományos főmunkatársa
Dr. Jung András	PhD, az Eötvös Lóránd Tudományegyetem, IK Térképtudományi és Geoinformatikai Intézet habilitált egyetemi docense
Dr. Kucsera Erika	ezredes, PhD, a KNBSZ munkatársa
Dr. Magyar Sándor	ezredes, PhD, a KNBSZ munkatársa az NKE Katonai Nemzetbiztonsági Tanszék vezetője, egyetemi docens
Dr. Pál István	PhD, az Eötvös Lóránd Tudományegyetem Bölcsészettudományi Kar oktatója
Dr. Puskás Béla	ezredes, PhD, a KNBSZ munkatársa
Tóth Csaba Mihály	ezredes, a KNBSZ munkatársa

A SZAKMAI SZEMLÉBEN TÖRTÉNŐ PUBLIKÁLÁS FELTÉTELEI

Etikai követelmények:

- Az írásmű másol, ebben a formájában még nem jelent meg;
- a szerző(k) kizárólagos szellemi tulajdona, amelyet a szerzői nyilatkozat kitöltésével és aláírásával igazol(nak);
- korrekt, visszakereshető – a szerzői útmutatóban meghatározott – hivatkozásokkal ellátott;
- bibliográfiával ellátott (amely tartalmazza a hivatkozott irodalom jegyzékét, az internetes anyagok jegyzékét a letöltés idejével együtt);
- a szerző(k) saját véleményét is tükrözheti, amely értelemszerűen nem mindig egyezik meg a Szolgálat álláspontjával.
- A kézirat azonban nem tartalmazhat rasszista, xenofób vagy szélsőséges nézeteket valló megállapítást.

Megjelenéssel kapcsolatos információk:

- A kéziratot elektronikus formában, kérjük megküldeni a szakmai.szemle@knbsz.gov.hu email címre.
- A közlésre elfogadott írásokért – a szerzői nyilatkozattal létrejött megállapodás figyelembevételével – szerzői honorárium fizethető.
- A kéziratokat a Szerkesztőbizottság minden esetben lektoráltatja. (A kiadványban megjelentetni kívánt írásokat a Szolgálat kompetens, tudományos fokozattal rendelkező munkatársai vagy más szakértők lektorálják.)
- A Szerkesztőbizottság – a lektori vélemények figyelembevételével – fenntartja a jogot, hogy a megjelenésre alkalmatlannak ítélt kéziratokat indoklás nélkül nem közli.
- A kiadványban bárki publikálhat, akinek az írását a Szerkesztőbizottság az etikai, tartalmi és formai követelmények alapján, kiadványban történő megjelentetésre, valamint az interneten történő közzétételre alkalmasnak tartja.
- A kézirathoz kérjük mellékelni a szerző vagy szerzők nevét, rendfokozatát, beosztását vagy munkakörét, állandó lakcímét, telefonon és interneten történő elérhetőségét, ORCID- és MTMT-azonosítójukat – amennyiben utóbbiakkal rendelkeznek.

Tartalmi követelmények:

- A folyóiratokban – jellegével összhangban – a honvédelemmel, azon belül elsősorban a nemzetbiztonsággal, hírszerzéssel, felderítéssel, katonai biztonsággal és a biztonságpolitikával kapcsolatos tudományos igényű kérdéseket feldolgozó és elemző írásokat – tanulmányokat, cikkeket és más témákat, anyagokat – jelentetünk meg;
- az írásmű legyen logikus, áttekinthető, tartalmilag összefüggő és jól tagolt – rendelkezzen bevezetés, tárgyalás és befejezés szövegrészekkel;

- a témával kapcsolatos saját koncepció megfogalmazása legyen érthető, a következtetések pedig megalapozottak, érvekkel, adatokkal alátámasztottak.

Formai követelmények:

- A szerzői kéziratok terjedelme lehetőleg ne haladja meg az egy szerzői ívet (40 000 karakter), azonban a kézirat tartalmát, témáját figyelembe véve egyedi (felelős kiadói) elbírálást követően nagyobb terjedelmű írások is megjelenhetnek.
- A kéziratot Calibri Light 12 pontos betűvel, másfeles sortávolsággal írva, a képeket és ábrákat feldolgozható (.jpg vagy .tif) formátumban a „szöveggel egy sorba” szerkesztve készüljön.
- A közleményhez rövid tartalmi összefoglalót (Absztrakt/Rezümé) kell mellékelni, maximum 10 –12 sorban, magyar és angol nyelven – a rövid tartalmi összefoglaló E/3 személyben íródjon és ne legyen megegyező a főszöveg bevezetőjével;
- a közleményhez három-öt kulcsszó megadása szükséges, magyar és angol nyelven;
- az írás angol nyelvű címét is kérjük megküldeni.
- A társadalomtudományokban a megszokott számozott hivatkozást az idézések lábjegyzetben módszerrel kérjük alkalmazni. (A folyóirat az MSZ ISO 690:2022 *„Információ és dokumentáció. Irányelvek az információforrások bibliográfiai hivatkozásaihoz és idézéseikhez”* és az MS ISO 832:1998 *„Információ és dokumentáció. Bibliográfiai leírás és hivatkozás. Bibliográfiai kifejezések rövidítésének szabályai”* szabványok az irányadók az alábbi leírásokban feltüntetett eltérésekkel. Abban az esetben, ha a szerző nem a szabványokat vagy a mellékelt segédletet alkalmazza, a szerző felkérhető a kézirat átdolgozására.)
- A négy számjegynél hosszabb számoknál a CTRL-SHIFT-SPACE (nem törő) szóközt alkalmazzuk, ne pedig a sima szóközt vagy a pontot; pl. 430 000. (A négyszámjegyű számoknál erre nincs szükség.)
- Az idézőjelek esetében a magyar változatot alkalmazzuk („...”), ne pedig az angol (“...”; ‘...’; ‘...!’) verziókat.
- Belső idézőjelet («...») használjunk az idézett szövegen belüli idézőjeles részhez – „Idézet eleje »belső idézet« idézet vége.”.
- Ha zárójeles részen (...) belül is szükségünk van záró-jelre, akkor a szögletes zárójelet [...] alkalmazzuk.
- Az idegen kifejezéseket, rövidítéseket magyarul és eredeti idegen nyelven kell az írásműben az első alkalommal feloldani lábjegyzetben (példa: WFP – World Food Program – ENSZ Világélelmészeti Programja).

Ábra, vázlat, térkép, diagram, egyéb melléklettel szembeni követelmények:

- A publikációkhoz tartozó, lényeges információkat tartalmazó ábrák, táblázatok, diagrammok, képek szerkesztése során szükséges azokat számozással – például 1. ábra –, címmel ellátni, továbbá lábjegyzetben megjelölni az illusztráció forrását vagy a saját szerkesztés tényét.

- Az ábrák és táblázatok megszerkesztése a szerző feladata, az illusztrációk a kéziratához minőségrontó formázás nélkül, beazonosítható módon elnevezve. Az ajánlott felbontás legalább 300 dpi legyen.
- Más kiadványból átvett ábra közlését a szerzőnek kell engedélyeztetnie, és saját szövegében a forrást is pontosan meg kell jelölnie.
- Az idegen nyelvű adatok magyarra fordítandók.
- Az információértékkel nem rendelkező, esetleg publikálásra alkalmatlan minőségű, illetve a bizonytalan forrású illusztrációk közlésétől a kiadó saját döntése alapján eltekinthet.

Idézetek, lábjegyzetelés során kérjük a következőket betartani:

- A szövegen belüli idézést követően felső indexként megadott sorszámok jegyzetekre utalnak, amelyeket a szövegbeli megjelenésük sorrendjében kell közölni. (Ezek a jegyzetek tartalmazhatják az idézéseket.)
- A lábjegyzetszám jellemzően a mondatrészt vagy mondatot záró írásjel mögé kerül.
 - A szövegrészhez közvetlen nem kapcsolódó, kiegészítő és magyarázó kiegészítéseket szintén lábjegyzetben kérjük feltüntetni.
 - Ha a szövegrészletben több műre kell hivatkozni, akkor csak egy felsőindex szám szerepeljen, és a lábjegyzetben szerepeljenek a művek pontosvevővel elválasztva.
 - Az első idézésnek tartalmazni kell legalább (ha rendelkezésre állnak): a szerző vezetéknevét – kiskapitális – keresztnévét: Cím. Kiadó, kiadás helye, kiadás éve úgy, ahogy azok a bibliográfiai hivatkozásokban meg vannak adva, továbbá az idézett rész oldalszáma. (Több szerző esetében hosszú kötőjel alkalmazásával kell elválasztani a szerzők nevét egymástól.)
 - Három vagy annál több szerző(k) esetén a lábjegyzetben az első szerző nevét követően az et al. rövidítést kell alkalmazni és a bibliográfiai jegyzékben kell kiírni az összes szerző nevét.
 - Az első idézést követően a további idézéseknek a következőket kell tartalmaznia: a szerző(k) vezetékneve – kiskapitális – kiadás éve, oldalszám. (Amennyiben a kéziratban található ugyanazon vezetéknevű és megjelenési évvel hivatkozott mű, úgy a keresztnév első betűjét is alkalmazni kell – pl. Szabó M. 2014, 9.)
 - Ha a szerző ismeretlen, úgy az Sz.n. rövidítést kell alkalmazni.
 - Ha a kiadás éve ismeretlen, úgy az „é.n” rövidítést kell alkalmazni.
 - Ha a kiadás helye ismeretlen, úgy a „h.n.” rövidítést kell alkalmazni.
 - Ha a kiadó ismeretlen, úgy a „k.n.” rövidítést kell alkalmazni.
 - Ha a hivatkozott mű a latin betűs nyelvtől eltérő nyelven jelent meg (pl. orosz vagy kínai), úgy a szerzőnek a hivatkozott művet latinbetűkre is át kell írni.
 - Az első idézést követő közvetlen ismételt idézés során az uo. rövidítést kell alkalmazni.

Bibliográfiai hivatkozások jegyzéke:

- A bibliográfiai hivatkozások jegyzékében a hivatkozásokat az első adatelem betűrendjében kérjük megadni.
- Amennyiben a hivatkozott mű rendelkezik ISBN számmal, azt a bibliográfiai adatok megadása után kérjük feltüntetni.
- Amennyiben a cikk rendelkezik ISSN vagy DOI-azonosítóval, azt kérjük a bibliográfiai adatok megadása után feltüntetni.

SZERKESZTŐBIZOTTSÁG

Az idézések fő fajtái:

HIVATKOZOTT MŰ TÍPUSA	SZÖVEGBELI ELSŐ HIVATKOZÁS	TOVÁBBI HIVATKOZÁS SZÖVEGBEN	IRODALOMEGYZÉKI HIVATKOZÁS
Egyszerűs mű	Ács Tibor: <i>A reformkor hadikultúrájáról.</i> Magyar Tudománytörténeti Intézet, Piliscsaba, 2005. 34. o.	Ács 2005, 34.	Ács Tibor: <i>A reformkor hadikultúrájáról.</i> Zrínyi Kiadó, Budapest, 2005. ISBN 963 9276 45 6
Két-, háromszerűs mű	SZENES Zoltán – SÍPOSNÉ Kecskeméthy Klára: <i>MATÓ 4.0 és Magyarország.</i> Zrínyi Kiadó, Budapest, 2019. 55. o.	SZENES – SÍPOSNÉ 2019, 55.	SZENES Zoltán – SÍPOSNÉ Kecskeméthy Klára: <i>MATÓ 4.0 és Magyarország.</i> Zrínyi Kiadó, Budapest, 2019. ISBN 978 963 327 770 6
Szerkesztett mű	BEREK Lajos: A hadtudományi kutatómunka alapjai. In: Szilágyi Tivadar (szerk.): <i>Szemelvények.</i> Zrínyi Miklós Katonai Akadémia, Budapest, 1994. 33. o.	BEREK 1994, 33.	BEREK Lajos: A hadtudományi kutatómunka alapjai. In: SZILÁGYI TIVADAR (szerk.): <i>Szemelvények.</i> Zrínyi Miklós Katonai Akadémia, Budapest, 1994. 31–50. o.

HIVATKOZOTT MŰ TÍPUSA	SZÖVEGBELI ELSŐ HIVATKOZÁS	TOVÁBBI HIVATKOZÁS SZÖVEGBEN	IRODALOMJEGYZÉKI HIVATKOZÁS TÍPUSA
Folyóirat (nyomtatott)	KOVÁCS Jenő: Az új magyar hadtudomány gyökerei, fejlődésének szemléleti problémái. <i>Új Honvédségi Szemle</i> , 1993/6., 6. o.	KOVÁCS 1993, 6.	KOVÁCS Jenő: Az új magyar hadtudomány gyökerei, fejlődésének szemléleti problémái. <i>Új Honvédségi Szemle</i> , 1993/6., 1-7. o. ISSN 1216-7436
Folyóirat (elektronikus)	FORGÁCS Balázs: A hadikultúra fogalmának histográfiája II. <i>Hadtudományi Szemle</i> , 2009/3., 4. o.	FORGÁCS 2009, 4.	FORGÁCS Balázs: A hadikultúra fogalmának histográfiája II. <i>Hadtudományi Szemle</i> , 2009/3., 1-8. o. Elérhető: https://epa.oszk.hu/02400/02463/00006/pdf/EPA02463_hadtudomanyi_szemle_2009_3_001-008.pdf (Letöltés ideje: 2024.08.09.)
Elektronikus tartalom	ABRAMS, Lawrence: Ransomware attack at German hospital leads to death of patient. Bleepingcomputer, 2020. szeptember 17.	ABRAMS 2020.	ABRAMS, Lawrence: Ransomware attack at German hospital leads to death of patient. Bleepingcomputer, 2020. szeptember 17. Elérhető: https://www.bleepingcomputer.com/news/security/ransomware-attacks-german-hospital-leads-to-death-of-patient/ (Letöltés ideje: 2024. 03.17.)
	Sz.n.: Operation Ghost Stories. fbi.gov, 2011. 10. 31.	Operation Ghost Stories 2011.	Sz.n.: Operation Ghost Stories. fbi.gov, 2011. 10. 31. Elérhető: https://www.fbi.gov/news/stories/operation-ghost-stories-inside-the-russian-spy-case (Letöltés ideje: 2024. 02. 20.)

HIVATKOZOTT MŰ TÍPUSA	SZÖVEGBELI ELSŐ HIVATKOZÁS	TOVÁBBI HIVATKOZÁS SZÖVEGBEN	RODALOMJEGYZÉKI HIVATKOZÁS
Doktori értekezések, diplomamunkák, szakdolgozatok	SOMKUTI Bálint: <i>A negyedik generációs hadviselés: az érdekvényszerítés új lehetőségei</i> . PhD-disszertáció. Nemzeti Köszölgélati Egyetem Hadtudományi Doktori Iskola, 2012. 95. o.	SOMKUTI 2012, 95.	SOMKUTI Bálint: <i>A negyedik generációs hadviselés: az érdekvényszerítés új lehetőségei</i> . PhD-disszertáció. Nemzeti Köszölgélati Egyetem Hadtudományi Doktori Iskola, 2012. DOI: 10.17625/NKE.2012.019
Konferencia	HOLCZINGER Norbert: Fenntartható fejlődés és finanszírozás. Előadás: <i>A fenntartható fejlődés a fejlesztéspolitikákban – 20 éves a magyar EU-tagság</i> . Nemzeti Köszölgélati Egyetem, Ludovika, Budapest, 2024. 04. 23.	HOLCZINGER 2024.	HOLCZINGER Norbert: Fenntartható fejlődés és finanszírozás. Előadás: <i>A fenntartható fejlődés a fejlesztéspolitikákban – 20 éves a magyar EU-tagság</i> . Nemzeti Köszölgélati Egyetem, Ludovika, Budapest, 2024. 04. 23. Elérhető: https://kfi.uni-nke.hu/hirek/2024/04/29/fenntarthato-fejlodes-a-fejlesztéspolitikakban (letöltés ideje: 2024. 07. 10.)

HIVATKOZOTT MŰ TÍPUSA	SZÖVEGBELI ELSŐ HIVATKOZÁS	TOVÁBBI HIVATKOZÁS SZÖVEGBEN	IRODALOMJEGYZÉKI HIVATKOZÁS TÍPUSA
Törvény	2013. évi V. törvény a Polgári Törvénykönyvről	Ptk. 183. § vagy Ptk. 183. § (1) bekezdés vagy Ptk. 183. § (1)-(3) bekezdés	2013. évi V. törvény a Polgári Törvénykönyvről
Rendelet	100/2009. (V. 8.) Korm. rendelet az árva mű egyes felhasználásainak engedélyezésére vonatkozó részletes szabályokról	100/2009. (V. 8.) Korm. rendelet	100/2009. (V. 8.) Korm. rendelet az árva mű egyes felhasználásainak engedélyezésére vonatkozó részletes szabályokról
Határozat	1100/1997. (IX. 30.) Korm. határozat szerzői jogszabályainak felülvizsgálatáról	1100/1997. (IX. 30.) Korm. határozat	1100/1997. (IX. 30.) Korm. határozat szerzői jogi jogszabályainak felülvizsgálatáról

