NEMZETBIZTONSÁGI SZEMLE

Kiemelt közlemények

13. évf. (2025)
2. szám

ISSN 2064-3756 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

Impresszum

Nemzetbiztonsági Szemle
A Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézetének elektronikus (online) megjelenésű tudományos folyóirata

HU ISSN 2064-3756 (elektronikus)

Szerkesztőség
Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet
Szerkesztő: Dr. Deák József
Szerkesztőségi titkár: Mezei József
Internetes elérhetőség: https://folyoirat.ludovika.hu/index.php/nbsz

Kiadó
Nemzeti Közszolgálati Egyetem | Ludovika Egyetemi Kiadó
Kapcsolat: www.ludovika.hu; kiadvanyok@uni-nke.hu
Székhely: 1083 Budapest, Ludovika tér 2.
A kiadásért felel: Dr. Deli Gergely rektor
Olvasószerkesztők: Farkas-Nagy Judit, Resofszki Ágnes
Tördelőszerkesztő: Kőrösi László

Tartalom

NEMZETBIZTONSÁGI SZEMLE
13. évfolyam (2025) 2. szám 3–17. | DOI: 10.32561/nsz.2025.2.1

Szabolcs Lóránt[1]

Public Intelligence in Public Diplomacy

U.S. Strategic Intelligence Sharing in the New Age of Great Power Competition

This paper examines the evolution of intelligence sharing as a tool of public diplomacy through analysis of two recent cases: the U.S. intelligence disclosures preceding Russia's 2022 invasion of Ukraine and the 2023 Chinese surveillance balloon incident. Drawing on declassified documents and contemporary reporting, the article demonstrates how intelligence sharing has transformed from a purely operational tool into a sophisticated instrument of public diplomacy. The paper reveals distinct approaches to intelligence disclosure: systematic pre-emptive sharing in Ukraine versus rapid crisis response during the balloon incident. Both cases, however, demonstrate the U.S. Intelligence Community's growing sophistication in balancing operational security with strategic communication needs. Through comparative analysis, the article identifies key patterns in how intelligence sharing can shape international narratives, build coalition support, and counter adversary messaging while maintaining credibility and protecting sources. This evolution in intelligence sharing practices, formalised in U.S. Intelligence Community Directive 405, represents a significant development in how intelligence services engage with both foreign governments and public audiences in an era of digital information warfare and great power competition.

Keywords: *intelligence sharing, public diplomacy, intelligence diplomacy, strategic communication, narrative control*

Introduction

The strategic use of intelligence in international relations has evolved dramatically in recent years, particularly in its relationship with public diplomacy – the practice of openly conducting diplomatic efforts to influence foreign public opinion.[2] Intelligence can serve

[1] PhD candidate, Ludovika University of Public Service, Doctoral School of Military Sciences, e-mail: lorant.szabolcs@stud.uni-nke.hu

[2] See "public diplomacy, n." Oxford English Dictionary Online.

as a powerful tool for public diplomacy, providing governments with evidence-based legitimacy for their decisions rather than relying on ideology or instinct.[3]

This evolution is particularly evident in today's rapidly changing intelligence landscape, where the fusion of technological capabilities with strategic communication has become increasingly crucial. As Anne Neuberger, former NSA Chief Risk Officer, argues, while AI and technological advancement are revolutionising intelligence capabilities – from rapid translation to pattern recognition – the art of intelligence remains deeply human.[4]

Israel's recent Hezbollah pager operation illustrates this duality perfectly. While the technical sophistication of creating untraceable booby-trapped devices was remarkable, the true intelligence mastery lay in the decade-long deception operation, involving elaborate front companies, strategic timing of the attack, and carefully orchestrated information release. As one Mossad agent described it to CBS News: "We create a pretend world [...] we write the screenplay, we're the directors, we're the producers, we're the main actors, and the world is our stage."[5]

The strategic use of intelligence in the public domain – what we might call "public intelligence diplomacy" – has become a sophisticated tool of statecraft. The U.S. Intelligence Community, in its directive ICD 405, defines intelligence diplomacy (ID) as follows: "ID is the sharing of intelligence [...] either directly with a foreign government or, where appropriate, publicly, to encourage engagement, collaboration, or collective action among foreign governments." The ICD clearly distinguishes between the different layers of activities:

> "An ID effort must satisfy three criteria: First, it has to involve the sharing of objective intelligence, either publicly or directly to a foreign government; this by itself is 'intelligence sharing'. Second, it has to have the goal of exchanging perspectives with a foreign government on a specific threat or issue; this by itself is 'intelligence engagement'. Third, it has to be done in support of advancing a preferred policy objective which may lead to unilateral, joint or multilateral action. The third criterion is what separates intelligence sharing and engagement from ID."[6]

Through selective disclosure of intelligence information, nations can shape international narratives, influence foreign audience perceptions, build coalition support, and counter adversary messaging. This strategic deployment of intelligence serves multiple purposes: from warning allies of imminent threats to exposing adversary operations, from building international consensus to undermining hostile disinformation campaigns.

In this evolving context, today's intelligence landscape is not just about who has the most advanced AI models or the best satellite imagery. It is about how nations strategically leverage their intelligence capabilities – both technological and human – to advance their geopolitical interests in an increasingly complex world.

This conceptual framework helps explain why intelligence sharing can be particularly effective in diplomatic engagement, as the disclosure of intelligence carries unique weight in international discourse.

---

3 Pinkus 2014: 33.
4 Neuberger 2025.
5 Berg 2024.
6 Intelligence Community 2025.

This article employs a comparative case study approach, focusing on two recent events: the pre-invasion intelligence sharing campaign regarding Ukraine (2021–2022) and the Chinese surveillance balloon incident (2023). Primary sources include official statements, intelligence releases, media reporting, supplemented by academic analysis of intelligence sharing practices. The use of these sources contributes to our understanding of how intelligence sharing practices differ across contexts and their diplomatic impact. This examination reveals not only the tactical variations in intelligence sharing approaches but also broader strategic implications for public diplomacy in an era of digital information warfare.

Theoretical framework: evolving understanding of intelligence diplomacy

The concept of intelligence diplomacy has undergone significant evolution, particularly in recent years. While existing literature predominantly focuses on intergovernmental aspects of intelligence diplomacy, recent policy developments suggest a broader conceptual framework that includes public engagement and strategic communication.

Traditional scholarly understanding of intelligence diplomacy emphasises intelligence chiefs "coming out of the shadows" to engage in direct diplomatic interactions with foreign counterparts.[7] This classical interpretation primarily concerns government-to-government relations, in line with the scope of the US ICD 403 (2013) directive and its definition of foreign entities as "foreign governments or components thereof; international organizations or coalitions consisting of sovereign states".[8]

The introduction of ICD 405 marks a significant development in intelligence sharing practices in the United States. Pinkus has already identified the concept of "public use of intelligence" (citing Hastedt), which he interpreted as "using intelligence for public diplomacy".[9]

Building on this foundation, this article proposes the term "public intelligence diplomacy" to specifically describe the comprehensive framework formalised by ICD 405, where intelligence sharing becomes an active diplomatic tool aimed at fostering international engagement and collective action. This conceptual distinction helps differentiate between tactical use of intelligence for domestic audiences, as exemplified in the Iraq War case,[10] and the strategic deployment of intelligence as a diplomatic tool for international engagement. The ICD 405 directive explicitly codifies this practice at the policy level, extending beyond both traditional intergovernmental frameworks and tactical domestic communication.

This evolution in intelligence sharing practices represents a significant departure from traditional approaches. As Gioe (2025) highlights, intelligence cooperation has historically operated through what practitioners term "liaison" – deliberately hidden channels meant to remain unaffected by international politics and shifts in foreign policy.

7 Taylor 2023.
8 Intelligence Community 2013.
9 Pinkus 2014: 36.
10 Hastedt 2013: 26.

These traditional liaison relationships focused exclusively on secret government-to-government exchanges, with intelligence services carefully maintaining separation from public diplomatic channels.[11]

The emergence of public intelligence diplomacy, therefore, marks a fundamental shift in how intelligence services engage with both foreign governments and public audiences. This transformation aligns with broader changes in diplomatic practice and information sharing in the digital age, while presenting new challenges in balancing transparency with operational security.

The distinction between classical intelligence diplomacy and this emerging strategic approach represents a crucial theoretical development. While the former focuses on covert or semi-covert diplomatic channels between intelligence services, the latter encompasses strategic public communication of intelligence to achieve broader diplomatic objectives through both direct and public channels. Unlike tactical intelligence sharing for domestic audiences, this approach explicitly seeks to "encourage engagement, collaboration, or collective action among foreign governments" while maintaining "analytical integrity, objectivity and rigor in accordance with ICD 203".[12]

This evolution aligns with what observers[13] highlight about intelligence services chiefs increasingly taking active roles in diplomatic processes and foreign policy formation, with intelligence diplomacy complementing conventional diplomacy while maintaining strategic intelligence's crucial role in foreign policy decisions.

This theoretical framework helps illuminate the practical challenges of intelligence disclosure. Intelligence sharing in diplomatic contexts operates within what Carnegie and Carson[14] describe as the "disclosure dilemma" – balancing the potential diplomatic benefits of wide dissemination against operational risks and source protection. This dilemma shaped both the proactive Ukraine disclosures and reactive balloon incident response, though with different risk calculations and strategic objectives.

Strategic information environment

The strategic use of intelligence sharing as a diplomatic tool must be understood within the context of fundamental changes in the global information environment. As Leonardson's review of Rid's work highlights, modern information warfare builds on decades of evolution in influence operations, where success relied on mixing verifiable facts with carefully crafted falsehoods. Digital platforms have dramatically accelerated this dynamic – what historically took months to spread now moves from fringe to mainstream media within hours.[15]

11 Gioe 2025.

12 Intelligence Community 2025. Note: The mentioning of ICD 203 is particularly relevant here because: It addresses potential criticism that public intelligence sharing might compromise intelligence integrity for diplomatic gains; ICD 203 specifically requires intelligence analysis to be objective and unbiased, so mentioning it shows that public intelligence diplomacy must still adhere to core intelligence principles; It distinguishes this approach from past problematic uses of intelligence for public diplomacy (like the Iraq War case) where intelligence was potentially politicised.

13 Marinho et al. 2024.

14 Cited in Brattvoll 2024.

15 Leonardson 2020.

In the context of what Valle de Frutos identifies as the "unprecedented challenges of hyperconnectivity generated by digital globalization",[16] intelligence sharing has emerged as a strategic response to establish authoritative narratives. As Rid argues, discussed in Leonardson (2020), mainstream media's vulnerability to manipulation through accelerated news cycles has made traditional counter-disinformation approaches insufficient.

This transformation is particularly evident in U.S. approaches to great power competition, where intelligence sharing has evolved from a primarily secret, state-to-state activity to a public diplomatic instrument. Leonardson's (2020) analysis of Rid's work emphasises how the rise of "amateur surrogates" in information operations – such as social media trolls rather than trained intelligence officers – has necessitated new approaches to maintaining narrative credibility in an environment characterised by systematic manipulation through social networks and artificial intelligence.

This evolution reflects what Brattvoll terms the "capital of the secret" – the special social and political status[17] accorded to classified information, "as it is perceived to be more valuable than other forms of information".[18]

Within this transformed information environment, states must balance the diplomatic advantages of intelligence disclosure against operational security concerns, particularly when countering systematic disinformation campaigns.

The evolution of intelligence sharing frameworks

Since 9/11, the U.S. intelligence community[19] has worked to resolve what the Congressional Research Service identified as a fundamental paradox: intelligence is valuable only when shared with those who need it, but wider sharing increases risks of compromise.[20] This tension directly relates to the frameworks established by ICD 403 and 405, which attempt to balance these competing imperatives.

The initial response focused on removing barriers between intelligence and law enforcement agencies, but this soon expanded into a broader reconsideration of how intelligence could be shared more effectively while maintaining security.

Intelligence Community Directive 403 (2013) and its associated guidance, particularly ICPG 403.3 (2014), emerged from this effort to create structured frameworks for intelligence sharing. These directives established clear procedures for both routine and emergency disclosures of intelligence.

This institutional evolution proved crucial in December 2021, when the United States launched what observers called an "unprecedented" campaign of intelligence sharing about

16 Valle de Frutos 2024.

17 Note: As ICD 403 highlights "U.S. intelligence is a national asset to be conserved and protected and will be shared with foreign entities only when consistent with U.S. national security and foreign policy objectives and when an identifiable benefit can be expected to accrue to the U.S." Intelligence Community 2013.

18 Brattvoll 2024.

19 The U.S. Intelligence Community consists of 18 organisations: two independent agencies (ODNI and CIA), nine Department of Defense elements (including DIA, NSA, NGA, NRO, and the intelligence elements of the five military services), and seven elements within other federal departments (Energy, Homeland Security, Justice, State, and Treasury).

20 Best 2011.

Russia's planned invasion of Ukraine.[21] The campaign operated within frameworks carefully developed to balance operational security with strategic communication needs. ICD 403 established baseline requirements for protecting sources and methods, while ICPG 403.3 specifically authorised rapid intelligence sharing when necessary to prevent imminent threats or protect critical operations.

The continuing evolution of intelligence sharing frameworks is evident in the recent ICD 405 (2025), which further formalises intelligence diplomacy practices and provides updated guidance on using intelligence disclosure to advance U.S. foreign policy objectives. This directive represents the Intelligence Community's ongoing efforts to adapt its policies to meet emerging strategic communication needs while maintaining essential security protocols.

The CRS 2011 report's discussion of the shift from a strict "need-to-know" to a more flexible "need-to-share" paradigm after 9/11 helps explain the institutional context in which the 2021–2022 Ukraine disclosures occurred.

Intelligence sharing in practice

The 2022 Threat Assessment

The 2022 Annual Threat Assessment, published in February 2022, provides crucial insight into how the Intelligence Community viewed evolving information warfare dynamics on the eve of Russia's invasion. The assessment acknowledged Russia's aggressive posture, noting that "Russia is pushing back against Washington where it can – locally and globally – employing techniques up to and including the use of force".[22]

The assessment was particularly prescient regarding Ukraine, stating that "Russia continues to prepare for a military attack against Ukraine, with well over 100,000 troops massed near the Ukraine border, including Russian military forces in Belarus, occupied-Crimea, and the separatist forces in Eastern Ukraine. Moscow is sending more forces."[23] This clear identification of Russian preparations provided the foundation for subsequent intelligence disclosures.

The 2022 Annual Threat Assessment was particularly significant in its characterisation of Russia's influence operations. The document identified Russia as "one of the most serious foreign influence threats to the United States", noting Moscow's use of "intelligence services, proxies, and wide-ranging influence tools" to divide Western alliances and undermine U.S. global standing. Crucially, the assessment highlighted Russia's adaptability, observing that Russian influence actors were "adept at capitalizing on current events in the United States to push Moscow-friendly positions to Western audiences".[24]

This understanding of Russia's sophisticated influence capabilities provided important context for the Intelligence Community's subsequent approach to Ukraine. By recognising Moscow's established pattern of using multiple channels to shape international narratives,

[21] Brattvoll 2024.
[22] ODNI 2022: 4.
[23] ODNI 2022: 10.
[24] ODNI 2022: 12.

the U.S. Intelligence Community could anticipate and pre-empt Russian disinformation about Ukraine through its unprecedented disclosure campaign. The assessment's emphasis on how Russia would "seek out new methods of circumventing technology companies' anti-disinformation activities to further expand its narratives globally"[25] helps explain why traditional counter-disinformation approaches alone were deemed insufficient.

The U.S. intelligence sharing campaign in Ukraine

The intelligence sharing campaign preceding Russia's invasion of Ukraine represents a watershed moment in the strategic use of intelligence for diplomatic purposes. As Dylan and Maguire (2022) document, this carefully orchestrated campaign marked a significant evolution in how intelligence can be deployed to shape international responses to emerging security threats. Through systematic disclosure of Russian military preparations and intentions from November 2021 through February 2022, the U.S. and its allies demonstrated how intelligence sharing could serve multiple diplomatic objectives simultaneously: building coalition consensus, establishing narrative control, and attempting strategic deterrence.

The campaign's sophistication is evident in its carefully calibrated approach to timing, content, and audience targeting. By gradually escalating the specificity and scope of intelligence disclosures – from early warnings to detailed assessments of military capabilities and ultimately to specific predictions of invasion timing – the U.S. established a pattern of credible intelligence that helped overcome initial scepticism among European allies. However, this unprecedented level of intelligence sharing also highlighted persistent challenges in balancing operational security with diplomatic effectiveness, particularly given the legacy of previous intelligence controversies.

This evolution in intelligence sharing strategy is particularly evident when examining the specific characteristics and implementation of the Ukraine campaign. The Ukraine case demonstrates a shift from reactive to proactive intelligence sharing. Unlike previous instances of public intelligence sharing, such as Colin Powell's widely discredited 2003 UN presentation on Iraq,[26] where Washington pre-emptively shared intelligence to justify military action, the Ukraine campaign emphasised pre-emptive disclosure to prevent and deter aggression and this way shape diplomatic outcomes.

As Dylan and Maguire note, this approach allowed Western allies to "pre-bunk" Russian disinformation rather than merely respond to it. This strategic shift reflects broader changes in the information environment, where rapid disclosure can help establish narrative dominance. This was not revolutionary but rather evolutionary, building on previous experiences from the Cuban Missile Crisis through to recent cyber threat disclosures. However, the scope, vigour, and frequency of intelligence dissemination, particularly between mid-January and mid-February 2022, marked a novel development in modern international statecraft.[27]

[25] ODNI 2022: 12.
[26] Borger 2021.
[27] Dylan–Maguire 2022.

Some of the key elements characterised this novel approach: the use of high-level, highly sanitised intelligence-led communications[28] deployed through accessible formats, in the press,[29] as well as in social media, the unprecedented use of formal intelligence assessment language in public communications (e.g. "we judge it to be highly likely"), which was previously unusual in public discourse, and the coordination between intelligence and policy communities to manage both the message and the risks.

Coalition management challenges

The campaign revealed both opportunities and limitations in using intelligence for coalition building. While U.S. (and U.K.) intelligence sharing helped shift European positions, particularly in Germany, it also exposed tensions in how different allies assess and use intelligence. The French intelligence community's scepticism of Anglo-American assessments, reminiscent of debates before the Iraq War, highlights how different strategic cultures and intelligence traditions can complicate coalition building through intelligence sharing. This divide was particularly stark between East-Central European nations – for example while Hungary maintained its diplomatic presence and unchanged travel recommendations despite U.S. warnings,[30] Baltic security analysts were sounding the alarm bell warning of an imminent invasion.[31]

Strategic framework and implementation

The U.S.-led intelligence sharing campaign during the Ukraine crisis demonstrates a sophisticated understanding of intelligence's dual role – as both an information source and an instrument of diplomatic influence. As Brattvoll (2024) argues, intelligence disclosure gains particular potency through what he terms the "capital of the secret" – the special social status accorded to classified information that makes its disclosure an especially powerful diplomatic tool. The deliberate disclosure of intelligence served multiple purposes: pre-empting adversary narratives – to let "people around the world [...] see it [the Russian invasion] for what it was"[32] –, building coalition consensus, and demonstrating diplomatic resolve. This represents a departure from traditional intelligence practices where secrecy was paramount.

[28] Note: "intelligence-led communication" refers to intelligence information that was carefully screened to remove/protect sources and methods, sensitive technical capabilities, classified operational details, reformatted for public consumption – simplified technical language, removed intelligence jargon, structured for clear public messaging. Example from Riehle (2024): In the Ukraine case, intelligence about Russian military movements was shared publicly but with technical collection methods and specific sources removed while maintaining the core assessment. The "led" component in the term indicates that while derived from intelligence, the final communication is shaped for diplomatic messaging rather than pure intelligence reporting.

[29] Harris–Sonne 2021.

[30] Hungary Today 2022.

[31] Thomas 2022.

[32] Shapiro 2024.

The campaign's evolution also reflects what Brattvoll (2024) identifies as a crucial shift in strategic objectives: while initially aimed at deterring Russian aggression, intelligence sharing ultimately proved more effective in unifying NATO allies and establishing narrative control. This transformation occurred within what he terms the "disclosure dilemma", where states must balance the potential diplomatic benefits of intelligence sharing against operational risks and source protection concerns.

Risk management

Dylan and Maguire identify three primary categories of risk in public intelligence sharing:

- Adaptation costs: the risk that adversaries will change behaviour or improve their security measures in response to disclosures
- Escalation costs: the potential for public disclosures to limit diplomatic flexibility and force escalatory responses
- Audience costs: the challenge of maintaining credibility when intelligence assessments cannot be fully supported with public evidence

The U.S. approach in Ukraine has shown sophisticated handling of these risks through graduated disclosure and careful institutional coordination.

However, this approach has not been without its critics. As experts note, CIA veterans warned that extensive disclosure could enable adversaries to plant misleading intelligence, arguing "our side has said too much".[33]

Operational effectiveness

The Ukraine crisis marked what Brattvoll (2024) documents as an "unprecedented scale" of intelligence disclosure, with U.S. (as well as U.K.) intelligence services making systematic pre-emptive releases rather than reactive disclosures. As Brattvoll, Dylan and Maguire's work documents, while initial disclosures aimed to deter Russian aggression, they ultimately proved more effective in achieving what he terms "narrative superiority" among NATO allies. This shift from deterrence to coalition building represents a significant development in how intelligence serves diplomatic objectives.

The effectiveness of these disclosures seemed to be amplified by weaknesses in Russian covert actions. Despite Russia's attempts to maintain plausible deniability, their actions were unveiled due to what Riehle sees as a combination of "ignorance, indifference, and incompetence". Russian operations appeared to display ignorance of likely Western reactions, indifference to international opinion, and operational incompetence that made their activities easier to expose. This pattern of behaviour, Riehle argues, ultimately limited Russia's diplomatic and strategic options while strengthening the credibility of Western intelligence disclosures.[34]

[33] Dylan–Maguire 2022.
[34] Riehle 2024.

In brief, the effectiveness of intelligence sharing as a diplomatic tool ultimately depends on maintaining credibility while achieving strategic objectives. The Ukraine case demonstrates how this balance could be achieved through careful institutional management and strategic consideration of risks and benefits. As this practice continues to evolve, the integration of intelligence sharing into broader diplomatic strategy will likely become more sophisticated and nuanced.

The Chinese balloon incident

The "spy balloon episode" of 2023 represents a significant case study in modern intelligence disclosure and public diplomacy.

It emerged against a backdrop of growing U.S. awareness of Chinese intelligence collection capabilities. A declassified National Intelligence Estimate from April 2021 had already identified China's focus on developing "new sophisticated technologies and techniques to collect intelligence from space", establishing important context for understanding the subsequent balloon crisis.[35]

On 1 February 2023, residents in Montana spotted an unexpected white object hovering above them, initiating what would become a complex international diplomatic crisis. The U.S. Department of Defense quickly identified it as a high-altitude surveillance balloon from China, while Chinese authorities maintained it was a civilian weather research vessel that had strayed off course.[36]

The incident highlighted fundamental differences in U.S. and Chinese approaches to strategic communication and public opinion management. As Zhang et al. document, CNN characterised the event as "a watershed moment in the world's dangerous new superpower rivalry", while Chinese media viewed U.S. reactions as "too dramatic" and emphasised international legal frameworks. The technical and legal aspects became central to narrative construction: both sides leveraged Article 8 of the Chicago Convention, which specifies requirements for unmanned aircraft. This ambiguity allowed China to emphasise the "balloon" designation to stress its unmanned, uncontrollable nature, while U.S. military sought evidence from debris to refute this characterisation. Public opinion analysis reveals distinct cognitive differences between Chinese and American audiences. Zhang et al. found marked variation in how media coverage framed the incident – U.S. media emphasised surveillance and security threats, while Chinese coverage focused on legal frameworks and proportionality of response.[37]

The incident's significance lies in how it demonstrates the evolution of intelligence disclosure as a public diplomacy tool. The situation presented a unique opportunity for the parties involved to "leverage murky events to justify their behaviours, rally political support, and promote favourable worldviews". The absence of immediately verifiable facts created what Wong and Mulupi term "raw material" for narrative construction, that is to "construct issue narratives that engaged identity and system narratives".[38]

[35] ODNI 2021.
[36] Wong–Mulupi 2024.
[37] Zhang et al. 2024.
[38] Wong–Mulupi 2024: 1, 4.

The U.S. response demonstrated sophisticated understanding of narrative control in modern information environments. Their immediate characterisation of the object as a "surveillance balloon" achieved remarkable penetration in global discourse. Quantitative analysis shows this framing dominated international coverage, with "almost all of the U.S. (99.39%) and international (93.88%) samples, and more than four-fifths of the Chinese news articles circulating this narrative".[39] This success in narrative establishment forced China into a reactive position, struggling to promote its alternative interpretation of events.

The technical intelligence disclosure strategy employed by the U.S. proved effective. The balloon was "flying as high as 60,000 feet above ground, which puts it at about ten times closer than the lowest Earth-orbiting satellites".[40] This technical detail, combined with information about the balloon's path over sensitive military installations, helped the U.S. establish its surveillance narrative. As Wong and Mulupi document, this allowed the U.S. to reinforce the "king of spying" narrative of China. The incident revealed sophisticated layering of narrative elements. Beyond immediate crisis management, the U.S. successfully connected the balloon incident to broader strategic narratives about Chinese surveillance activities. As Wong and Mulupi observe, this allowed the U.S. to reinforce the narrative of "the identity of China as a surveillance state". This expansion from tactical to strategic messaging demonstrates evolution in U.S. intelligence disclosure practices.[41]

China's counter-narrative efforts, while substantial, struggled to gain international traction. Their alternative framing of the balloon as a civilian weather research vessel affected by "force majeure" found limited resonance in international media. Wong and Mulupi (2024) document that while this narrative achieved 71.11% coverage in Chinese media, it failed to effectively challenge the dominant U.S. interpretation in global discourse.

The incident's aftermath revealed the lasting impact of initial narrative establishment. Even as China attempted to shift discussion toward accusations of U.S. overreaction and violation of international norms, the fundamental U.S. characterisation of the event as a surveillance incident remained dominant. Wong and Mulupi[42] argue that this demonstrates how "the framing in the initial issue narrative could be crucial in the following narrative contest that expands to the identity and system levels".

The evolution of intelligence disclosure in public diplomacy: a comparative analysis

This section represents an analytical synthesis of the cases previously discussed in detail.

The Ukraine and Chinese balloon cases demonstrate distinct yet complementary approaches to intelligence disclosure in modern diplomatic practice. While fundamentally different in their circumstances and execution, these cases jointly illuminate the sophisticated development of U.S. intelligence disclosure strategy in contemporary diplomatic contexts. As Wong, Mulupi (2024) and Brattvoll (2024) demonstrate, both cases show how intelligence

[39] Wong–Mulupi 2024: 10.
[40] Ng–Carley 2023.
[41] Wong–Mulupi 2024: 15.
[42] Wong–Mulupi 2024: 16.

disclosures can shape international narratives, though through markedly different approaches and under varying pressures.

The fundamental distinction lies in the approach to intelligence disclosure in each case. The Ukraine disclosures represented systematic pre-emptive disclosure, where intelligence releases were carefully planned and sequenced to achieve specific diplomatic objectives. In contrast, the balloon incident required rapid response under crisis conditions, demonstrating a different aspect of intelligence sharing as a diplomatic tool.

The timing dimension reveals crucial differences in operational approach while highlighting similar strategic principles. In the Ukraine case, the United States could carefully select and prepare intelligence for release, timing disclosures for maximum diplomatic impact. The balloon incident, however, demanded immediate response. The United States demonstrated remarkable agility in establishing narrative control, achieving dominant global narrative power even under time pressure.

Both cases required sophisticated management of what Dylan and Maguire (2022) identifies as the three primary risks in intelligence disclosure: adaptation costs, escalation costs, and audience costs. The Ukraine disclosures demonstrated careful calibration of these risks through graduated release of intelligence, while the balloon incident required rapid risk assessment under crisis conditions. The contrasting approaches to intelligence sharing in the Ukraine and balloon cases reflect what Brattvoll (2024) identifies as a fundamental tension in modern intelligence diplomacy: the balance between strategic effectiveness and the protection of intelligence sources, methods, and capabilities.

The technical nature of intelligence disclosure also evolved between the cases. In Ukraine, the systematic release focused on Russian military capabilities and intentions, requiring careful calibration of what technical intelligence could be shared while protecting sources and methods. The balloon incident, conversely, required careful balance in technical disclosure – revealing enough about surveillance capabilities to support the narrative while maintaining strategic ambiguity about U.S. counter-surveillance capabilities.

Audience targeting strategies differed significantly between the cases. Ukraine disclosures operated on multiple levels: building international coalition support, shaping global public opinion, and attempting to influence Russian decision-making. This multi-tiered approach required careful calibration of intelligence sharing to address diverse audience needs simultaneously. The balloon incident, however, focused primarily on managing bilateral tensions with China while maintaining broader international credibility about U.S. capabilities and intentions.

Together, these cases demonstrate how intelligence sharing has evolved from a purely operational tool to a sophisticated instrument of public diplomacy, capable of serving different strategic objectives under both planned and crisis conditions.

Conclusions and future implications

Drawing together the threads of our analysis, these cases represent more than isolated incidents of intelligence sharing – they signal a fundamental shift in how the United States deploys intelligence as an instrument of public diplomacy in what Valle de Frutos (2024) identifies as an era of digital geopolitical globalisation. This evolution reflects both

technological changes and the increasing importance of information warfare in great power competition.

The success of these intelligence disclosure campaigns suggests several implications for future U.S. public diplomacy practice. First, selective intelligence sharing has proven to be a powerful tool for shaping international narratives when deployed with precision and credibility. The Ukraine case particularly demonstrates how early, accurate intelligence disclosures can help build international coalitions and pre-empt adversary messaging, while the balloon incident shows how rapidly shared intelligence can effectively manage crisis situations and maintain narrative control even under time pressure.

Second, these cases indicate that traditional concerns about protecting sources and methods must be balanced against the strategic benefits of public disclosure. The U.S. Intelligence Community's ability to navigate this balance – revealing enough to achieve diplomatic objectives while protecting critical capabilities – will likely become increasingly important in future scenarios.

The cases presented in this paper demonstrated the diplomatic potential of intelligence sharing. Brattvoll (2024), however, argues that such extensive disclosures are unlikely to become the norm, given the persistent operational risks and institutional constraints. The challenge for the future practice of public intelligence diplomacy lies in maintaining the diplomatic leverage gained through the "capital of secrecy" while protecting intelligence capabilities and sources.

Looking ahead, this merger of intelligence sharing and public diplomacy may become a standard feature of U.S. strategic communication, particularly in confronting challenges from peer competitors. However, its effectiveness will continue to depend on maintaining the credibility established through accurate disclosures in these precedent-setting cases.

References

Berg, Raffi (2024): Ex-Israeli Agents Reveal How Hezbollah Pager Attacks were Carried Out. *BBC,* 23 December 2024. Online: https://www.bbc.com/news/articles/cwy3l02wxqdo

Best, R. A. (2011): *Intelligence Information: Need-to-Know vs. Need-to-Share.* Congressional Research Service Report. Online: https://www.everycrsreport.com/reports/R41848.html

Borger, Julian (2021): Colin Powell's UN Speech: A Decisive Moment in Undermining US Credibility. *The Guardian,* 18 October 2021. Online: https://www.theguardian.com/us-news/2021/oct/18/colin-powell-un-security-council-iraq

Brattvoll, Joakim (2024): Intelligence Disclosure as a Strategic Messaging Tool. *NATO Review,* 16 December 2024. Online: https://www.nato.int/docu/review/articles/2024/12/16/intelligence-disclosure-as-a-strategic-messaging-tool/index.html

Dylan, Huw – Maguire, Thomas J. (2022): Secret Intelligence and Public Diplomacy in the Ukraine War. *Survival,* 64(4), 33–74. Online: https://doi.org/10.1080/00396338.2022.2103257

Gioe, David V. (2025): How America's Allies Boost U.S. Intelligence. *Foreign Affairs,* 13 February 2025. Online: https://www.foreignaffairs.com/united-states/how-americas-allies-boost-us-intelligence

Harris, Shane – Sonne, Paul (2021): Russia Planning Massive Military Offensive against Ukraine Involving 175,000 Troops, U.S. Intelligence Warns. *The Washington Post,* 4 December 2021. Online: https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html

Hastedt, Glenn (2013): The Politics of Intelligence and the Politicization of Intelligence: The American Experience. *Intelligence and National Security,* 28(1), 5–31. Online: https://doi.org/10.1080/02684527.2012.749062

Hungary Today (2022): Ukraine Crisis: Hungarian Foreign Ministry Will Not Evacuate Employees. *Hungary Today,* 24 January 2022. Online: https://hungarytoday.hu/ukraine-crisis-evacuation-nato-hungary-russia-orban-biden-putin/

Intelligence Community (2013): ICD Directive 403. *Office of the Director of National Intelligence,* 13 March 2013. Online: https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives

Intelligence Community (2025): ICD Directive 405. *Office of the Director of National Intelligence,* 14 January 2025. https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives

Leonardson, J. E. (2020): Review of Active Measures: The Secret History of Disinformation and Political Warfare. *Studies in Intelligence,* 64(1).

Marinho, Jorge – Ventura, Júlio – Ribeiro, Lourenço (2024): Strategic Intelligence and Intelligence Diplomacy in the Sphere of Foreign Policy – Diplomat magazine, 2 June 2024. Online: https://diplomatmagazine.eu/2024/06/02/strategic-intelligence-and-intelligence-diplomacy-in-the-sphere-of-foreign-policy/

Neuberger, Anne (2025): Spy vs. AI. *Foreign Affairs,* 15 January 2025. Online: https://www.foreignaffairs.com/united-states/spy-vs-ai

Ng, Lynnette H. X. – Carley, Kathleen M. (2023): Deflating the Chinese Balloon: Types of Twitter Bots in US-China Balloon Incident. *EPJ Data Science,* 12(1), Article 1. Online: https://doi.org/10.1140/epjds/s13688-023-00440-3

ODNI (2021): *Chinese Space Activities Will Increasingly Challenge US Interests Through 2030.* April 2021. Online: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/3645-chinese-space-activities-will-increasingly-challenge-u-s-interests-through-2030

ODNI (2022): *Annual Threat Assessment of the U.S. Intelligence Community.* February 2022. Online: https://www.odni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

Pinkus, Jonathan (2014): Intelligence and Public Diplomacy: The Changing Tide. *Journal of Strategic Security,* 7(1), 33–46. Online: https://doi.org/10.5038/1944-0472.7.1.3

Riehle, Kevin P. (2024): Ignorance, Indifference, or Incompetence: Why are Russian Covert Actions so Easily Unmasked? *Intelligence and National Security,* 39(5), 864–878. Online: https://doi.org/10.1080/02684527.2023.2300165

Shapiro, Jeremy (2024): Letter from Washington: All-Knowing America and US Intelligence Diplomacy. *ECFR,* 18 April. Online: https://ecfr.eu/article/letter-from-washington-all-knowing-america-and-us-intelligence-diplomacy/

Taylor, Chris (2023): *'Doing Good Deeds Quietly': The Rise of Intelligence Diplomacy as a Potent Tool of Statecraft.* Australian Strategy Policy Institute Strategic Insights. Online: https://www.jstor.org/stable/resrep53516

Thomas, Matthew (2022): Major Russian Invasion of Ukraine Imminent. *Baltic Security Foundation,* 21 January 2022. Online: https://balticsecurity.eu/major_russian_invasion_of_ukraine_imminent

Valle de Frutos, S. (2024): La opinión pública internacional en el contexto de la geopolítica de la globalización desinformativa. Análisis desde la teoría de la complejidad y de la baja racionalidad. *Relaciones Internacionales,* (56), 75–93. Online: https://doi.org/10.15366/relacionesinternacionales2024.56.004

Wong, Frankie H. C. – Mulupi, Dinfin (2024): Up in the Air: A Strategic Narrative Contest in the U.S.–China Balloon Incident 2023. *International Communication Gazette,* 0(0). Online: https://doi.org/10.1177/17480485241290361

Zhang, Baoyu – Chen, Tao – Li, Qiang – Zhang, Weishan – Wang, Fei-Yue (2024): Spy Balloon or Sputnik Moment: A Comparative Analysis of Public Opinion in China and the United States. *IEEE Transactions on Computational Social Systems,* 11(3), 3729–3740. Online: https://doi.org/10.1109/TCSS.2023.3333954

NEMZETBIZTONSÁGI SZEMLE
13. évfolyam (2025) 2. szám 18–33. | DOI: 10.32561/nsz.2025.2.2

Szabó Lajos[1]

Az ukrán szélsőséges nacionalista szervezetek és pártok félkatonai alakulatainak alkalmazása a 2014-es kelet-ukrajnai harcokban

Deployment of Paramilitary Formations of Ukrainian Extremist Nationalist Organisations and Parties in the Fighting in Eastern Ukraine in 2014

A szélsőséges ukrán nacionalista pártok Ukrajna függetlenné válását követően megjelentek az országos politikában, de csak Nyugat-Ukrajnában rendelkeztek jelentős támogatottsággal és az ukrán parlamenti, illetve elnökválasztásokon sohasem értek el jelentős politikai eredményt. A 2013–2014-es „Méltóság Forradalmáig" ezek a pártok és szervezetek, illetve a hozzájuk kötődő paramilitáris szervezetek inkább csak „egzotikus anakronizmust" jelentettek, és nem valódi politikai tényezőt.

A szélsőséges nacionalista szervezetek és paramilitáris alakulatok térnyerése, valamint politikai súlyának megnövekedése szorosan összefügg a „Méltóság Forradalmát" követő eseményekkel, a Krím annektálásával és a donbászi fegyveres konfliktus kirobbanásával. Az ukrán nacionalista paramilitáris alakulatok a donbászi háború időszakában a meggyengült központi államvezetés és a hadrafoghatóság határán billegő, az ország fegyveres védelmére alkalmatlan ukrán haderő kiegészítéseként, illetve alkalmanként helyette védték meg Ukrajnát a pro-orosz szeparatista erők fegyveres felkelésétől.

Kulcsszavak: *Ukrajna, szélsőséges nacionalista szervezetek, paramilitáris alakulatok, Donbász, Krím*

Extremist Ukrainian nationalist parties entered national politics right away after Ukraine's independence, but only had significant support in Western Ukraine. These parties never achieved significant political results in the Ukrainian parliamentary or

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: thunderlala13@gmail.com

presidential elections. Until the "Revolution of Dignity" of 2013–2014, these parties and organisations, as well as the paramilitary organisations associated with them, were more of an "exotic anachronism" than a real political factor.

The rise of extremist nationalist organisations and paramilitary formations are closely linked to the events following the "Revolution of Dignity", the annexation of Crimea and the outbreak of the armed conflict in Donbas. During the war in Donbas, Ukrainian nationalist paramilitary formations defended Ukraine from the armed uprising of pro-Russian separatist forces as a complement to and occasionally instead of the Ukrainian armed forces, which were incapable of defending the country with arms.

Keywords: *Ukraine, extremist nationalist organisations, paramilitary formations, Donbas, Crimea*

Bevezető

Az 1991-ben önállóvá vált Ukrajnában a nemzeti gondolkodás és a nemzetépítés már a függetlenné válás első napjaitól fogva jelen volt. A nemzetépítő, nacionalista politikai irányvonal kormányzati szinten 2004-től vált fokozatosan dominánssá. Az erősödő ukrán nacionalizmus Kijev nyugati integrációs politikájával együtt egyre növekvő biztonságpolitikai kihívást jelentett Moszkva számára, ami a „Méltóság Forradalma" 2013-as kirobbanásával az ukrán–orosz kétoldalú kapcsolatok végleges megromlásához, a Krím annektálásához és a kelet-ukrajnai, ukránellenes megmozdulások kirobbanásához vezetett.

Az ukrán szélsőséges nacionalista pártok és a részben azokból kinövő önkéntes félkatonai alakulatok[2] aktív és döntő szerepet játszottak mind a „Méltóság Forradalmában", mind pedig a 2014-ben kirobbant kelet-ukrajnai fegyveres összecsapásokban. A cikkem célja az, hogy bemutassam ezeknek a paramilitáris alakulatoknak a katonai szerepét és súlyát a 2014-es harcok során, katonai szempontból értékeljem az alkalmazásukat és annak katonai és politikai következményeit. A cikkemben a „szélsőséges ukrán nacionalista" jelzőt azokra az Ukrajna függetlenné válását követően létrehozott pártokra és paramilitáris alakulatokra használom, amelyek a két világháború közötti időszakban kialakult ukrán nacionalista gondolkodást, ezen belül a Sztepan Bandera vezette OUN-B[3] szervezet ideológiáját, és a II. világháború során a német csapatok alárendeltségében harcoló ukrán alakulatok, illetve az ukrán nacionalisták által létrehozott UPA[4] hagyományait követik. Ezekben az esetekben az ukrán nemzeti eszmét kimondottan kirekesztő módon, adott esetben a szélsőjobboldali ideológiával és akár a fasizmussal társító, más nemzetekkel

[2] A cikkben szereplő félkatonai alakulatok hivatalos ukrán megnevezése: „Добровольче військове формування України" amit alkalmanként „Добровольчий батальйон", vagy „Добробати" névvel határoznak meg. A szó szerinti fordítása „ukrán önkéntes katonai alakulat", illetve „önkéntes zászlóalj". Ez utóbbi ugyanakkor nem feltétlenül jelent zászlóalj harcértékű köteléket.

[3] Organisation of Ukrainian Nationalists – Ukrán Nacionalisták Szervezete, 1929-ben létrehozott ukrán nacionalista szervezet. 1938-ban két részre szakadt, a radikálisabb elveket képviselő szárnyat Sztepan Bandera vezette, ezt hívjuk OUN-B-nek.

[4] UPA: Українська повстанська армія – Ukrán Ellenálló Hadsereg. Az ukrán szélsőséges nacionalista szervezetek által a II. világháborúban létrehozott ellenálló haderő.

(orosz, magyar, lengyel) szemben agresszívan fellépő ukrán politikai mozgalmakról van szó. A cikkben nem térek ki minden egyes, 2014-ben létrejött ukrán önkéntes paramilitáris alakulatra (2014 tavaszán összesen 32 önkéntes alakulat jött létre[5]), csak a jelentősebb katonai szerepet játszó és egyértelműen szélsőséges nacionalista politikai háttérrel rendelkezőkre koncentrálok, és azok 2014-es tevékenységét vizsgálom.

Jelentősebb ukrán szélsőséges politikai pártok 1991 és 2014 között

Az UNA-UNSZO („Українська Національна Асамблея – Українська Народна Самооборона", Ukrán Nemzeti Gyűlés – Ukrán Népi Önvédelem)

Az 1990. november 4-én megalakult, és politikai pártként funkcionáló UNA-ból, illetve a felvállaltan paramilitáris szervezetként 1991 augusztusában létrejött UNSZO-ból állt össze, mint két, formálisan független szervezet szoros együttműködése.[6] A szervezet egyértelműen a két világháború közötti szélsőséges ukrán mozgalmak örökségét vállalta fel, a tagjai a kilencvenes években számos oroszellenes megmozdulást szerveztek, és gyakorlatilag az összes posztszovjet fegyveres konfliktusban harcoltak Oroszország ellen.

A szervezetnek a népszerűsége csúcsán körülbelül 10 ezer tagja volt, de csak Lviv, Poltava, Ternopil és Rivne megyékben volt hivatalosan bejegyzett tagszervezete, és a tagjainak közel 90%-át a fiatalabb, 35 év alatti generáció alkotta. Az UNA 2014-ben beleolvadt a jelenleg is működő „Pravij Szektorba" (lásd később), míg a paramilitáris UNSZO önállóan működött tovább.[7]

Az Ukrán Nacionalisták Kongresszusa (Конгрес українських націоналістів – KUN)

1992. október végén alapították a harmincas években működő OUN[8] Sztepan Bandera által vezetett szárnyának emigrációból visszatért tagjai. Ennek megfelelően a KUN a Bandera által képviselt szélsőséges nacionalista elveket vallotta a megalakításakor. A párt az 1998-as parlamenti választásokon a nacionalista pártokat tömörítő „Nemzeti Front" választási szövetségben indult, és kimondottan gyenge eredményt ért el (2,72% listás eredmény és öt egyéni parlamenti hely).[9] A párt 2002-ben csatlakozott a Viktor Juscsenko vezette Mi Ukrajnánk Blokkhoz (Блок Наша Україна – Народна Самооборона), amely abban az időszakban egyfajta ernyőszervezetként működött, és elsősorban a mérsékeltebb nacionalista

[5] Puglisi 2015: 6.
[6] Ramet 1999: 290.
[7] Hivatalos pártként regisztrálták a „Jobb Szektort" 2014.
[8] Organisation of Ukrainian Nationalists – Ukrán Nacionalisták Szervezete, 1929-ben létrehozott ukrán nacionalista szervezet.
[9] 1998 Parliamentary Elections 1998.

szervezeteket képviselte. A KUN 2012-ig, egy rövid megszakítással, a Mi Ukrajnánk Blokk pártszövetség tagjaként indult a választásokon.

A szervezet égisze alatt 1993 októberében létrehozták a „Trizub" paramilitáris szervezetet (Всеукраїнська організація "Тризуб" імені Степана Бандери – Trizub Sztepan Banderáról elnevezett összukrán szervezet), amely egy egyesített, független Ukrajna létrehozását tűzte ki célul, amely mentes többek között a fasiszta, kommunista, liberális és kozmopolita eszméktől. A szervezet egyik legfontosabb „eredménye" az volt, hogy itt kezdte meg a politikai pályafutását 2002-ben az Azov paramilitáris alakulatot létrehozó Andrij Bileckij.

Az Ukrán Szociál-Nemzeti Párt (Соціал-національна партія України – SNPU)

Ugyancsak szélsőjobboldali nézeteket vall, 1991. október 13-án Lvivben hozták létre, de csak 1995-ben regisztrálták hivatalos politikai pártként.[10] A szimbolikájában náci elemet[11] tartalmazó szervezet ideológiája kombinálta a radikális nacionalista, neofasiszta és antikommunista elveket, és alapvetően az OUN[12] politikai örökségét képviselte.

A párt a kilencvenes években inkább a köztörvényes akcióival vált híressé és nem a politikájával, miközben a soraiban skinheadek és futballhuligánok jelentek meg. Az 1998-as parlamenti választásokon a párt az „Ukrajna Független Államisága" (Всеукраїнське об'єднання «Державна самостійність України) párszövetség tagjaként indult, de így is alig ért el 0,16%-ot a listás szavazáson. Oleh Tjáhnibok azonban egyéni jelöltként bekerült a parlamentbe.[13] 1999-ben a párt létrehozta az „Ukrajna Patriótái" (Патріот України) paramilitáris szervezetet az ukrán haderő támogatása érdekében. A szervezet története meglehetősen kaotikus: 2004-ben feloszlatták, majd 2005-ben újjáalakult mint a „szociál-nemzeti" eszmék élcsapata, de a tevékenységét többnyire csak rasszista támadások, illetve a borispili Lenin-szobor felrobbantását célzó terrorcselekmény jellemezte 2013-ig.[14]

Az SNPU utódpártjának tekinthető Szvoboda („Всеукраїнське об'єднання »Свобода«" – „Összukrán Szövetség: »Szabadság«")

Ultranacionalista párt 2004-ben alakult meg Oleh Tjáhnibok nacionalista politikus vezetésével. Tjáhnibok ugyan kizárta az új pártból az egyértelműen fasiszta ideológiát vallókat, de a párt az ultranacionalista nézetektől nem távolodott el. Tjáhnibok többször kihangsúlyozta, hogy a „Szvoboda" nem rasszista, nem xenofób és nem antiszemita párt, hanem kizárólag egy pro-ukrán szervezet. Az országos politikai szerepvállalás tekintetében a Szvoboda

10 Iovenko 2015.
11 A szervezet címerében található jel a német „Wolfsangel" egy változata, amelyet a náci Németország egyes SS-alakulatai is alkalmaztak a II. világháborúban.
12 Rudling 2016: 31.
13 1998 Parliamentary Elections 1998.
14 Interfax 2011.

volt a legsikeresebb, szélsőséges nemzeti értékeket valló párt, és a népszerűsége csúcsán, a 2012-es ukrán parlamenti választásokon a listás szavazatok 10,45%-át kapta meg.[15]

A „Pravij Szektor" („Правий сектор", „Jobb Szektor" – PSZ)

Jelenleg is az egyik meghatározó szélsőséges nacionalista szervezet Ukrajnában. A PSZ-t 2013 novemberében, a „Méltóság Forradalma" kezdeti megmozdulásának tekinthető „Euromajdan" idején hozták létre Dmitro Jarosh vezetésével mint deklaráltan szélsőjobboldali, nacionalista félkatonai szervezetet. A szervezet 2014. február 22-én nyilvánította magát párttá, és 2014. május 22-én jegyezte be hivatalosan az ukrán belügyminisztérium.[16] Az alapítói között több, kimondottan szélsőséges, paramilitáris nacionalista csoport, így az UNA-UNSZO és az SNA tagjai is megtalálhatók. Történelmi példaképei közül a szovjet és a német haderő, illetve az orosz és a lengyel partizánok ellen egyaránt harcoló UPA[17] volt a legjelentősebb.

A fenti szervezetek egy részére jellemző volt, hogy nyíltan vállalták az ideológiai közösséget a két világháború közötti időszak szélsőséges ukrán mozgalmaival, így Sztepan Banderával és az UPA-val. Ez megjelent a szimbolikájukban, a fasizmushoz lazán köthető jelképek és/vagy a harmincas évek ukrán nacionalizmusára, illetve az UPA-ra jellemző vörös és fekete színek használatában. A szélsőséges nacionalista pártok azonban, a Szvoboda kivételével, nem tettek szert országos szinten érdemi támogatásra, csak Nyugat-Ukrajnában voltak népszerűek, és általában csak egy-egy egyéni képviselőt juttattak be a parlamentbe.

A szélsőségesen nacionalista pártok ugyanakkor már 2014-et megelőzően is képesek voltak Nyugat- és Közép-Ukrajnában több ezer támogatót mozgósítani egy-egy utcai demonstrációra, illetve egyes politikai célok elérése érdekében nem állt távol tőlük az erőszakos megmozdulás sem. Példa erre, hogy amikor 1997-ben Leonyid Kucsma ukrán elnök megpróbálta betiltani az UNA-UNSO-t, erőszakos utcai megmozdulásokhoz vezetett. Az UNA-UNSO aktivistái az SNPU támogatóival együtt aktívan részt vettek a 2000-es „Ukrajna Kucsma nélkül" kampányban is.

Az ukrán önkéntes alakulatok szerepe a „Méltóság Forradalma" során

Viktor Janukovics elnök külpolitikai „hintapolitikája" 2013 végén egy újabb belpolitikai válságot hívott életre, amely erőszakos megmozdulásokhoz és fegyveres összecsapásokhoz vezetett Kijevben, illetve a polgárháború szélére sodorta az országot. A 2014-es „Méltóság Forradalma" a 2022 februárjában kitört orosz–ukrán háború felé vezető út első mérföldköve volt, amiben az ukrán nacionalista pártok és önkéntes félkatonai szervezetek döntő szerepet játszottak.

[15] *Kyiv Post* 2012.
[16] LB 2021.
[17] UPA: Українська повстанська армія – Ukrán Ellenálló Hadsereg. Az ukrán szélsőséges nacionalista szervezetek által a II. világháborúban létrehozott ellenálló haderő.

A Janukovics-ellenes utcai tiltakozásokhoz az vezetett, hogy az ukrán elnök visszakozott a korábban külpolitikai célként meghirdetett Ukrajna–EU társulási szerződéstől és a szabadkereskedelmi egyezménytől, illetve 2013. november 21-én a kormány bejelentette az EU-val kötendő szerződés aláírásának elhalasztását.[18] A lépés mögött egyértelműen Moszkva politikai és gazdasági nyomása állt, amely gazdasági ellenlépésekkel néhány hónap alatt 4 milliárd USD veszteséget okozott Ukrajnának, majd felajánlotta az Eurázsiai Gazdasági Unióhoz való csatlakozást mint megoldást az ukrán gazdasági problémákra.

Az elnök döntését követően szinte azonnal utcai tiltakozások kezdődtek, elsősorban Kijevben, majd Nyugat-Ukrajnában, amelynek célja kezdetben Ukrajna európai uniós csatlakozása melletti kiállás volt, amit az esemény nem hivatalos neve, „Euromajdan" (a majdan teret jelent ukránul) is jelzett. Az eredetileg békés, de már a kezdetektől több ezres megmozdulás 2014 januárjára véglegesen radikalizálódott, és az ukrán rendőrség egyre erőszakosabb fellépése nyomán a tüntetők között megjelentek a radikális nacionalista szervezetek tagjai, akik felvették a harcot az ukrán rohamrendőrökkel. Az UNA-UNSZO és a 2013. november végén társadalmi szervezetként megalakult PSZ tagjai aktívan részt vállaltak a „Berkut" ukrán rendőri alakulat tagjaival való összecsapásokban. Többek között 2013. december 1-jén ott voltak az első sorokban, amikor a tüntetők megtámadták a kijevi városi adminisztráció épületét.[19] A fenti két szervezet tagjaihoz köthető a Molotov-koktélok tömeges alkalmazása az összecsapások során, a rendőri erőkkel szemben. A PSZ tagjai Nyugat-Ukrajnában is aktívak voltak, és az ottani megmozdulások során a szervezet tagjai több rendőrkapitányságot elfoglaltak, amely során nagy mennyiségű kézifegyvert zsákmányoltak.

A fent leírtaknak megfelelően elsősorban a PSZ szervezte meg a megmozdulások önvédelmét, még a tüntetés „hivatalos önvédelmi erejének" („A Majdan Önvédelmi Szervezeteinek Tanácsa" – „Egyesített Forradalmi Haderő", amelyet február 7-én, Andrij Parubij ellenzéki politikus vezetésével hoztak létre)[20] megalakítása előtt. A PSZ és az UNA-UNSZO mellett elsősorban az „Ukrajna Patriótái" paramilitáris szervezet tagjai vettek részt aktívan a rohamrendőrökkel folytatott összecsapásokban, és így jelen voltak a Janukovics elnök vezette „Ukrajna Régiói" kormánypárt kijevi székházának elfoglalásakor is 2018. február 20-án.[21] A PSZ az erőszakos ellenállás megszervezésével fokozatosan átvette a tüntetések irányítását, háttérbe szorítva a politikai válság tárgyalásos rendezésén az EU bevonásával dolgozó ukrán ellenzéki politikusokat. Ez végül döntőnek bizonyult, mivel a 2014. február 21-én Janukovics elnök és az ellenzéki politikai vezetők között megkötött, az EU és Oroszország által is támogatott megállapodást Dmitro Jarosh a PSZ nevében elutasította, és kijelentette, hogy kizárólag Janukovics elnök lemondását fogadja el. Ekkorra a kijevi megmozdulásokon részt vevő ukrán aktivisták döntő többsége már a PSZ iránymutatásait követte, az ukrán rendőrök befejezték a tüntetés felszámolását célzó műveleteiket, ezt követően pedig a tüntetők elfoglalták a kormányzati épületeket. Ez, illetve az ukrán parlament február 22-i döntése Viktor Janukovics elnök hatalomból való elmozdításáról ahhoz vezetett, hogy az elnök elhagyta Kijevet, majd Oroszországba utazott.[22]

---

18 Fedinec et al. 2021: 426.
19 *Ukrainszka Pravda* 2013.
20 Euromaidan PR 2014.
21 Interfax-Ukraine 2014.
22 *Kyiv Post* 2014.

Az ukrán szélsőséges nacionalista pártok és paramilitáris szervezetek katonai szerepe a 2014-es donbászi harcokban

A 2014. január végén egyre erőszakosabbá váló nyugat-ukrajnai és kijevi tüntetések hatására Kelet- és Dél-Ukrajnában, ezen belül a Donbász[23] több nagyvárosában ukránellenes és oroszbarát megmozdulásokra került sor. Az elsősorban Luhanszk és Donyeck városában zajló tüntetések kezdetben békés „antimajdan" megmozdulásokként indultak, de gyorsan erőszakos jelleget öltöttek. 2014. március 4-én, az Ukrajna egysége mellett fellépő ellentüntetés résztvevőire provokátorok támadtak, majd március 13-án egy ukránbarát aktivista megölésével megtörtént az első haláleset is.[24] 2014 áprilisára vége szakadt mind a békés „antimajdan", mind az „ukránbarát" tüntetéseknek, orosz szeparatista fegyveres csoportok vették át az irányítást Donyeck, Luhanszk megye egy része felett, és kikiáltották az Ukrajnától független, úgynevezett Donyecki és Luhanszki Népköztársaságot.

Harkiv városában hasonló eseményekre került sor: 2014. február végétől a kijevi eseményeket támogató „Euromajdan", illetve az azt elutasító „antimajdan" megmozdulásokra is sor került. A Donbaszhoz hasonlóan Harkivban is elsősorban a kijevi megmozdulásokat támogató aktivistákat érte atrocitás az ukrán rendőrség és a provokátorok részéről. Egyes információk szerint az ukránellenes tüntetéseken Oroszországból szervezett keretek között szállított aktivisták is részt vettek, ami valószínűsíti az orosz titkosszolgálatok beavatkozását. Az „antimajdan" aktivisták március 1-jén elfoglalták a megyei adminisztráció épületét, ahol orosz zászlók is megjelentek, április 8-án pedig kikiáltották a rendkívül rövid életű „Harkivi Népköztársaságot".[25] Ezzel egy időben, 2014. február végén Oroszország elkezdte a Krím elfoglalására kidolgozott terv végrehajtását. Február 27-én, az oroszbarát demonstrációkat követően az orosz haderő felségjelzés nélküli katonai alakulatai megkezdték a Krím elcsatolását célzó katonai műveletet.

A Krím orosz megszállása és a Donbászban kialakult ukránellenes fegyveres felkelés természetesen újabb reakciót váltott ki az ukrán szélsőséges nacionalista pártok és szervezetek részéről. Az ukrán nemzet önvédelmi képességének erősítése érdekében megkezdődött a célzottan rendvédelmi, katonai feladatok végrehajtására is alkalmas önkéntes félkatonai alakulatok formális létrehozása. A folyamatot erősítette, hogy a romló donbászi biztonsági helyzet, illetve az ukrán haderő reguláris alegységei által végrehajtott műveletek ismétlődő kudarcai miatt Arszen Avakov ukrán belügyminiszter 2014. április 13-án lehetővé tette paramilitáris alakulatok felállítását az orosz szeparatizmus elleni harcra, 12 ezer főben maximálva az összlétszámot.[26]

[23] A Donbász annak az elsősorban orosz ajkú lakosságból álló kelet-ukrajnai régiónak a neve, amely Luhanszk és Donyeck megyéket foglalja magában.
[24] Forró 2022: 27–35.
[25] Хоменко 2015.
[26] Time Note 2015.

A 2014-es ukrán katonai műveletek törvényi és ideológiai háttere

Az ukrán paramilitáris alakulatok alkalmazásának bemutatása előtt szükségesnek tartom tisztázni, hogy az ukrán politikai és katonai vezetés hivatalosan milyen katonai műveletnek minősítette a Donbászban 2014 áprilisa és az orosz invázió 2022. február 24. közötti időszakban zajló harctevékenységet. A hivatalos ukrán álláspont szerint 2014. április és 2018. február között terrorelhárító tevékenység zajlott a Donbászban, amely során az ukrán haderő és rendvédelmi erők az orosz haderő és titkosszolgálatok által támogatott, orosz nacionalista elveket valló terroristák ellen harcoltak. A műveletet ebben az időszakban „Antiterrorista Műveletnek" (*Антитерористична Операція,* ATO) minősítették, amelyet formálisan a kémelhárítással és terrorelhárítással is foglalkozó legnagyobb ukrán titkosszolgálat, az SZBU (Ukrajna Biztonsági Szolgálata) irányított.

2018. február 20-án Petro Porosenko Egyesített Erők Műveletére (*Операція об'єднаних сил,* OOSZ) nevezte át a műveletet, amelyet az ukrán nemzet biztonsága és védelme érdekében, Oroszország Luhanszk és Donyeck megye területén elkövetett katonai agressziója ellen folytattak.[27] Ebből egyértelműen következik, hogy Ukrajna a donbászi harcokat nem polgárháborúnak, hanem kezdetben terrortevékenységnek, majd nyílt orosz katonai agressziónak tekintette, ugyanakkor még a 2018-as rendelkezés szerint sem hirdetett hadiállapotot vagy rendelt el mozgósítást, illetve hadat sem üzent Oroszországnak. Ennek megfelelően a katonai műveletek során az ukrán belügyminisztérium alárendeltségébe tartozó Nemzeti Gárda alakulatainak, a belügyminisztérium speciális rendőri egységeinek, illetve önkéntes paramilitáris alegységeinek bevetése a Donbászban magától értetődő volt.

Az ukrán vezetés ugyan nemzetközi jogi értelemben nem hirdetett háborút Oroszország ellen, de az előző fejezetben, az OOSZ indoklásában felsorolt elemek egyértelműen tartalmazzák az igazságos háború, 1970-es években Michael Walzer által meghatározott elemeit: Ukrajna a területi integritását védelmezte, Oroszország agressziót követett el Ukrajna ellen, amire válaszul Ukrajna önvédelmi háborút folytat. Az igazságos háború elmélete elemeinek felhasználása ideológiai szempontból megalapozta az ukrán haderő és a rendvédelmi erők hazai földön való bevetését, és elősegíthette az önkéntes paramilitáris alakulatok felállítását és a lakosság mozgósítását.[28]

„Právij Szektor" Ukrán Önkéntes Hadtest (Добровольчий український корпус „Правий сектор") – DUK PSZ

A PSZ tagjai 2014 áprilisában állították fel az első önkéntes fegyveres alakulatot Dnyipro-2 néven, de az ukrán hatóságok hivatalosan ezt az elnevezést nem engedélyezték, mivel a belügyminisztérium kötelékében már volt egy Dnyipro-1 különleges alakulat.[29] A PSZ fegyveres szárnyának első bevetésére a Donbászban 2014. április 20-án sor került, amikor

[27] Ponomarenko 2018.
[28] Boda 2023.
[29] Bitep 2015.

a PSZ diverzáns feladatot kapott a Szlovjanszk visszafoglalását célzó ukrán katonai művelet támogatása érdekében. A feladat a városi televízióállomás elektromos ellátását biztosító elosztó állomás megsemmisítése volt, amit 20 harcossal, négy civil gépjárművel és alapvetően kézi lőfegyverekkel terveztek végrehajtani. A célpont előtt a konvoj egy korábban nem felderített oroszbarát szeparatista ellenőrző-áteresztő pontba futott bele, tűzharc tört ki, így az eredeti feladatot nem tudták végrehajtani.[30]

A DUK PSZ-t hivatalosan 2014. július 17-én mint a PSZ paramilitáris fegyveres alakulata hozták létre. A DUK PSZ a többi önkéntes paramilitáris alakulattal szemben nem kívánt az ukrán belügyminisztérium alárendeltségébe tartozni, és önállóan kezdett el működni. Ez jelentős feszültséget generált a paramilitáris alakulat és az ukrán rendőrség között, ami halálos áldozattal járó összecsapáshoz vezetett.[31]

2014 júliusára a DUK PSZ a saját nyilvántartása alapján körülbelül 5000 harcossal rendelkezett, ugyanakkor nem volt elég nehézfegyverzetük, az ukrán haderő pedig nem vállalta az alakulat felfegyverzését. A kezdeti időszakban a PSZ tagjai a 2013–2014-es tüntetések során feltört rendőrségi és katonai bázisokról zsákmányolták a kézifegyverek jelentős részét. Az egység első jelentősebb bevetésére 2014. július 16-án, Avdiivka visszafoglalása alkalmával került sor, ahol a DUK PSZ 5. zászlóalja sikeresen együttműködött az ukrán haderő 93. gépesített dandárjával.[32] A paramilitáris egység augusztus 1-jén részt vett Krasznohorivka elfoglalásában, ezúttal az 51. gépesített dandárral együttműködve.[33]

2014. augusztus közepére a kezdeti katonai sikerek ellenére tovább mélyült a konfliktus a PSZ paramilitáris alakulata és az ukrán belügyminisztérium között. Az ukrán rendőrség házkutatást tartott a DUK PSZ egyik bázisán, letartóztatott több PSZ harcost, és fegyvereket foglalt le. Jaros erre válaszul a PSZ harcosainak frontról való kivonását helyezte kilátásba arra az esetre, ha a belügyminisztérium nem vonja felelősségre az ügyben eljáró rendőröket, de rövid időn belül visszavonta ezt a nyilatkozatát.[34] A konfliktus ezzel nem oldódott meg, a teljes önállósággal rendelkező, senki által nem kontrollált alakulat egyre több problémát okozott az egyébként rendkívül rosszul teljesítő ukrán biztonsági erőknek, a PSZ pedig folyamatosan azzal vádolta az ukrán belügyminisztériumot, hogy az alakulat felszámolására törekszik.

A DUK PSZ 2014 szeptemberében Doneck város nyugati térségébe és a Donecki Nemzetközi Repülőtérre telepítette az alegységeit, és az ukrán haderő egyes alegységeivel együtt aktívan részt vett a repülőtér – azóta már legendássá vált – védelmében. Az önkéntes alegységeket végül 2014. november közepén vonták ki Donbász városának térségéből. 2014. decembertől a DUK PSZ alegységei 2015 februárjáig elsősorban rendészeti feladatokat láttak el a donbászi frontvonal körzetében, a Donbász szeparatista ellenőrzés alatt álló területei irányába tartó humanitárius forgalom ellenőrzése és a fegyvercsempészet megakadályozása érdekében.

30 Бутусов 2016
31 Вітер 2015.
32 Бійці ДУК та 93 бригада ЗСУ знайшли катівню ДНР і тіло вбитого ними цивільного 2014.
33 Ukrainszka Pravda 2014.
34 Global Security [é. n.].

Azov zászlóalj (батальйон »Азов«) – Azov

Az Azov paramilitáris alakulatot 2014 májusában alapították Andrij Bileckij vezetésével, aki korábbi politikai pályafutása során a Trizub és az SNPU szélsőséges nacionalista szervezeteknél is tevékenykedett. Az Azov tekinthető a legismertebb és legsikeresebb, szélsőséges nacionalista eszméket valló ukrán paramilitáris szervezetnek, amelynek népszerűségét Mariupol, illetve az Azovsztal Fémművek hónapokig tartó védelmében játszott szerepe még tovább erősített. A szervezet jelentőségét az is növeli, hogy ez az a paramilitáris alakulat, amelyet az orosz politika és média az elmúlt években rendszeresen felhasznál annak érdekében, hogy a „fasiszta Ukrajna" létezését bizonyítsa. A 2014-es felvételek, illetve riportok alapján megállapítható, hogy Azov megalakításakor az állomány többsége oroszajkú volt, ami az ukrán nacionalizmus egyik sajátosságára vezethető vissza: az anyanyelv nem feltétlenül határozza meg a nemzeti hovatartozást, így egy orosz anyanyelvű ukrán is lehet elvakult ukrán nacionalista.

Bileckij már az alakulat hivatalos létrejötte előtt, 2014. március közepén irányított Harkiv városában egy „Black Korps" elnevezésű paramilitáris egységet, amely az Azov elődszervezetének tekinthető. A „Black Korps" az orosz támogatást élvező fegyveres csoportoktól próbálta megvédeni a városban működő ukrán állami intézményeket és ukrán érzelmű aktivistákat. 2014 márciusában a donbászi eseményekkel párhuzamosan Harkivban is megszaporodtak a pro-orosz megmozdulások, aminek hatására kivonták a városból az SZBU és az ukrán rendőrség erőit. Ezt követően a „Black Korps" körülbelül 60, könnyűfegyverzettel felszerelt harcosa bevonult a városba, rendfenntartó járőrtevékenység, illetve az ukrán állami intézmények védelme érdekében. 2014. március 14-én az orosz nacionalista „Oplot" fegyveresei megtámadták az ukrán önkéntesek egy csoportját és az „Ukrán hazafi" állami szervezet irodáját Harkiv központjában. A „Black Korps" harcosai automata kézifegyverekkel visszaverték a támadást, a tűzharc során két orosz fegyveres életét vesztette. Általában véve ezt a tűzharcot tekintik az első nyíltan ukrán–orosz fegyveres összecsapásnak, amennyiben eltekintünk a Krím orosz megszállásától.[35]

A „Black Korps" mellett a „Harkiv Metalist FC" labdarúgó klub „Sect 82" elnevezésű szurkolócsoportjának bázisán létrejött önvédelmi alakulat is szerepet játszott a harkivi összecsapásokban. A „Sect 82" aktivistái a harkivi ukránellenes megmozdulások során részt vettek a megyei adminisztráció épületének védelmében. A „Sect 82" bázisán létrehozták a „Keleti Hadtest Speciális Rendőrjárőr" („Компанія Схід") alakulatot, amely 2014 novemberében az ukrán rendőrség hivatalos alegységévé vált.[36]

A harkivi biztonsági helyzet rendeződése után a „Black Korps" harcosait kivonták Harkivból, majd az Azov hivatalos megalakulását követően beleolvadt a szervezetbe. Az Azov 50 fős, 2014. június 26-án Mariupolba útnak indított, frissen kiképzett alegysége a „Black Korps" felvarróit viselte az egyenruháján.[37]

Az Azov már a megalakulásától fogva teljesen függetlennek tekintette magát az ukrán állami szervektől. A paramilitáris szervezet finanszírozását ukrán oligarchák vállalták magukra, akik közül ki kell emelni az akkori Dnyipropetrovszki kormányzót,

[35] Бутусов 2017.
[36] Time Note 2015.
[37] Демкова 2014.

Igor Kolomojszkijt, aki az egyik legsikeresebb ukrán üzletember volt abban az időszakban. Kolomojszkij zsidó gyökerekkel rendelkezett, így amikor 2014 augusztusában az Azov parancsnokhelyettese, Ihor Moszijcsuk nyíltan antiszemita megjegyzést tett, Kolomojszkij a pénzügyi támogatás befagyasztását helyezte kilátásba. A problémát Moszijcsuk Azovtól való távozása oldotta meg.[38]

Az Azov első komolyabb bevetését és sikerét Mariupol városának visszafoglalása jelentette 2014. május 15. és június 14. között („első mariupoli csata"), amelyben az ukrán haderő és a belügyminisztérium egyes alakulataival együttműködve vett részt. Mariupol Ukrajna legfontosabb kikötővárosa az Azovi-tenger partján, amit a Donyecki Népköztársaság harcosai a márciusi megmozdulások során elfoglaltak. A kikötőváros megtartása kiemelten fontos volt az akkor még az ukrajnai konfliktusba hivatalosan be nem avatkozó Oroszország számára, amit az is jelez, hogy az orosz haderő három, azonosítójel nélküli T-64-es harckocsit és több BM-21-es sorozatvetőt vezényelt a Mariupolt védő pro-orosz harcosok támogatására.

A mariupoli harcok befejező szakaszában, június 13-án az Azov harcosai a Dnyipro-1 speciális rendőri zászlóaljjal együtt több kulcsfontosságú épületet foglaltak el, megsemmisítettek egy BRDM-2-es páncélozott felderítő harcjárművet és egy páncélozott tehergépjárművet. Az alakulat legalább 100 fővel vett részt a műveletben, amely során nem rendelkezett nehézfegyverzettel.[39]

Mariupol felszabadítását követően az Azov a város térségben települt, majd az ukrán haderő – elsősorban a 93. gépesített dandár – egyes alegységeivel, a különleges rendőri erőkkel (Dnyipro-1 zászlóalj), illetve a Donbász és Sahtarsk önkéntes zászlóaljak egyes alegységeivel együtt részt vett az Ilovajszk elleni 2014. augusztus 10–11-i támadásban. A művelet kezdetben sikertelennek bizonyult, amiért a város bekerítésébe késve, és a szükségesnél kisebb élőerővel bekapcsolódó Azovot tették felelőssé. Ilovajszkot az ukrán erők végül augusztus 20-án foglalták el, aminek utolsó lépéseként az Azov zászlóalj három lövész és egy felderítő rajt telepített Ilovajszk keleti határára. Az Azov alegységei rövid tisztogató és rendfenntartó feladatok ellátása után, augusztus 23-án áttelepültek a Mariupoltól 45 kilométerre lévő Novoazovszkba, mivel felderítő információk alapján az orosz haderő egy oszlopa megindult a város irányába. Az ilovajszki művelettel egy időben az Azov egyik alegysége az ukrán haderő egyik ejtőernyős alakulatának alegységével visszafoglalta Mariinka települést, és behatolt Donyeck külvárosába.

A zászlóalj Ilovajszkból való kivonásának köszönhetően már nem volt a térségben, amikor az oroszbarát szeparatista erők, az orosz reguláris haderő egységeinek hatékony és közvetlen támogatásával augusztus 24–25. között bekerítették és gyakorlatilag megsemmisítették az ukrán haderő és az önkéntes alakulatok város térségében tartózkodó, támadó műveletet folytató alegységeit. Az ilovajszki katasztrófa egyik okaként később az ukrán haderő vezetésének inkompetenciája mellett, az Azov és a Sahtarsk önkéntes zászlóaljak térségből való idő előtti kivonását jelölték meg.[40]

A Novoazovszk térségében augusztus 25–28. között lezajlott ütközetben az ukrán erők ismét vereséget szenvedtek, ami elsősorban annak volt köszönhető, hogy az orosz haderő

[38] Young 2022.
[39] Drobnjakovich–McHugh 2014.
[40] Rachkevych 2015.

itt is támogatta harckocsikkal és nehézfegyverzettel a szeparatista erőket. Novoazovszk elvesztését követően az orosz szeparatista erők szeptember elején újabb támadást indítottak Mariupol ellen. Az Azov zászlóalj körülbelül 500 fővel vett részt a város védelmében. Az alakulat harcosai elsősorban felderítő feladatokat hajtottak végre Mariupol keleti előterében, illetve részt vettek a polgári lakosság köréből toborzott milícia tagjainak kiképzésében. Az ukrán erők szeptember 4-én indított ellentámadása megállította a szeparatista erők támadását, a szeptember 5-én megkötött tűzszünet pedig stabilizálta a frontvonalat. A művelet során az Azov továbbra is elsősorban könnyűfegyverzettel hajtotta végre a feladatokat, de az ukrán haderő harckocsikkal és páncélozott szállító harcjárművekkel támogatta a paramilitáris alakulatot.[41]

Az Azov zászlóaljat 2014 szeptemberében ezreddé szervezték át, majd november 11-én hivatalosan is beintegrálták a belügyminisztérium alárendeltségébe tartozó Nemzeti Gárda kötelékébe. Az Azov integrálása a Nemzeti Gárdába az ukrán kormány azon törekvésének volt az eredménye, hogy minden önkéntes paramilitáris alakulat a belügyminisztérium alárendeltségébe kerüljön. Az Azov integrációját követően az alakulat állami forrásokhoz is hozzáfért, és elkezdték nehézfegyverzettel felszerelni az alegységeket. Bileckij 2014 októberében kilépett az alakulat kötelékéből.

„Szics" Különleges Rendeltetésű Zászlóalj (батальйон особливого призначення Січ) – Szics

A Szics az Azovhoz és a DUK PSZ-hez képest lényegesen kisebb szerepet játszott a donbászi harcokban. A „Szvoboda" aktivistái 2014 júniusában hozták létre a „Szics" Különleges Rendeltetésű Zászlóaljat, amelyet az ukrán belügyminisztérium 2014. június 12-én jegyzett be. A zászlóalj állományát a létrehozásakor a „Szvoboda" önkéntesei, a Zaporizzsja megyei Rendkívüli Helyzetek Szolgálatának egyes munkatársai, illetve nem tisztázott hátterű „Irakban szolgált veteránok" alkották. Az alakulat már a létrehozásakor az ukrán belügyminisztérium alárendeltségébe tartozott mint speciális rendeltetésű rendőri egység.[42]

Az alakulat névválasztása megítélésem szerint magyarázatra szorul: a rendelkezésre álló információk alapján a Szics[43] névvel a zaporizzsjai kozákok örökségét vállalták fel, így a névválasztás nem az 1938 novemberében, Kárpátalján létrehozott Kárpáti Szics Népi Önvédelmi Szervezetre utal (Kárpáti Szics – Організація народної оборони «Карпатська Січ»). Az alakulat 2014. augusztus végén egy körülbelül 100 fős alegységet telepített az ATO-ba, ahol elsősorban a kurakhovói gát védelmét látták el, illetve Szlovjanszk városában rendfenntartó feladatokat látott el 2015 februárjáig.

41 MacAskill–Walker 2014.
42 Korrespondent 2014.
43 A 16–17. században szicsnek a zaporizzsjai kozákok által épített kisebb erődítményeket, illetve erődített településeket nevezték.

Összegzés

Az ukrán ultranacionalista paramilitáris alakulatok megjelenésére és alkalmazására Ukrajna modern kori történetének legnagyobb belpolitikai válsága idején került sor. A tény, hogy a 2014-ig marginális politikai szerepet játszó pártok és szervezetek, illetve az általuk létrehozott fegyveres alakulatok a politika első vonalába kerülhettek, annak köszönhető, hogy Ukrajna politikai vákuumba került Janukovics elnök és a kormány bukását követően. A paramilitáris alakulatok szerepének jelentőségét növelte az is, hogy a kelet-ukrajnai harcok kitörésekor az ukrán haderő az alulfinanszírozottság és a kiképzési hiányosságok miatt gyakorlatilag nem volt hadra fogható. Ebben a helyzetben a gyorsan reagáló és ideológiailag erősen motivált nacionalista önkéntesek katonai szerepvállalása alkalmanként döntőnek bizonyult.

Az ukrán önkéntes alakulatok a belügyminisztériumhoz tartozó Nemzeti Gárda alárendeltségébe tartoztak, nemcsak rendfenntartó feladatokat végeztek, hanem az első vonalban, az ukrán haderő alakulataival együtt támadó és védelmi feladatokat is elláttak. A bevetésük során alkalmanként az irreguláris gerilla hadviselés elemei is felmerültek (felderítési és diverzáns feladatok ellátása az ellenség mélységében), de az esetek döntő részében a paramilitáris erők – az ukrán haderő alegységeivel együttműködésben – hagyományos harceljárásokat alkalmaztak.

A „Méltóság Forradalmát", illetve elsősorban a Krím annektálását követően természetesen nemcsak a nacionalista szervezetek alakítottak önkéntes paramilitáris alakulatokat, de létszáma, és tevékenysége alapján a „Právij Szektor" által létrehozott DUK PSZ, illetve a Trizubhoz és SNPU-hoz köthető Azov is kiemelkedik a sorból. Az ukrán nacionalista szervezetek gyorsabban és hatékonyabban tudtak reagálni azokra a kelet-ukrajnai proorosz fegyveres felkelésekre, és fontos szerepet játszottak Harkiv és Mariupol védelmében. Amennyiben az úgynevezett Harkivi Népköztársaság, a Donyeckihez és Luhanszkihoz hasonlóan meg tudta volna vetni a lábát Északkelet-Ukrajnában, illetve Mariupol a Donyecki Népköztársaság uralma alá került volna, az orosz haderő 2022. február 24-én sokkal kedvezőbb hadműveleti helyzetből kezdhette volna meg a támadást Ukrajna ellen. Ne felejtsük el, hogy az oroszoknak több mint fél évükbe telt Mariupol elfoglalása, ami alapvetően befolyásolta a Zaporizzsja megyei támadó műveleteket. Harkiv elfoglalása pedig az orosz–ukrán háború három éve alatt sem sikerült az orosz haderőnek.

Az új ukrán kormány ugyanakkor a kezdetektől fogva tisztában volt azzal, hogy a szélsőségesen nacionalista önkéntes alakulatok kétélű fegyvert jelentenek: adott esetben akár a regnáló ukrán kormány ellen is felhasználhatók. Ennek megfelelően már 2014 tavaszától arra törekedtek, hogy az alkalmanként „elszabadult hajóágyúként" viselkedő paramilitáris alakulatokat beintegrálják a Nemzeti Gárda alárendeltségébe, és teljes mértékben a kormány irányítása alá vonják azokat. Ez ugyanakkor folyamatos feszültséget okozott, és alkalmi összecsapásokhoz vezetett a paramilitáris alakulatok és az ukrán rendőrség között.

Megítélésem szerint az ukrán nacionalista félkatonai szervezetek és alakulatok 2014-es harcokban játszott szerepe felveti azt a kérdést, hogy az egyébként a fősodorba tartozó politika és a társadalom döntő többsége számára kevéssé vállalható ideológiát követő szélsőséges politikai szervezetek tagjaival az állam – váratlan és az állam fennmaradását veszélyeztető külső katonai fenyegetettség esetén – számolhat-e mint gyorsan mozgósítható és bevethető katonai, illetve rendfenntartó segédcsapatok. Az ukrajnai

tapasztalatok alapján ezeknek a szervezeteknek a tagjai gyorsabban mozgósíthatók, az átlagosnál jobban motiváltak a haza védelmére, és általában rendelkeznek katonai alapképzéssel. Más kérdés persze az, hogy az azonnali veszély elmúltát követően már nehéz visszadugni a szellemet a palackba.

Felhasznált irodalom

1998 Parliamentary Elections (1998). Online: https://web.archive.org/web/20040809223530/http://www2.essex.ac.uk/elect/database/indexElections.asp?country=UKRAINE&election=ukr98

Бійці ДУК та 93 бригада ЗСУ знайшли катівню ДНР і тіло вбитого ними цивільного (2014). július 31. Online: https://web.archive.org/web/20140802150200/http://ps-zahid.info/news/bijtsi-duk-ta-93-bryhada-zsu-znajshly-kativnyu-dnr-i-tilo-vbytoho-nymy-tsyvilnoho

Бутусов, Юрий (2016): Дмитро Ярош: "Перший наступальний бій війни відбувся 20 квітня 2014-го – добровольці атакували блокпост під Слов'янськом". *Censor.net,* 2016. Online: https://censor.net/ru/r385673

Бутусов, Юрий (2017): 14 марта 2014 года – добровольцы Харькова отразили атаку российского террориста Арсена Павлова на улице Рымарской. *Censor.net,* 2017. március 13. Online: https://web.archive.org/web/20200122225522/https://censor.net.ua/resonance/431983/14_marta_2014_goda_dobrovoltsy_harkova_otrazili_ataku_rossiyiskogo_terrorista_arsen%20a_pavlova_na_ulitse

Вітер, Марта (2015): Позивний Мольфар. Письменник на війні. *Ukrainszka Pravda,* 2015. február 6. Online: https://web.archive.org/web/20150206133626/http://life.pravda.com.ua/person/2015/02/6/188936/

Boda Mihály (2023): Az igazságos háború elmélete és a teremtésvédelem: az igazságos háború elméletének története a középkortól a 20. századig a teremtésvédelem szempontjából. *Hadtudományi Szemle,* 16(4), 123–137. Online: https://doi.org/10.32563/hsz.2023.4.6

Демкова, Слава (2014): «Чорний корпус» відправився в зону АТО. *Uapress.info,* 2014. június 24. Online: https://web.archive.org/web/20220619223209/https://uapress.info/uk/news/print/28835

Drobnjakovich, Marko – McHugh, David (2014): Ukrainian Troops Drive Rebels Out of Mariupol. *AP News,* 2014. június 14. Online: https://apnews.com/general-news-040fce7786064fd6872e4d045c29955d

Euromaidan PR (2014): The Council of Maidan Self-Defense Organizes "United Revolutionary Army" throughout Ukraine. *Euromaidan PR,* 2014. február 8. Online: https://euromaidanpr.wordpress.com/2014/02/08/the-council-of-maidan-self-defense-organizes-united-revolutionary-army-throughout-ukraine/

Fedinec Csilla – Font Márta – Szakál Imre – Varga Beáta (2021): *Ukrajna története: régiók, identitás, államiság.* Budapest: Gondolat.

Forró, Tomáš (2022): *Nászutas lakosztály a Háború Hotelben.* Ford. Mészáros Tünde. [h. n.]: Lábnyom.

Global Security [é. n.]: Volunteers. *Global Security,* [é. n.]. Online: https://web.archive.org/web/20230308125421/https://www.globalsecurity.org/military/world/ukraine/volunteers.htm

Хоменко, Святослав (2015): "ХНР": Харківська невдала республіка. *BBC News Ukraina,* 2015. április 8. Online: https://www.bbc.com/ukrainian/politics/2015/04/150406_kharkiv_sx

Interfax (2011): SBU Opens Criminal Case Against 'Vasylkiv Terrorists'. *Interfax,* 2011. augusztus 23. Online: https://en.interfax.com.ua/news/general/77439.html

Interfax-Ukraine (2014): Radical Protesters Burst into Party of Regions' Kyiv Office. *Kyiv Post,* 2014. február 18. Online: https://archive.kyivpost.com/article/content/ukraine-politics/radical-protesters-burst-into-party-of-regions-kyiv-office-337006.html

Iovenko, Artem (2015): The Ideology and Development of the Social-National Party of Ukraine, and Its Transformation into the All-Ukrainian Union "Freedom," in 1990–2004. *Communist and Post-Communist Studies,* 48(2–3), 229–237. Online: https://doi.org/10.1016/j.postcomstud.2015.06.010

Korrespondent (2014): Партія Свобода створює власний батальйон. *Korrespondent,* 2014. június 13. Online: https://ua.korrespondent.net/ukraine/politics/3377514-partiia-svoboda-stvoruiie-vlasnyi-batalion

Kyiv Post (2012): With All Party Lists Ballots Counted, Regions Party Gets 30%, Batkivschyna 25.54%, UDAR 13.96%, Communists 13.18%, Svoboda 10.44%. *Kyiv Post,* 2012. november 8. Online: https://archive.kyivpost.com/article/content/oct-28-parliamentary-election/with-all-party-lists-ballots-counted-regions-party-gets-30-batkivschyna-2554-udar-1396-communists-1318-svoboda-1044-315790.html

Kyiv Post (2014): Parliament Votes 328-0 to Impeach Yanukovych on Feb. 22; Sets May 25 for New Election; Tymoshenko Free. *Kyiv Post,* február 23. Online: https://archive.kyivpost.com/article/content/ukraine-politics/euromaidan-rallies-in-ukraine-feb-21-live-updates-337287.html

LB (2021): Політична партія "Правий сектор". *LB.ua,* szeptember 30. Online: https://lb.ua/file/party/1610_politichna_partiya_praviy_sektor.html

MacAskill, Ewen – Walker, Shaun (2014): Heavy Shelling in Ukrainian Port of Mariupol Hours Before Agreed Ceasefire. *The Guardian,* 2014. szeptember 5. Online: https://www.theguardian.com/world/2014/sep/05/ukraine-heavy-shelling-hours-before-ceasefire-russia

Ponomarenko, Illia (2018): Goodbye, ATO: Ukraine Officially Changes Name of Donbas War. *Kyiv Post,* 2018. február 20. Online: https://www.kyivpost.com/ukraine-politics/goodbye-ato-hello-taking-measures-ensure-national-security-defense-repulsing-deterring-armed-aggression-russian-federation-donetsk-luhansk-oblasts.html

Puglisi, Rosaria (2015): *Heroes or Villains? Volunteer Battalions in Post-Maidan Ukraine* Istituto Affari Internazionali, 2015. március 8. Online: https://www.iai.it/sites/default/files/iaiwp1508.pdf

Rachkevych, Mark (2015): Turning Point. *Kyiv Post,* 2015. augusztus 20. Online: https://archive.kyivpost.com/kyiv-post-plus/turning-point-396222.html

Ramet, Sabrina P. ed. (1999): *The Radical Right in Central and Eastern Europe Since 1989.* Pennsylvania State University Press.

Романенко, Валентина (2023): УПЦ МП заборонили на Житомирщині. *Українська правда, ВВС Україна,* 2023. április 27. Online: https://www.pravda.com.ua/news/2023/04/27/7399690/

Rudling, Per Anders (2016): The Cult of Roman Shukhevych in Ukraine: Myth Making with Complications. *Fascism: Journal of Comparative Fascist Studies,* 5(1), 26–65. Online: https://doi.org/10.1163/22116257-00501003

Stern, David (2012): Svoboda: The Rise of Ukraine's Ultra-Nationalists. *BBC News,* 2012. december 26. Online: https://www.bbc.com/news/magazine-20824693

Time Note (2015): The Azov Special Operations Detachment. *Timenote.info,* 2015. Online: https://timenote.info/en/events/The-Azov-Special-Operations-Detachment

Ukrainszka Pravda (2013): У КМДА побили вікна та двері. *Ukrainszka Pravda,* 2013. december 1. Online: https://www.pravda.com.ua/news/2013/12/1/7003983/view_print/

Ukrainszka Pravda (2014): Сили АТО звільнили Красногорівку – Ярош. *Ukrainszka Pravda,* 2014. augusztus 1. Online: https://web.archive.org/web/20140804025019/http://www.pravda.com.ua/news/2014/08/1/7033707/

Young, Cathy (2022): Heroes of Mariupol or Neo-Nazi Menace? *The Bulwark,* 2022. május 25. Online: https://www.thebulwark.com/p/heroes-of-mariupol-or-neo-nazi-menace

NEMZETBIZTONSÁGI SZEMLE
13. évfolyam (2025) 2. szám 34–50. | DOI: 10.32561/nsz.2025.2.3

Bottyán Sándor[1]

A nagy nyelvi modellek működése és képzése, valamint alkalmazásuk stratégiai elemzése, 2. rész

The Operation and Training of Large Language Models and a Strategic Analysis of Their Application, Part 2

A nagy nyelvi modellek működése komplexitásukból adódóan nehezen érthető és magyarázható tárgykör, de ez a kétrészes tanulmány megkísérli közérthetően bemutatni annak alapvetéseit és a velük tapasztalható jelenségeket. A második részben kifejtjük a nagy nyelvi modellek képzési ciklusát, a képzés alapjául szolgáló adatkészletek típusait, az előképzés, a finomhangolás módszertanát és jellegzetességeit, valamint a modellek gyakori alkalmazási módozatait. A nagy nyelvi modellek alkalmazásának előnyeit és hátrányait egy SWOT-elemzés keretében analizáljuk, kiegészítve azon releváns belső és külső tényezőkkel, amelyek egy szervezet által folytatott információfeldolgozási folyamatban jelentkezhetnek. A tanulmányt azoknak ajánljuk, akik a nemzetbiztonsági területen folytatott információfeldolgozás iránt érdeklődnek, továbbá akik átfogó ismeretanyagot keresnek a nagy nyelvi modellekről, és azt saját kutatásaikban szeretnék felhasználni.

Kulcsszavak: *nagy nyelvi modell, mesterséges intelligencia, ChatGPT, gépi tanulás*

The complexity of large language models makes them a difficult subject to understand and explain, but this two-part study attempts to present their basic principles and the phenomena they reveal in a clear and accessible way. In the second part, the training cycle for large language models, the types of data sets on which the training is based, the methodology and characteristics of pre-training and fine-tuning, and common applications are explained. Furthermore, in order to provide a comprehensive understanding of the advantages and disadvantages of the large language models, a detailed SWOT analysis has been carried out to evaluate the relevant internal and

[1] Hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Műszaki Doktori Iskola, e-mail: bottyan.sandor@gmail.com

external factors that may be involved in the information processing procedure of an organisation. The study is recommended for those interested in the field of information processing by national security, who are looking for a comprehensive knowledge on the large language models and want to use it in their own research.

Keywords: *large language model, artificial intelligence, ChatGPT, machine learning*

Bevezetés

Napjainkban a mesterséges intelligencia (MI) területén tapasztalható gyors fejlődés egyik legmeghatározóbb vívmánya a nagy nyelvi modellek (*large language models,* LLM) megjelenése. Ezek a modellek hatalmas mennyiségű szöveges adat feldolgozására, valamint összefüggések és mintázatok felfedezésére képesek – olyan hatékonysággal, amelyhez emberi erőforrással csak rendkívüli idő- és munkaráfordítással tudnánk felérni. A modern LLM-eket alkalmazó keretrendszerek lehetővé teszik a szöveges tartalmak és metaadatok közel valós idejű, együttes elemzését, mégpedig olyan volumenben, amelyet hagyományos módszerekkel csak nehezen vagy egyáltalán nem lehetne megvalósítani. A modellek leghatékonyabb működéséhez jelentős erőforrások biztosítása és a hozzájuk kapcsolódó eljárások harmonizálása szükséges, amelyet biztosítani csak kellő szakértelemmel (például adattudósok, számítástechnikai mérnökök, nyelvtudósok stb.) és jelentős tőkebevonással lehet. Bár ezek még közismert tények, a legújabb LLM-fejlesztések eredményei (például otthon, lokális környezetben futtatható modellek) lehetővé teszik új felhasználási módok megjelenését. A modellek segítségével a friss adathalmazokból kinyerhető időszerű tudás rendkívül értékes, és ez a nemzetbiztonsági tevékenységek (például hírszerzés és kockázatelemzés) területén sincs másként. A széles körű adatgyűjtés és annak gyors feldolgozása alapvető fontosságú a nemzetbiztonsági szervek számára. Az evidenciák összekapcsolásával létrejövő új tudás felismerése megelőzheti az állami működésre veszélyes kritikus eseményeket, elősegítheti a terrorizmus elleni küzdelmet, továbbá támogatást nyújthat a kiberhadviselésben és a diplomáciai tevékenységekben is. Míg a kétrészes tanulmány első részében a modellek technikai vonatkozásainak néhány aspektusát vizsgáltuk, addig ebben a második részben inkább a szervezeti követelményekre és az alkalmazás során fellépő ismert tényezőkre (erősségek, gyengeségek, lehetőségek, fenyegetések) koncentrálunk, illetve ezek közös értékelését végezzük el. Az LLM-ek offenzív felhasználása (például kártékony kódok írása, terrorista cselekmények tudástámogatása) ma már nem példa nélküli, ugyanakkor ez az összeállított tudásanyag hozzásegít ahhoz, hogy a nagy nyelvi modellekre egy hatékony információkinyerési eszközként gondoljunk, és felismerjük a nemzetbiztonsági feladatokhoz kapcsolódó eljárásokban betöltött szerepüket, így támogatva a technológia felhasználását az állambiztonság növelése érdekében.

Nagy nyelvi modellek képzése

A nagy nyelvi modellek által biztosított képességek olyan hatékonyságnövelő lehetőségek, amelyekkel a legtöbb szervezet élni szeretne, azonban önálló modellek létrehozása

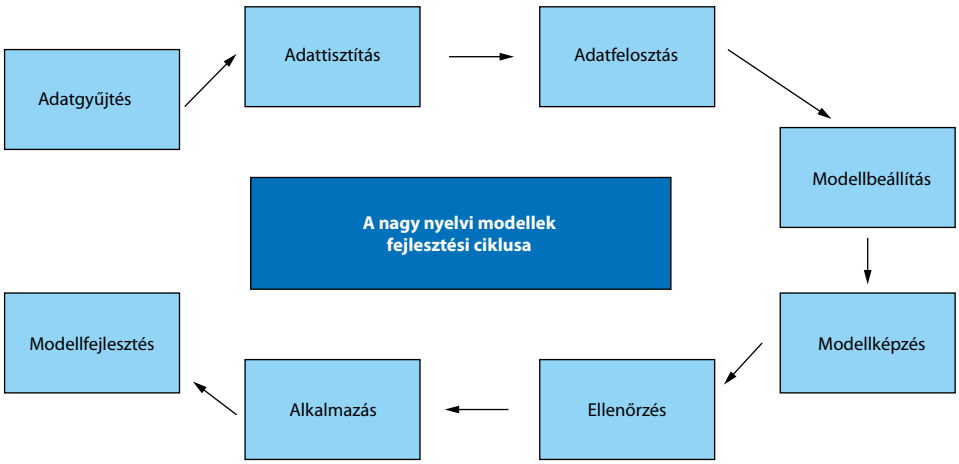
leginkább az óriásvállalatokra vagy kutatóközpontokra jellemző, de néhány esetben közösségi kezdeményezések is előfordulnak. Ennek oka, hogy a modellfejlesztés és üzemeltetés monumentális erőforrásokat igényel, emellett az eljárás hosszas és költséges. Jelentős tőkebevonás szükséges a hosszú távú projektfolyamatok (például infrastruktúra-tervezés, adatvásárlás, adatgyűjtés és előkészítési eljárások, emberi erőforrások, K+F folyamatok, termékfejlesztés stb.) pénzügyi támogatására. Nagy adatkészletek szükségesek a modellek tanítási folyamataihoz és az eredmények kiértékeléséhez egyaránt, az adatok felkészítése a modellképzéshez is jelentős erőforrásokat emészt fel. A versenyképes interdiszciplináris szakértelem (például adattudósok és adatmérnökök, gépitanulás-kutatók, nyelvészek, NLP[2] szakértők, szoftverfejlesztők és mérnökök, etikai, adatvédelmi és jogi szakértők stb.) biztosítását nem lehet kizárólag anyagi forrásból biztosítani, az leginkább a szervezett kutatási és fejlesztési háttérrel rendelkező technológiai nagyvállalatok privilégiuma. A nagyszabású számítási képességre képes informatikai infrastruktúra rendelkezésre állása szintén nem könnyen biztosítható feltétel, bár már egyes felhőalapú rendszerek és adattközpontok gazdaságosan hozzáférhetők.

A tőkebevonás mértékének durva becsléséhez segítségül jöhet néhány szakirodalmi információ. 2020-ban az Open AI kutatótudósai közzétettek egy tanulmányt a GPT-3 modell részletezéséről,[3] az itt publikált adatok alapján független szakértők 12 millió dollárra becsülték a modell képzési költségét.[4] A szükséges informatikai infrastruktúra becsléséhez költségpéldázat lehet az MT-NLG (Megatron-Turing Natural Language Generation)[5] nagy nyelvi modellről kiadott információk elemzése, amely szerint a modell képzése egy *Selene* szuperszámítógépen[6] történt, és minden modellreplika betanítása 560 db DGX A100 GPU teljesítményét igényelte, amelyeknek darabontként a piaci ára több mint 200 ezer dollár. A tömérdek számítási művelet végrehajtása irreálisan hosszú betanítási időt (akár több hét vagy hónap) eredményezhet, így a tanítási folyamat tervezése és megvalósítása során kiemelt figyelmet kell fordítani az algoritmusok, a szoftverek és a hardverek együttes optimalizálására.[7] Amennyiben az említett feltételek rendelkezésre állnak, abban az esetben megkezdhető a modell fejlesztési folyamata, a következőkben ennek bemutatására térünk rá.

A fejlesztési ciklus

A nagy nyelvi modellalkotás lépéseinek részletezésére a terjedelmi korlátok okán nincs lehetőségünk, így ezt a folyamatot csak általánosságban érintjük. A részfolyamatok (például adatfeldolgozás, fejlesztés, képzés, értékelés stb.) összességére mint eljárásra hivatkozhatunk képzési folyamatként, modellfejlesztési folyamatként is. De az „adattól a modellig" megközelítésre egy olyan fejlesztési ciklusként tekinthetünk, amelynek alábbi főbb pontjait minden eltérő modellalkotási folyamatban közel azonosan megtaláljuk (1. ábra).

[2] Natural language processing, vagyis természetes nyelvfeldolgozás.
[3] Brown et al. 2020.
[4] Wiggers 2020.
[5] Egy nagy nyelvi modell, amelyet a Microsoft és az Nvidia fejlesztett ki. Több száz milliárd paraméterrel rendelkezik. Az egyik legnagyobb és legfejlettebb transzformer alapú nyelvi modell.
[6] Harangi 2020.
[7] Kharya–Alvi 2021.



1. ábra: A nagy nyelvi modellek megalkotásának főbb lépései
Forrás: a szerző szerkesztése

A nagy nyelvi modellek fejlesztési ciklusának főbb lépései:

1. Az *adatgyűjtés (data gathering)* fázisában összegyűjtik a nyelvi modell képzéséhez szükséges adatokat. A cél az, hogy elegendő mennyiségű és változatos adat álljon rendelkezésre, továbbá amennyiben speciális felhasználásra tervezzük a modellt, abban az esetben a tartományspecifikus[8] adatkészlet összeállítása is szükséges.
2. Az *adattisztítás (data cleaning)* szükséges eljárás annak okán, hogy az összegyűjtött adatok gyakran tartalmaznak hibás, irreleváns vagy torz információkat. A folyamat célja az adatkészlet felkészítése a tanítási folyamatra. Ebben a lépésben eltávolítják azokat az elemeket, amelyek zavarnák a modell tanulási folyamatát, például helyesírási hibák, duplikált adatok vagy irreleváns tartalmak.
3. Az *adatok felosztása (data splitting).* A tanítóanyagot általában három különböző részre osztják: tanítási adat *(training data),* validálási adat *(validation data)* és tesztadat *(test data).* A tanítási adatokra építve tanul a modell, a validálási adatokkal ellenőrzik a modell teljesítményét a képzés során, a tesztadatokkal pedig a végső értékelést végzik a modell teljesítményéről. Az adatfelosztás biztosítja, hogy a modell ne tanulja meg a tesztadatokat, ezáltal a teljesítményértékelés objektív marad.
4. A modell beállítása vagy felállítása *(model setup)* során annak konfigurációját állítják be. Ez magában foglalja a modell tanulási folyamatát befolyásoló tényezők, tehát a modell architektúrájának (például típusa és mérete stb.) és

[8] A tartományspecifikus adatkészlet (angolul: *domain-specific dataset*) olyan különleges adatkészlet, amely nemcsak az általános nyelvi formulákat tartalmazza, hanem egy kiválasztott területről (pl. orvosi, jogi, mérnöki stb.), szakterületről használ fel szöveges tartalmat, így annak a szakterületnek a speciális nyelvi jellegzetességeit (pl. szaknyelv, terminológia stb.) is magában hordozza.

a hiperparaméterek, valamint a képzési eljárás optimális konfigurációjának meghatározását (például batch size,[9] epochok[10] száma).

5. A modell tanítása vagy képzése *(model training)* alatt a modell a tanítóadaton keresztül próbálja optimalizálni a paramétereit, felismerni a mintázatokat, és fokozatosan javítja a predikciós képességeit. A legnagyobb forrásszükségletű eljárás, hiszen tömérdek számítást igényel, ezáltal sok időt is vesz igénybe. A képzés általában egy kétciklusú (előképzési és finomhangolási) mechanizmusra bontva történik, utóbbi a modellfejlesztési ciklusban is végrehajtható.
6. A modell ellenőrzése *(model checking)* a teljes fejlesztési ciklus során gyakori szükséglet, hiszen a kiemelkedő erőforrás-felvétel megindokolja a folyamatok helyes működéséről való rendszeres meggyőződést, így a modell tanítása közben és után is ellenőrzik a modell teljesítményét, valamint igyekeznek elkerülni a túltanulás *(overfitting)*[11] állapotát.
7. A modell alkalmazhatósága vagy a használhatóságáról *(model usability)* való meggyőződés során megvizsgálják, hogy mennyire hatékony a gyakorlati alkalmazásokban. Ez a lépés magában foglalja annak értékelését, hogy a modell milyen jól teljesít azokon a feladatokon, amelyekre tervezték.
8. A ciklus zárásaként, a folyamatban feltárt információkra alapozva lehetőség nyílik a modell fejlesztésére *(model enhancement)*. Miután a modell használhatóságát tesztelték, lehetőség van a továbbfejlesztésére, például több adat hozzáadásával további finomhangolás *(fine tune)* elvégzésére, a módosítható paraméterek utólagos módosítására, annak érdekében, hogy a modell teljesítménye tovább javuljon.

A képzési adatkészletek

Az eddigiekben több alkalommal lett érintve, hogy a képzéshez a jelentős szöveges tartalmat biztosító adatkészlet vagy korpusz *(corpus)* egyfajta fundamentum. Ebben a fejezetben rövid bemutatás következik az alkalmazható adatokhalmazok általános típusairól és forrásaikról.

Az alapvető források közé tartoznak:

- Nyilvános adatkészletek *(public datasets)*. Különféle forrásból származó, szabadon hozzáférhető adathalmazok, amelyeket leggyakrabban tudományos intézmények vagy kormányzati szervek osztanak meg nyilvánosan (például weboldalak, könyvek, cikkek). Előnyük a sokféleségükben és méretükben rejlik.[12]
- A tartományspecifikus adatkészleteket *(domain-specific datasets)* egy adott területre vagy iparágra szabták, hiszen úgy lettek összeállítva, hogy tartalmazzák a területre

[9] A tanítóanyag azon részhalmazára, amelyet egyszerre fel tud dolgozni a modell, egy tételként *(batch)* hivatkozunk.

[10] Amikor a modell képzése során az a teljes tanítóanyagon egyszer végighalad, azt egy korszaknak *(epoch)* jelöljük.

[11] Az overfitting, magyarul túltanulás vagy túlilleszkedés egy nem optimális, de gyakori jelenség a gépi tanulás során, *beleértve* a nagy nyelvi modellek képzését is. A modell túlságosan „ráilleszkedik" a tanítóadatra, beleértve annak hibáit is. Ennek eredményeképpen a modell nagyon jól teljesít a validálási és tesztadatokkal végzett értékelések során, de amikor olyan feladat végrehajtására alkalmazzuk, amelyre a tanítóadatban nem látott példát, a modell teljesítménye jelentősen romlik.

[12] Chawre 2023.

jellemző egyedi nyelvi mintákat és terminológiát. A finomhangolás során leginkább alkalmazott adatkészlet, hiszen ezzel javítható a nyelvi pontosság olyan egyedi tématerületeken, mint például a jog, az orvostudomány vagy a pénzügy.[13]

- Felhasználói tartalmakból összeállított adatkészlet *(user-generated contents)* a közösségi médiában megjelent bejegyzésekből, fórumbeszélgetésekből, termékismertetőkből, blogbejegyzésekből származó, változatos nyelvi stílust és kifejezést tartalmazó összeállítást jelent. Hatalmas mennyiségével biztosítja az LLM-ek számára a folyamatosan frissülő adatkészletet, valamint a naprakész információkat és nyelvi formátumokat.[14]
- Liszenszelt korpuszok *(licensed data corpora).* Megbízható forrásból származó, strukturált adatgyűjtemény, amelynek használatát legalább kétoldalú megállapodás szabályozza. Leginkább kiadóktól és adatszolgáltatóktól szerezhetők be, szövegeket, képeket, hangfelvételeket tartalmaznak.[15] A képzés szempontjából értékesek és minőségiek, és a szerzői jogok tekintetében garantálják a jogbiztonságot, ugyanakkor felhasználásuk költséges és korlátozott.[16]
- Kódtárak *(code repositories).* Programozási forráskódok gyűjteménye, valamint az ehhez fűződő dokumentumok és egyéb megjegyzések széles köre, amelyek leginkább olyan felületen érhetők el, mint például a GitHub,[17] GitLab[18] és Bitbucket.[19] A kódtárak elemzésével az LLM-ek megtanulják a programozással kapcsolatos szövegezés megértését és generálását, így jártasságot szerezve a szoftverfejlesztés (például *text to code*[20] feladatok) területén.[21]
- Szintetikus adatkészlet *(synthesized datasets).* Technikai megoldással létrehozott adathalmaz, amely során mesterséges adatokat állítanak elő olyan esetekben, amikor a természetes adatok szűkösek, érzékenyek, vagy elérésük költséges. Létrehozásukhoz olyan algoritmusokat alkalmaznak, amelyek a valós adatok jellemzőivel megegyező tartalmat állítanak elő. Előnyük van adatvédelem, méretezhetőség és sokszínűség tekintetében, azonban nem mindig valósághűek, a generáló algoritmusok fejlesztése és finomhangolása időigényes.[22]

Az LLM-ek képzési adatkészletei általában minden fentebb felsorolt csoportból tartalmaznak legalább egy típusú forrást, de a források összetételét leginkább az határozza meg, hogy milyen célú felhasználásra tervezték a modellt, mert előzetesen ennek alapján tervezik és szervezik össze a képzési adatkészletet is (1. táblázat).[23]

---

13 Chawre 2023.
14 Chawre 2023.
15 Ilyenek angol nyelven a Corpus of Contemporary American English (COCA), vagy a British National Corpus (BNC), magyar nyelven a Magyar Nemzeti Szövegtár (MNSZ), továbbá egyéb digitális könyvtárak vagy könyvtári adatbázisok.
16 Chawre 2023.
17 GitHub. Lásd: https://github.com/
18 GitLab. Lásd: https://gitlab.com/
19 Bitbucket. Lásd: https://bitbucket.org/
20 A *text to code* gyűjtőnévvel hivatkoznak azon feladatok körére, amikor a modellek természetes nyelven kiadott emberi utasítások alapján programozási forráskódokat állítanak elő.
21 Chawre 2023.
22 Chawre 2023.
23 Bottyán 2024: 43.

1. táblázat: A LLaMa modell alaptanítása (pre-training) alatt alkalmazott tanítóanyag összetétele és felhasználása

Adatkészlet	Mintavétel (%)	Korszakok	Méret (GB)
CommonCrawl	67,0	1,10	3,3
C4	15,0	1,06	783
Github	4,5	0,64	328
Wikipedia	4,5	2,45	83
Books	4,5	2,23	85
ArXiv	2,5	1,06	92
Stack Exchange	2,0	1,06	78

Forrás: Touvron et al. 2023: 2.

Általánosságban elmondható – de a zavarosabb adatkészletek esetében szükségszerű –, hogy a képzési adatokat felkészítésnek vetik alá: átalakítják, osztályozzák, tokenizálják, tisztítják, deduplikálják, pontozzák és priorizálják, illetve elvetik az alacsony minőségű adatkészletet. A folyamat előkészítésének részeként a modell működési célját tekintve kiválasztják a legcélszerűbb és/vagy a legminőségibb adatkészletet, és ennek megfelelően bontják fel azt a képzési folyamatban úgy, hogy az adatkészlet változatossága azért megmaradjon.[24]

Az előképzés

Az előképzés vagy alapképzés *(pre-training)* során súlyozódnak be a képzetlen modell paraméterei annak érdekében, hogy a megismert minta (például az előző tokenek sorozatának szekvenciája és a kontextus jelentésének reprezentációja) alapján sikerrel jelezze elő a soron következő tokent. A nagy nyelvi modellek képzési folyamatára általánosságban felügyelet nélküli tanulásként hivatkozunk, hiszen előzetesen nem kap definiált kimenetet, azonban a modell architektúrájának perspektívájából ez egy úgynevezett *önfelügyelt tanulás,* hiszen a predikciót követően a tanulóanyagtól megkapja a jó választ (a soron következő helyes tokent), majd az esetleges hibás predikciót követően újrakalibrálódnak a szükséges paraméterek.[25] Az előképzési folyamat végén, a modellel elért teljesítményre a validációs veszteség (*lm loss value),*[26] valamint a perplexitás *(lm loss ppl)*[27] mérőszámaival hivatkoznak.[28]

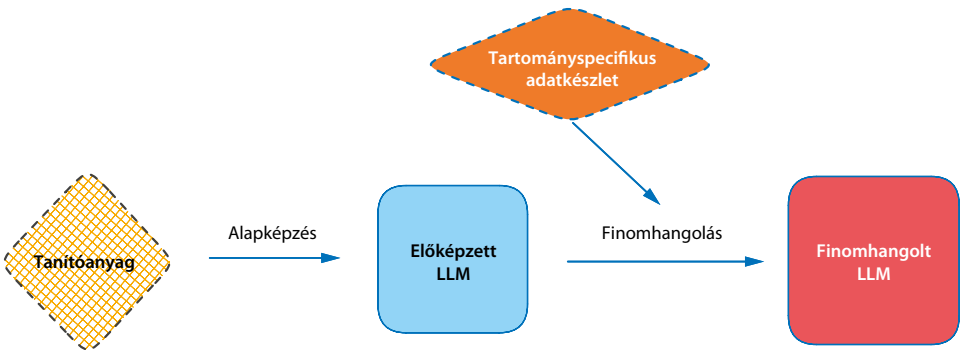
A nyilvánosan elérhető nagy nyelvi modellek gyakorta elő vannak tanítva, hiszen a természetes nyelvek alapvető szekvenciális kapcsolatai és kontextusbeli jelentései azonosak a korpuszokban, így azt nem szükséges újra végrehajtani. Egy adott modell nulláról történő betanítása csak abban az esetben válhat szükségessé, amennyiben azt olyan

[24] Bottyán 2024: 43.
[25] Drost 2023.
[26] A nyelvi modell tanítása során mért veszteség azt méri, hogy mennyire jól teljesít a modell a következő token előrejelzésében.
[27] A perplexity az *„lm loss value"* exponenciális transzformációja, és azt mutatja, hogy átlagosan hány lehetőséget vesz figyelembe a modell, amikor a következő token előrejelzésén dolgozik. Az alacsony ppl érték jobb modellteljesítményt jelez, mivel a modell kevesebb lehetőséget kezel.
[28] Yang Zijian et al. 2023: 7.

speciális feladatra szükséges tanítani, amelynek tanítóanyaga[29] eltér a természetes nyelvi struktúrától és jellemzőktől.

A finomhangolás

A finomhangolás során az előképzett modell további tanítása speciális adatkészlet felhasználásával történik, amely az alapképzésnél felhasznált korpuszoktól kisebb, azonban specifikus (tartományspecifikus) adatkészlettel igyekszik a modellt a célfeladat nyelvi környezetével és jellemzőivel felvértezni. E képzési folyamat (2. ábra) során csak az architektúra utolsó rétegeiben található paraméterek újrakalibrálása történik meg, ezáltal a képzési erőforrások töredékét igényli és gyorsabban is végrehajtható. Itt meg kell említeni a finomhangolás egy alkalmazott speciális esetét, az emberi visszacsatolású megerősített tanulást *(reinforcement learning from human feedback),* amely során a modellt arra konfigurálják, hogy emberi csevegéshez hasonló eredményt produkáljon (például ChatGPT), és ehhez valós emberi visszajelzéseket vesznek alapul.

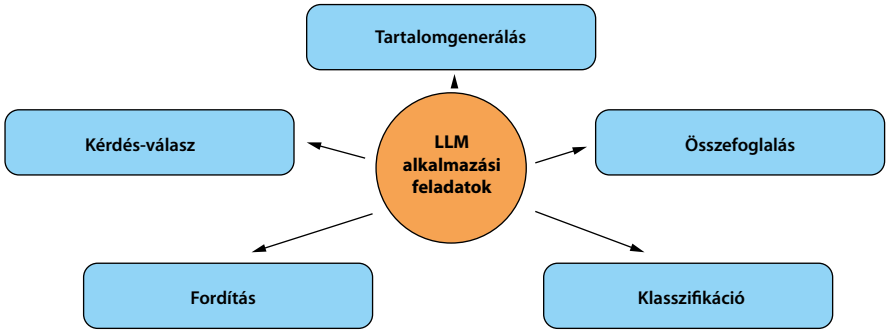


2. ábra: A finomhangolás folyamata
Forrás: a szerző szerkesztése

Alkalmazhatóság

A generatív mesterséges intelligenciák közül az LLM jelentős hatást gyakorol a szociális (például politika, tudományos kutatások, pszichológia stb.) és a gazdasági folyamatokra (például média, marketing, oktatás, szoftverfejlesztés, gyógyszeripar, orvosi tevékenységek, építési technológia) egyaránt.[30] Ezeken a területeken leginkább különböző ügynökként *(agent)* alkalmaznak LLM-képességeket, amelyek a feladatra tervezett és illesztett

[29] Ilyenek lehetnek például a programozási nyelvek, DNS-adatok, matematikai formulák, kémiai szerkezetek stb.
[30] Wang et al. 2024: 13–17; Hadi et al. 2025: 4–5.



3. ábra: A nagy nyelvi modellek főbb alkalmazási területei
Forrás: a szerző szerkesztése

keretrendszerekben kapnak helyet. A szövegalapú *(text-based)* tartalmak tekintetében az alábbi főbb feladatokban (3. ábra) alkalmazzák azokat:

- *Kérdés-válasz tevékenység (question-answer, QA).* Az alapképzést követően kifejezetten kérdéseket és válaszokat tartalmazó korpusszal finomhangolt LLM-ek eredményességüknek köszönhetően megkerülhetetlenné váltak a QA-rendszerekben. A betanított adatok mellett a figyelemmechanizmusnak és kontextusmegértésnek köszönhetően a kérdésekre nagy pontosságú válasz szintetizálható. Erre a képességre alapozva sikeresek chatbot és asszisztencia jellegű felhasználásban.[31]
- A *tartalomgenerálás* (például történetek, marketingtartalmak, blogtartalmak, bulvár- vagy kutatási cikkek, közösségimédia-tartalmak, termékleírások, programozási forráskódok, e-mailek stb.) hasznos alkalmazási módja az LLM-rendszereknek. Erre a képességre alapozva további automatizált ügynökök (például asszisztencia-alkalmazások) hozhatók létre.
- A hosszú szöveges tartalmak (például hírek, jelentések, értekezletek jegyzőkönyveinek, jogi dokumentumok stb.) koherens *összefoglalása* szintén fontos és előnyös tulajdonsága a nagy nyelvi modelleknek. A gyors és lényegi információkinyerés kulcsfontosságú lehet olyan keretrendszerek megalkotásában, ahol jelentős mértékben történik információfelvétel, továbbá ezzel összefüggésben gyors és hatékony feldolgozás válik szükségessé.
- A *szövegosztályozást* avagy *klasszifikációt* igénylő feladatokra automatizált keretrendszerekben szintén hatékony az LLM modell, hiszen előre meghatározott jellemzők szerinti tartalomelemzés és kategorizálás hatékonyan képes hozzájárulni olyan speciális feladatok eredményességéhez, mint például a nyelvazonosítás, a szentimentelemzés, a spam-szűrés, a tartalommoderálás vagy az ügyfélvisszajelzések elemzése.
- A természetes nyelvek közötti *fordításban* is eredményes annak okán, hogy a beágyazás következtében a különböző nyelvek közötti fogalmak által felvett vektorértékek között hatékonyan kimutathatók a kapcsolatok. Ennek köszönhetően kivételes pontossággal képes egyik nyelvről a másikra fordítani szöveges tartalmat.[32]

[31] Lásd: https://www.nvidia.com/en-us/glossary/large-language-models
[32] Hadi et al. 2023: 19–20.

Az eltérő célok szerint alkotott LLM-architektúrát alkalmazó szoftvereknek természetesen differens jellemzői is vannak, azonban magában az LLM-architektúrában és a hozzá tartozó külső kapcsolatokban megfigyelhetők olyan tulajdonságok (például erősségek, gyengeségek, lehetőségek, fenyegetések), amelyek azonosíthatók heterogén alkalmazási formulákban. E jellemzők együttes feltárására kiváló eszköz a SWOT-analízis.[33]

Nagy nyelvi modellek SWOT-analízise

A tanulmányban több helyen említettük a nagy nyelvi modellek komplexitását, így természetesen tulajdonságaik és jellemzőik áttekintése is összetett megközelítést igényel. A szakirodalmi bázisban az ilyen témákat feldolgozó tanulmányok gyakoriak, hiszen a technológia alkalmazásával járó kockázatok feltárása népszerűnek mondhatók. Yupeng Chang és munkatársai tanulmányukban[34] vizsgálták az LLM gyengeségeit és erősségeit, Muhammad Usman Hadi és munkatársai két hasonló tanulmányukban[35] pedig az alkalmazással járó kihívásokat és limitációkat járták körbe. Az általuk tett megállapítások felhasználásával, valamint az eddigiekben bemutatott ismeretanyag felhasználása alapján a szerző egy SWOT-analízisben összegezte azokat.

2. táblázat: Nagy nyelvi modellek SWOT-analízise

	NAGY NYELVI MODELLEK SWOT-ANALÍZISE	
	Erősségek *(strengths)*	**Gyengeségek** *(weaknesses)*
Belső tényezők	• Döntéstámogatás • Folyamatos fejlődés • Folyékony, koherens szövegalkotás • Fordítási képesség • Kiváló NLP teljesítmény • Kontextuális megértés • Nyelvi megértés • Összefoglalás • Programozási nyelvek kezelése • Szövegosztályozás • Tartalomgenerálás • Többnyelvű alkalmazás	• Adatszükséglet, adatfüggés és toxicitás • Aritmetikai és logikai következtetés • Információszivárgás • Gyenge NLI*-teljesítmény • Hallucináció és hiteltelenség • Jelentős erőforrás-felhasználás, költség és képzési időigény • Jelentős válaszidő • Kiberbiztonsági sebezhetőség • Kontextuális információhiány • Korlátozott ismeretkezelés • Korlátozott tudásfrissítés • Nehéz értelmezhetőség • Nem optimális környezet • Összetett kontextusértelmezés

[33] A SWOT-analízis egy stratégiai tervezési eszköz, amely egy szervezet erősségeit *(strengths)*, gyengeségeit *(weaknesses)*, lehetőségeit *(opportunities)* és fenyegetéseit *(threats)* vizsgálja, hogy átfogó képet nyújtson a belső és külső tényezőkről.

[34] Yupeng Chang et al. 2023.

[35] Hadi et al. 2025.

	NAGY NYELVI MODELLEK SWOT-ANALÍZISE	
	Lehetőségek *(opportunities)*	**Fenyegetések** *(threats)*
Külső tényezők	• Diszruptivitás • Energiaigények csökkentése • Felhasználók bizalmának erősítése • Forrásfelhasználás-csökkentés • Globális szerepvállalás • Komponensként alkalmazás • Multifunkcionalitás • Szabályozás • Szabványosítás	• Gyors elévülés • Etikai problémák • Polgári jogi fenyegetés • Szabályozási kihívás • Társadalmi megítélés • Kibertámadási fenyegetettség • Szintetikus adatok terjedése

*Megjegyzés: * NLI (natural language inference), azaz természetes nyelvi következtetés. Az NLI egy olyan folyamat vagy feladat, amely során a rendszer megpróbálja megállapítani, hogy egy adott állítás logikailag következik-e egy másik szöveges állításból, ellentmondásban áll-e vele, vagy semleges viszonyban van vele.*

Forrás: a szerző szerkesztése

Erősségek (strengths)

Jelentős mennyiségű információ rendelkezésre állása esetén az LLM-ek hasznosak a döntéstámogatásban, hiszen a modellek képesek hatékonyan meghatározni, hogy egy adott kontextusban mely válasz vagy akció a legvalószínűbb. Azonban e mögött nem reális döntéshozatal rejlik, hanem egy mintafelismerés, amelyben a leggyakoribb választ fogalmazzuk meg az összefüggések figyelembevételével. Továbbá a modellek rendkívül eredményesek a folyékony, természetes nyelvű, koherens szövegalkotásban (például tartalomkészítés, párbeszédek alkotása), valamint a szöveges tartalom különböző részei közötti összefüggések alapján végzett következtetésben, amely biztosítja a kontextuális megértés (például kivonatolás) képességét is. A klasszikus NLP képességeik (szemantika, szintaktika, szentimentelemzés, entitásfelismerés, kérdés-válasz stb.) erősségként listázhatók, de egyéb nyelvi feldolgozási feladatokban (nyelvi fordítások) is kiválóak, jól teljesítenek a programozási nyelvek feldolgozásában és generálásában *(text to code)*. Ide sorolható a modellek többnyelvű alkalmazásának lehetősége, hiszen a több természetesen nyelvet tartalmazó tanítóadatnak köszönhetően számos nyelven utasítható, és a megtanult kontextusbeli jelentések fordíthatók a kívánt modell által ismert nyelvre. A gépi tanulás és a nagy nyelvi modell mint technológia fejlesztése az utóbbi években rendkívüli iramot diktál, rendszeresen újabb variánsok jelennek meg, így biztosítva a folyamatos fejlődést. A megújulás folyamatosan indukálja az új felhasználási opciók megjelenését, aminek köszönhetően az alkalmazási lehetőségek köre is bővül.

Gyengeségek (weaknesses)

Az analízisben a gyengeséghez sorolható tulajdonságok egyértelműen számbeli többségben vannak a többi rendszerezett jellegzetességhez képest. Elsőként, bár a legfrissebb modellek egyre jobb eredményeket érnek el az NLI-teljesítményben, ide kell sorolnunk

az emberi ellentmondások nehézkes kezelését (például nem racionalitáson alapuló véleménykülönbségek azonosítása). Korlátozott képességként szintén ide sorolandó a szöveges tartalmakban megtalálható események közötti szemantikai hasonlóság és az absztrakt gondolkodás felismerése, valamint az összetett kontextus értelmezése.[36] Szintén kritikus aspektus a kontextuális információ hiánya, hiszen amennyiben a modell nem rendelkezik kellő mennyiségben feldolgozható információval (például „gondolatláncolattal" megalkotott prompt), a szemantikai elemzések teljesítménye alulmarad az elvárttól.

Közismert tény a nagy nyelvi modellek „hallucinálása", vagyis, hogy valótlan vagy pontatlan információkat szolgáltatnak leggyakrabban annak okán, hogy megpróbálják áthidalni az ismerethiányból eredő korlátokat. A modellek nem rendelkeznek tényleges és teljes körű „tudással" a világról, hanem statisztikai minták alapján hoznak létre válaszokat, így amennyiben olyan kérdéssel találkoznak, amelyhez nincs a tanítóadaton nyugvó, releváns és megalapozott ismeret, a valószínűségszámításon alapuló válaszadás nem feltétlenül lesz minden esetben igaz. A hallucináció oka összetett probléma, amely az architektúratípussal, a tanítóadattal és a tanítási folyamattal egyaránt összefügg.[37]

Az LLM egyik alapköve a tanítóanyag, ezáltal a képzés sikeressége függ a felhasznált adatok mennyiségétől és minőségétől. Tekintve, hogy a modellképzés során hatalmas mennyiségű tanítóanyag összeállítása, áttekintése, értékelése és előkészítése szükséges, ez komoly kihívást jelent. Hasonlóan a tanítóadatból ered a hiteltelenség problémája is. A téves vagy ellentmondásos információkat tartalmazó képzési adat nem befolyásolja a működést, azonban a modell nem képes különbséget tenni az igaz és hamis információk között, így előfordulhat, hogy valótlan információt használ fel a válaszadás során. Továbbá, amennyiben a tanítóadatban káros tartalom (például elfogultság, gyűlöletbeszéd, előítélek vagy más káros információ) jelenik meg, annak feldolgozása esetében sajnos a modell képes ugyanilyen jellemzőkkel bíró generatív eredményt produkálni (toxikus működés). Ezek alapján az LLM által szolgáltatott információ nem tekinthető teljes mértékben megbízható, hiteles forrásnak. E mellett egyértelmű, hogy a tanítóanyagként összeállított óriási adathalmazt manuálisan ellenőrizni lehetetlen, így a tisztításokat követően is tartalmazhatnak bizalmas információkat (például személyes adatokat). Ez a modellműködés során adatvédelmi szivárgásokhoz vezethet, véletlenszerűen vagy a rosszindulatú prompttevékenységeknek köszönhetően egyaránt.

Valós tapasztalás az is, hogy a nagy nyelvi modellek aritmetikai és logikai következtetési képességei erősen korlátozottak. A szöveges korpuszokon végzett tanítási folyamat és a modellek működése nem matematikai műveletek végrehajtására lett tervezve és optimalizálva. A modellek a szöveg alapján próbálnak mintákat felismerni, de nem rendelkeznek olyan explicit matematikai képességekkel, mint egy erre tervezett algoritmus.

A nagy nyelvi modellek képzése és működtetése jelentős és optimalizált számítási kapacitást biztosító infrastruktúrát igényel, ami nehezen biztosítható követelmény, és amelynek hiányában az alapjaiban is időigényes folyamatok az eredménytelenség mellett jelentős pénz- és energiapazarlással járhatnak.[38] Ugyanakkor, a modellek újratanítása szintén költséges folyamat, és rendszeres gyakorisággal nem fenntartható. Bár bizonyos architektúrák

[36] Bottyán 2024: 60.
[37] Greene 2022.
[38] A jelenséggel járó kockázatok elkerülésére már számos technikai megoldás létezik, például a *Parameter-Efficient Fine-Tuning, Low-Rank Adaptation (LoRA), LongLora* avagy a *QLora*.

esetében léteznek technikák a modellműködés módosítására, azonban ezeknek csak korlátozott lehetőségei vannak, így ebből a szempontból a működés limitáltnak tekinthető. Illetve a megfelelő konfigurációs beállítások meghatározása leginkább csak tapasztalati úton, próbálkozásokkal határozható meg, ami szintén jelentős erőforrás-felhasználással jár. További hátrány a nagy memóriafelhasználásból és számításikapacitás-igényből adódó hosszú válaszidő is.[39]

A nagy nyelvi modellekkel kapcsolatosan elmondható, hogy azok működése nehezen magyarázható és értelmezhető, nem szakértő személyek számára kihívást jelent az ezzel kapcsolatos ismeretek elsajátítása. Működése a társadalom jelentős részének egyfajta misztikum, ez nehezíti a technológia térnyerését és az azzal kapcsolatos felelősségvállalást és etikus alkalmazást. Korlátozott ismeretkezelés: az alaptanítással képzett modellek szakmai tudást igénylő tartományi (például jog, egészségügy stb.) felhasználás esetében finomhangolás nélkül nem eredményesek, ennek okán nehéz generális feladatokra hatékony modellt létrehozni. Emellett a promptok kétértelműsége és a logikai műveletek megértésével kapcsolatos belső korlátok miatt fellépő következtetési hibák okán komplex tervkészítési feladatokban nem kellően eredményesek a modellek.

Lehetőségek (opportunities)

A nagy nyelvi modellek lehetőségei nem csupán a technológia önálló fejlődéséből erednek, hanem olyan külső tényezőkből is származtathatók, amelyek hatással vannak annak alkalmazására. Amennyiben sikerül azon területeken fejlődést elérni, amelyek kedvezően befolyásolják a gépi tanulási környezeteket, az hozzájárulhat az LLM felhasználási gyakoriságának növeléséhez. A nagy nyelvi modellek gyengeségei közé sorolt energiaigények valóban hátráltatják a technológia térnyerését, azonban manapság számos kutatás igyekszik az adatközpontok energiaellátását csökkenteni. A környezetbarát megoldásokra való törekvés mellett az adatfeldolgozás, a mesterséges intelligencia és a fenntartható technológiák összekapcsolása jelentős előrelépést hozhat az LLM-ek széles körű alkalmazásában. Az újgenerációs mobilhálózatok (például 5G) és egyéb jövőbeni hálózati technológiák terjedése lehetővé teszi az LLM-ek valós idejű alkalmazását olyan területeken is, ahol korábban a sávszélesség vagy a késleltetés problémát jelentett.

A multifunkcionalitásnak köszönhetően felhasználása egyre népszerűbb, napjainkban az LLM-képességeket komponensként gyakorta integrálják különböző szoftverekbe, amely megoldások köre folyamatosan bővül. Továbbá eredményei okán diszruptív, hiszen új perspektívákat nyit meg az eddigi alkalmazott eljárásokban (például adatok kezelése, ügyfélszolgálati chatbot, automatikus fordítások), valamint forradalmasíthatja, felválthatja azokat. Modularitásának köszönhetően különböző technológiákkal bővíthető, ami tovább növeli a felhasználási lehetőségek körét. A nagy nyelvi modellek nem csupán a természetes nyelv feldolgozásának hatékonyságát javítják, hanem az automatizálás és az intelligens rendszerek fejlődését is támogatják. Ezen túlmenően az LLM-ek különösen

[39] Ehhez kapcsolódóan meg kell említeni, hogy bizonyos feladatügynökök több ciklusban hajtanak végre LLM-lekérdezéseket, az így felhalmozódó reakcióidő már számottevő. A jelenséget már speciális technikai megoldások (pl. kvantálás, *efficient attention, multi-attention query* stb.) alkalmazásával próbálják csökkenteni.

hasznosnak bizonyulhatnak a globális együttműködések terén. A nemzetközi szereplők közötti kommunikáció megkönnyítésével, a különböző nyelveken végzett automatizált fordításoknak köszönhetően segíthetik a globális szintű kapcsolatok (kereskedelem, gazdasági együttműködések) hatékonyságának növelését.

Nemzetközi szabványok (pl. ISO/IEC 42000 szabványcsalád) és a kapcsolódó jogi szabályozók (például AI Act) alkalmazásának elterjedése szintén pozitív hatással lehet az LLM-ek fejlődésére, az adatbiztonság és a magánélet védelmének e téren való érvényesítésére. Az egységes szabályozás elősegíti a technológia biztonságos és etikus alkalmazását, ami közvetetten hozzájárul ahhoz, hogy a felhasználók bizalommal forduljanak ezekhez a technológiákhoz.

Fenyegetések (threats)

Az LLM-re ható fenyegetések köre sokrétűnek mondható, azonban a legpotenciálisabb külső fenyegetés a rosszindulatú, a modell működését manipuláló vagy megakadályozó kibertámadások megvalósítása. Evidens, hogy a sebezhetőségek számának mennyisége a nyilvános kapcsolattal ellátott keretrendszerekbe foglalt LLM-ek esetében számottevőbb, mint lokálisan futatott modellek esetében. A kiberfenyegetések közül a prompt injection[40] típusú támadást jegyzik a leginkább, hiszen a modellek érzékenyek a promptokra, különösen a rosszindulatú promptokra. Ilyen műveletekkel nagymértékben manipulálható a modellek működése és kimenetkezelése egyaránt, azonban olyan további támadástípusokat is meg lehet említeni, mint a szolgáltatásmegtagadás-támadás,[41] a modelleltulajdonítás,[42] a tanítóadat-mérgezés,[43] az ellátási láncot célzó támadások[44] köre, és más egyéb ide sorolható módszerek. A nagy nyelvi modellek elektronikus információbiztonsági sebezhetősége valóban számottevő gyengeségi jellemző, így az azok kihasználására megjelenő rosszindulatú tevékenységek köre is számottevő és változatos. A téma górcső alá vétele jó eséllyel egy önálló tanulmány terjedelmét is felölelné, így ennek okán a további kibertámadási fenyegetések részletezésétől el kell tekintenünk.

Emellett az LLM-ek esetében a felhasznált tanítóanyaggal kapcsolatos szerzői és tulajdonjogi tárgyban indított polgári peres keresetek kimenetele eléggé bizonytalan. Amennyiben a képzési és működési eljárások alatt alkalmazott gyakorlatok nem kerülnek jogi szabályozás alá, számítani kell ilyen jellegű nehézségekre. Általánosságban elmondható, hogy a jelenleg alkalmazott tanítóanyagok jelentős részre webes tartalmakból összegyűjtött nyílt forrású adat. Az ilyen adathalmazzal végzett tanítások a későbbiekben

---

40 A prompt injection során a felhasználó vagy másik program úgy manipulálja a bemeneti parancsot vagy utasítást (a promptot), hogy a rendszer nem várt vagy nem kívánt műveleteket hajtson végre. Ez különösen releváns az LLM modellek esetében.

41 Angolul denial-of-service attack (DoS). A támadók nagy mennyiségű hálózati forgalommal árasztják el az LLM infrastruktúráját, ami a rendelkezésre állás megszűnéséhez vezet.

42 Angolul: model theft. Egy modell kifejlesztése rendkívül költséges, így valós fenyegetés irányul annak lemásolására.

43 A tanítóadatok rosszindulatú módosítása jelentősen befolyásolja a modell működését. Dezinformációs célok érvényesíthetők, akár hátsó kapuk (backdoor) hozhatók létre a modell manipulálására.

44 A fejlesztési ciklus során megjelenő, vagy az üzemeltetési fenyegetések érvényesítése során végrehajtott modellkompromittálás.

fellépő adatszivárgás esetén az adatgyűjtési eljárással és az adatok védelmével kapcsolatos olyan etikai problémákat hozhatnak a felszínre, amelyek akár könnyen jogi aktusokká fejlődhetnek. Az LLM-ek vonatkozásában is tény, hogy a fejlődésük okozta társadalmi hatásokkal a jog ereje nem bír lépést tartani, így a szabályozatlanságból eredő problémák fenyegetésként jelentkeznek. A webes tartalmakra visszatérve említendő az is, hogy a generatív mesterséges intelligenciák megjelenése óta a tanítóanyagként felhasználható, nyíltan elérhető szöveges tartalmak egyre nagyobb része szintetikus adat. A mesterségesen előállított szöveges tartalom nem tartalmazza azon természetes nyelvi sajátosságokat, amelyek a nagy nyelvi modellek további eredményes fejlesztéséhez szükségesek, ennek eredményeképp az így létrehozott szövegek gyarapodására fenyegetésként tekinthetünk.

Említeni kell még az MI-k társadalmi megítélésével kapcsolatos nehézségeket. A technológia nehezen értelmezhető, és társadalmi elfogadása még kialakulóban van, ebből kifolyólag a társadalom tagjai úgy ítélik meg megjelenését, mint ami veszélyezteti az emberek munkahelyeit. Számolni kell a technológia rosszindulatú felhasználásának kockázatával is, hiszen a nyílt forráskódú modellek esetében bárhogyan, hostolt modellek esetén a biztonsági védelem megkerülésével rosszindulatú célokra (például információgyűjtésre, dezinformációs tartalmak generálására, kibertámadásokra) is alkalmazható. Mindemellett a már említett rendkívül gyors ütemű fejlődésnek köszönhetően a legújabb modellek folyamatos fejlesztés és frissítés nélkül, bár képességeik tekintetében állandók, eredményeik tekintetében elavultnak számíthatnak rövid időn belül.[45]

Összefoglalás

Az összeállított ismeretanyag tekintetében megállapíthatjuk, hogy amennyiben valamely szervezet saját nagy nyelvi modell képzése, vagy bármely egyéb modellvariánst alkalmazó informatikai keretrendszer bevezetése mellett dönt, mindenféleképpen a szervezeti adatvagyon felmérése, valamint az azzal összefüggő adatgazdálkodási rendszer kialakítása az elsődleges feladata. Azonban emellett a modellek fenntarthatósága nagyban függ a fejlesztési ciklus rendszeres ismétlődésétől is. Egyrészt az erősségeket felhasználó és a lehetőségeket kihasználó fejlesztési szemlélet biztosítja a rendszeresen megújuló eredményességet, másrészt a modellt külsőleg fenyegető veszélyeket, valamint annak belső tulajdonságai között megjelenő gyengeségeket ciklusonként értékelve és kockázatokként kezelve biztosítható a nagy fokú rendelkezésre állás mellett az etikus és felelős használat.

A szervezeti adatvagyontól a generált szervezeti adat létrejöttéig számos feltételnek és folyamatnak kell teljesülnie, azonban a tanulmányban feltárt alapelvek és megállapítások figyelembevételével a modellek hatékonyan alkalmazhatók a szervezeti tevékenységekben. Amennyiben a nagy nyelvi modellek generatív képességét egy szervezet képes felelősen a saját szolgálatába állítani, az a hozzáadott érték mellett velejáróként alakítja a szervezet mesterségesintelligencia-kultúráját is.

A LLM-fejlesztésben jelenleg tapasztalt legfőbb irányok (például erőforrás-felhasználás szempontú architektúraoptimalizálás, kompakt modellek, multimodalitás stb.) egyértelműen annak hátrányainak és hibáinak felszámolására is törekednek amellett,

[45] Bottyán 2024: 62.

hogy a legkívánatosabb cél továbbra is a legeredményesebb modellek létrehozása. Ezt a jövőt vetíti elénk az a közelmúltban megjelent hír is, amely során az OpenAI vállalat bejelentése alapján o3 modelljük bizonyos teszteken egy átlagos ember eredményszintjét érte el. Amennyiben hitelesnek tekinthetjük a vállalat által közölt információkat, ez az elért eredmény azt sugallja, hogy sikerült létrehozniuk egy rendkívül alkalmazkodóképes modellt.[46] Erre a tapasztalásra alapozva, valamint arra, hogy egyre több technikai megoldás (például RAG[47], RIG[48] stb.) igyekszik az LLM hatékonyságát még tovább növelni, kijelenthető az a megállapítás, hogy napjainkban a nagy nyelvi modellek jelenlegi teljesítményértékei és felhasználási területei nincsenek kőbe vésve, és a következő időszakokban magasabb szintű eredményekre, az ezzel együtt járó hatásokra számíthatunk.

Felhasznált irodalom

Bennett, Michael T. – Perrier, Elija (2024): OpenAI Claims Its New Model Reached Human Level on a Test for 'General Intelligence.' What Does That Mean? *Gizmodo,* 2024. december 29. Online: https://gizmodo.com/openai-claims-its-new-model-reached-human-level-on-a-test-for-general-intelligence-what-does-that-mean-2000543834?utm_source=fark&utm_medium=website&utm_content=link&ICID=ref_fark

Bottyán Sándor (2024): *Nagy nyelvi modellel támogatott nyílt forrású információgyűjtés a kibertérben*. Tudományos diákköri dolgozat. Budapest: Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar.

Brown, Tom B. – Mann, Benjamin – Ryder, Nick – Subbiah, Melanie – Kaplan, Jared – Dhariwal, Prafulla – Neelakantan, Arvind – Shyam, Pranav – Sastry, Girish – Askell, Amanda – Agarwal, Sandhini – Herbert-Voss, Ariel et al. (2020): *Language Models are Few-Shot Learners*. Online: https://doi.org/10.48550/arXiv.2005.14165

Chawre, Huzefa (2023): Prominent Data Collection Methods and Tools for LLMs. *Turing,* 2023. november 21. Online: https://www.turing.com/resources/data-collection-methods-and-tools-for-llms

Drost, Dorian (2023): Different Ways of Training LLMs. *Towards Data Science,* 2023. július 21. Online: https://towardsdatascience.com/different-ways-of-training-llms-c57885f388ed

Greene, Jenna (2022): Will ChatGPT Make Lawyers Obsolete? *Reuters,* 2022. december 9. Online: https://www.reuters.com/legal/transactional/will-chatgpt-make-lawyers-obsolete-hint-be-afraid-2022-12-09/

Hadi, Muhammad Usman – Al-Tashi, Qasem – Qureshi, Rizwan – Shah, Abbas – Muneer, Amgad – Irfan, Muhammad – Zafar, Anas – Shaikh, Muhammad Bilal – Akhtar, Naveed – Al-Garadi, Mohammed Ali – Hassan, Syed Zohaib –

[46] Bennett–Perrier 2024.

[47] A Retrieval-Augmented Generation megoldás egy kimenetoptimalizálási folyamat, amely során a generatív folyamatokba szándékos beavatkozás történik. A válaszgenerálás előtt a képzési adatokon kívül egy hiteles tudásbázist (pl. adatbázisok és dokumentumok) is felhasznál a modell, ezáltal kiterjesztve a modell ismereteit, és csökkentve a hamis információfelhasználást, a hallucinációt és a pontatlanságot.

[48] A Retrieval-Integrated Generation technika a lekérdezési és generációs folyamatokat jobban összefűzi. Célja, hogy a modell jobban kihasználja a visszakeresett információkat és pontosabb, célzottabb választ adjon.

Shoman, Maged – Wu, Jia – Mirjalili, Seyedali – Shah, Mubarak (2023): *A Survey on Large Language Models: Applications, Challenges, Limitations, and Practical Usage*. TechRxiv. Online: https://doi.org/10.36227/techrxiv.23589741.v1

Hadi, Muhammad Usman – Al-Tashi, Qasem – Qureshi, Rizwan – Shah, Abbas – Muneer, Amgad – Irfan, Muhammad – Zafar, Anas – Shaikh, Muhammad Bilal – Akhtar, Naveed – Hassan, Syed Zohaib – Shoman, Maged – Wu, Jia – Mirjalili, Seyedali – Shah, Mubarak (2025): *LLMs: A Comprehensive Survey of Applications, Challenges, Datasets, Limitations, and Future Prospects*. TechRxiv. Online: https://doi.org/10.36227/techrxiv.23589741.v8

Harangi László (2020): Egy hónap alatt összeszerelte az NVIDIA a világ hetedik leggyorsabb szuperszámítógépét. *PCW,* 2020. augusztus 17. Online: https://www.pcwplus.hu/pcwpro/egy-honap-alatt-osszeszerelte-az-nvidia-a-vilag-hetedik-leggyorsabb-szuperszamitogepet-283131.html

Kharya, Paresh – Alvi, Ali (2021): Using DeepSpeed and Megatron to Train Megatron-Turing NLG 530B, the World's Largest and Most Powerful Generative Language Model. *Nvidia Developer,* 2021. október 11. Online: https://developer.nvidia.com/blog/using-deepspeed-and-megatron-to-train-megatron-turing-nlg-530b-the-worlds-largest-and-most-powerful-generative-language-model/

Touvron, Hugo – Lavril, Thibaut– Izacard, Gautier – Martinet, Xavier – Lachaux, Marie-Anne – Lacroix, Timothée – Rozière, Baptiste – Goyal, Naman – Hambro, Eric – Azhar, Faisal – Rodriguez, Aurelien – Joulin, Armand et al. (2023): *LLaMA: Open and Efficient Foundation Language Models*. Online: https://doi.org/10.48550/arXiv.2302.13971

Wang, Lei – Ma, Chen – Feng, Xueyang – Zhang, Zeyu – Yang, Hao – Zhang, Jingsen – Chen, Zhiyuan – Tang, Jiakai – Chen, Xu – Lin, Yankai – Zhao, Wayne Xin – Wei, Zhewei – Wen, Jirong (2024): A Survey on Large Language Model Based Autonomous Agents. *Frontiers of Computer Science,* 18. Online: https://doi.org/10.1007/s11704-024-40231-1

Wiggers, Kyle (2020): OpenAI's Massive GPT-3 Model is Impressive, But Size Isn't Everything. *VentureBeat,* 2020. június 1. Online: https://venturebeat.com/ai/ai-machine-learning-openai-gpt-3-size-isnt-everything

Yang Zijian Győző – Dodé Réka – Ferenczi Gergő – Héja Enikő – Jelencsik-Mátyus Kinga – Kőrös Ádám – Laki László János – Ligeti-Nagy Noémi – Vadász Noémi – Váradi Tamás (2023): *Jönnek a nagyok! BERT-Large, GPT-2 és GPT-3 nyelvmodellek magyar nyelvre*. XIX. Magyar Számítógépes Nyelvészeti Konferencia, Szeged, 2023. január 26–27. Online: https://acta.bibl.u-szeged.hu/78417/

Yupeng, Chang et al. (2023): A Survey on Evaluation of Large Language Models. *Arxiv.* Online: https://doi.org/10.48550/arXiv.2307.03109

NEMZETBIZTONSÁGI SZEMLE
13. évfolyam (2025) 2. szám 51–61. | DOI: 10.32561/nsz.2025.2.4

Márton Balázs[1]

Az Európai Unió Hírszerző Ügynöksége

Víziók és realitások

The European Union Intelligence Agency

Visions and Realities

Az Európai Bizottság elnökének felkérésére Sauli Niinistö egykori finn elnök részletesen megvizsgálta az Európai Unió polgári védelmi és háborús felkészültségének állapotát. A vizsgálat eredményéről készült jelentés javaslatai között egy teljes értékű uniós hírszerzési együttműködési szerv létrehozása is szerepel. Ennek nyomán olyan sajtócikkek láttak napvilágot, amelyek már egy önálló „európai CIA" felállítását vizionálják. A jelen tanulmányban áttekintem a hírszerzés jelenlegi helyét az Európai Unió alkotmányos és geopolitikai viszonyai között, az Európai Unió rendelkezésére álló ilyen jellegű kapacitásokat, valamint az önálló európai hírszerzési szervre vonatkozó elképzeléseket.

Kulcsszavak: *nemzetbiztonság, hírszerzés, Európai Unió, Niinistö-jelentés, INTCEN*

At the request of the President of the European Commission, former Finnish President Sauli Niinistö examined in detail the state of civilian and military preparedness of the European Union. The creation of a fully-fledged EU service for intelligence cooperation is among the recommendations of the report. As a consequence, press articles have already appeared that envisage the establishment of an independent 'European CIA'. In this study I review the current place of intelligence in the constitutional framework and geopolitical reality of the European Union, the current intelligence capacities available to the European Union, and the ideas regarding an independent European intelligence agency.

Keywords: *national security, intelligence, European Union, Niinistö report, INTCEN*

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Rendészettudományi Doktori Iskola, e-mail: Marton.Balazs@uni-nke.hu

Bevezetés

Az Európai Bizottság korábbi és újonnan megválasztott elnöke, Ursula von der Leyen arra kérte fel Sauli Niinistö egykori finn elnököt, hogy vizsgálja meg és készítsen részletes jelentést az Európai Unió (a továbbiakban: Unió) polgári védelmi és háborús felkészültségének állapotáról.[2] Az úgynevezett Niinistö-jelentés bemutatására 2024 őszén került sor. A nyilvánosságra hozott, *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness* címet viselő dokumentum számos javaslatot tartalmaz, amelyek egy része az Unió hírszerzési struktúrájának a megerősítésére vonatkozik, és végső soron egy teljes értékű uniós hírszerzési együttműködési szerv (*EU service for intelligence cooperation*) létrehozását célozza.[3] A Niinistö-jelentés hatására új lendületet vettek az uniós integráció nemzetbiztonsági hatásköreivel foglalkozó közpolitikai és szakmai viták, amelyek egyik fő fókusza az önálló uniós hírszerző szerv ideája.[4]

A jelen tanulmányban a fenti fejlemények nyomán áttekintem a hírszerzés helyzetét az Unió alkotmányos keretrendszerében. Az uniós jogon túl néhány gondolat erejéig foglalkozom azokkal a geopolitikai körülményekkel is, amelyek 2024-ben és valószínűleg az elkövetkezendő években a legnagyobb hatást fogják gyakorolni az integráció fejlődésének irányaira. Kitérek azokra a már meglévő hírszerzési képességekre, amelyekkel az Unió jelenleg támogatja a tagállamok és a saját biztonsági és védelmi döntéshozatalát. A Niinistö-jelentésből kiindulva említést teszek az önálló uniós hírszerző szerv felállítását célzó elképzelésekről. A tanulmány jogi és szakpolitikai dokumentumok kvalitatív módszertani elemzése útján kíván betekintést nyújtani az Unió létező hírszerzési jellegű aktivitásaiba, illetve azoknak a most még csak vizionált továbbfejlesztési lehetőségeibe.

A hírszerzés helyzete az Európai Unió alkotmányos és geopolitikai viszonyai között

Mindenekelőtt szükségesnek tartom tisztázni, hogy mit értünk hírszerzés alatt, és ez a fogalom miképpen viszonyul a nemzetbiztonság fogalmához. Mivel a hírszerzéssel és a nemzetbiztonsággal most uniós dimenzióban foglalkozom, ezért ki kell lépni a tagállami keretek közül, és egy olyan definíciót kell találni, amely kellően semleges és nemzetek feletti (szupranacionális). A szuverenisták már ennél a pontnál jó eséllyel amellett érvelnének, hogy szó sem lehet e fogalmak nemzetállami kötöttségektől való megtisztításáról, hiszen ezáltal azok lényegében az értelmüket veszítenék. A nemzetbiztonság *(national security)* vonatkozásában ezzel az érveléssel magam is egyetértek, ennélfogva uniós dimenzióban helyesebbnek tartom az „Unió biztonsága" szóösszetétel alkalmazását.

A hírszerzés *(intelligence)* esetében azonban ez az értelmezési korlát már nem feltétlenül áll fenn. Az elérhető meghatározások színe-java ugyan a hírszerzést is állami kontextusból értelmezi, lásd például Izsa Jenőt, aki szerint a hírszerzés egy állami funkció,[5] vagy

[2] European Commission 2024b.
[3] European Commission 2024a.
[4] Posaner 2024.
[5] Izsa 2009: 72–83.

J. Ransom Clarkot, aki a hírszerzés fogalmát az Amerikai Egyesült Államok rendszerén keresztül vezeti fel.[6] Jóllehet napjainkban a hírszerzés egyre inkább az információk döntéstámogatás érdekében való strukturált megszerzéseként definiálható, és nem korlátozódik az állami titkosszolgálatok klasszikus tevékenységére. Ezt látszik igazolni a szóösszetétel szemantikai lazulása, vagyis, hogy a hírszerzés kifejezést gyakran hallhatjuk az államtól teljesen független entitásokkal összefüggésben, úgymint üzleti hírszerzés vagy vállalati hírszerzés stb.

A nemzetbiztonságtól eltérően tehát a hírszerzés fogalmilag leválasztható az államról, sőt értelmezhető akár nem biztonsági és védelmi aspektusból. Tekintettel arra, hogy az Uniónak saját politikai döntéshozatali rendszere van, és ehhez kapcsolódóan autonóm erőforrások állnak a rendelkezésére, ezért véleményem szerint pusztán fogalmilag nem volna kizárt az ehhez kapcsolódó, ezt információkkal támogató hírszerzésről beszélni.

Az Uniót szuverén államok hozták létre a maastrichti szerződés aláírásával, és a közös célkitűzések elérése érdekében a tagállamok hatásköröket ruháztak rá.[7] Az Unió szuverén államok egyedi együttműködése, nem föderáció, csak annyi saját szuverenitással rendelkezik, amennyiről a tagállamok a saját elhatározásukból a közös célok hatékonyabb elérése érdekében lemondtak. Az Unió a hatalma – pontosabban szólva a nemzeti szuverenitásokból eredő és a rajta keresztül gyakorolt egyes hatáskörök – alapját nem közvetlenül a népszuverenitásból meríti, hanem a tagállamoktól kapja, ennek eredményeként a döntéshozatalában sajátos egyensúly alakul ki a kormányközi és a szupranacionális intézmények és eljárások között.[8] Az Unió egyes tulajdonságait illetően hasonlít az államokra, de legalább ennyi hasonlóságot mutat a nemzetközi szervezetekkel. Az Unió alkotmányos kereteit és ezen belül a tagállamoktól átruházott hatásköröket az elsődleges jog adja meg. Az Európai Unióról szóló szerződés (a továbbiakban: EUSZ) egyértelműen lefekteti, hogy az Unió és a tagállamok hatásköreinek elhatárolására a hatáskör-átruházás elve az irányadó.[9]

A hatáskör-átruházás elvének megfelelően az Unió kizárólag a tagállamok által a Szerződésekben foglalt célkitűzések megvalósítása érdekében, a Szerződésekben ráruházott hatáskörök határain belül jár el. Minden olyan hatáskör, amelyet a Szerződések nem ruháztak át az Unióra, a tagállamoknál marad.[10] Az EUSZ tehát egyértelműen fogalmaz, és önkorlátozásra inti az Uniót minden olyan területen, amelyet a Szerződések nem ruháztak reá.[11] A nemzeti biztonság *(national security)* pontosan ilyen terület. Az EUSZ 4. cikke értelmében „Az Unió tiszteletben tartja [...] az alapvető állami funkciókat, köztük az állam területi integritásának biztosítását, a közrend fenntartását és a nemzeti biztonság védelmét. Így különösen a nemzeti biztonság az egyes tagállamok kizárólagos feladata marad."[12] Ez egyértelmű önkorlátozást jelent az Unió számára a nemzetbiztonság területén, ami alapján úgy tűnik, hogy szó sem lehet önálló európai hírszerzésről. A valóságban a helyzet azonban ennél árnyaltabb, s jogilag sem ennyire egyértelmű. Az Európai Unió működéséről

6 Clark 2007.
7 Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata. HL C 326. 2012. október 26. 13-390. 1. cikk
8 Boros 2012: 14.
9 EUSZ 5. cikk (1).
10 EUSZ5. cikk (2).
11 EUSZ 4. cikk (1).
12 EUSZ 4. cikk (2).

szóló szerződés[13] (a továbbiakban: EUMSZ) a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségről szóló V. címe alatt található több cikke is felhatalmazza az Uniót jogalkotásra. Ilyen például az Unió által kialakított rendőrségi együttműködés, amely egyebek mellett kiterjedhet a bűnüldözési célú információgyűjtésre, felderítésre, a szervezett bűnözés felderítésére, továbbá a nemzetközi terrorizmus és a közös érdekeket sértő bűnözési formák üldözésére.[14]

Az EUMSZ ezekben az esetekben megosztott hatáskört ír elő, vagyis az Unió itt már elfogadhat jogszabályokat, és ha sor kerül erre, akkor a tagállami jog nem sértheti az uniós jogot. Nyilvánvaló, hogy a felsorolt területek mindegyike könnyedén a nemzetbiztonság és a hírszerzés érdeklődési körébe kerülhet, ezáltal viszont az a veszély állhat elő, hogy inkonzisztencia merül fel az említett területek és az EUSZ nemzetbiztonságot kizárólagosan tagállami hatáskörbe soroló, korábban idézett rendelkezése között. Ennek a veszélynek az elkerülése érdekében rögzítette az EUMSZ a 72. cikkében általános éllel, hogy az V. címe alatt található rendelkezések nem érintik a közrend fenntartásával, illetve a belső biztonság megőrzésével kapcsolatos tagállami hatáskörök gyakorlását.[15] Iain Cameron ugyanakkor rámutat arra, hogy az EUSZ 4. és az EUMSZ 72. bekezdéseiből idézett cikkek jogirodalmi értelmezésére különböző megközelítések láttak napvilágot.[16] Az eltérő értelmezések mögött ellenirányú érdekek húzódnak, hiszen az uniós intézmények a mozgásterük és ezáltal a politikai hatalmuk növelésére törekednek a nemzetbiztonság területén, amihez elengedhetetlen a hivatkozott normák tágító értelmezése. Ezzel szemben a tagállamok a szuverenitásuk védelme érdekében rendre inkább a szűkítő értelmezés mellett foglalnak állást.

A fogalmi keretek és a jogszabályok időnként talán túlságosan is elvont boncolgatása mellett érdemes azokra a geopolitikai fejleményekre is kitekinteni, amelyek a legnagyobb hatással vannak az Unióra. A *European Policy Centre* nevű prominens brüsszeli *think tank* munkatársai találóan „globális permakrízisnek" nevezik a korunkban tapasztalható nemzetközi állapotot.[17] Ezt az állapotot az egymást követő és különböző jellegű válságok jellemzik, amelyek együtt járnak a politikai bizonytalansággal. Anélkül, hogy az egyes kihívások részleteiben elmerülnék, – hiszen ez jócskán meg is haladná e tanulmány kereteit – példálózó jelleggel teszek említést a fegyveres konfliktusokról, a nagyhatalmak Uniót érintő hibrid és offenzív irányú beavatkozásairól, az illegális migrációról, a nemzetközi terrorizmusról, a belföldi radikalizációról stb. Jól látható, hogy ezek mindegyike a természeténél fogva komplex biztonsági fenyegetés, amely az uniós szintű döntések előkészítésében és meghozatalában minden eddiginél sürgetőbbé és indokoltabbá teszi a stratégiai előrejelzést *(strategic foresight).* Ehhez pedig elengedhetetlen a minél szélesebb körből beszerzett információk gyors, pontos és alaposan feldolgozott rendelkezésre állása.[18] Nem nehéz felismerni, hogy ennek az egyik legfontosabb előfeltétele a hatékony

13 EUMSZ.
14 EUMSZ 87–88. cikkek.
15 EUMSZ 72. cikk.
16 Cameron 2020.
17 Zuleeg – Emmanouilidis – Borges de Castro 2021.
18 Borges de Castro 2024.

hírszerzés. A hírszerzés egyre erősödő szerepét maguk az érdekeltek, vagyis a tagállamok hírszerzői is alátámasztják.[19]

Hírszerzési célú európai együttműködések

Az Uniónak jelenleg is vannak olyan szervei, amelyek működése a hírszerzési tevékenység során ismeretes elemeket foglal magában. Az említett uniós szervek mellett kialakultak az Unió biztonságával kapcsolatos információk egyesítésére és megosztására különböző formációban ülésező és eltérő mélységű együttműködések. Egyszóval, a hírszerzési célú európai kooperáció kapcsán többféle entitás is felmerülhet, ráadásul ezek egyáltalán nem mentesek a hatásköri átfedésektől.

Először is evidensnek tűnik, hogy – ezzel ugyan nem kétségbe vonva a jelentőségüket, de – a vizsgálódás köréből kizárjuk az informális, állandó intézményi háttérrel nem rendelkező, Unión kívüli államok bevonásával ülésező és elsődlegesen nem az uniós döntéshozatal támogatására kialakított olyan együttműködési platformokat, mint amilyen a Berni Klub, a Madrid Csoport vagy az Antiterrorista Szakértői Csoport (CTG).[20]

Másodszor, mivel a Niinistö-jelentés az uniós szintű döntéshozatalnak kifejezetten a biztonsági és védelmi szektorban való támogatásáról szól, erre tekintettel a vizsgálódás köréből ki kell rekeszteni azokat az uniós szerveket, amelyek eredeti mandátuma a szabadságon, a biztonságon és a jog érvényesülésén alapuló térséghez tartozó bel- és igazságügyi szakpolitikák tagállamok közötti hatékonyságnövelésére irányul. Egyebek mellett ebbe a körbe sorolható a Bűnüldözési Együttműködés és Képzés Európai Ügynöksége (a továbbiakban: Europol) és az Európai Határ- és Partvédelmi Ügynökség (a továbbiakban: Frontex). Az Europol és a Frontex szervezeteiben egyaránt találhatók az úgynevezett fúziós központok tulajdonságait magukon viselő egységek, továbbá mindegyikük készít olyan stratégiai és operatív szintű előrejelzéseket, amelyek az uniós döntéshozatalba becsatornázódnak, ráadásul a működésük során számos, az Unió biztonsága szempontjából releváns információ keletkezik. Mindezek ellenére elmondható, hogy a fenti halmazba tartozó uniós szervek elsődleges feladata nem az uniós szintű döntéshozatalhoz szükséges információk megszerzése, egyesítése és megosztása, hanem a tagállamok támogatása.

Ha tehát az Unión belül keressük a hírszerzési célú együttműködés plasztikus példáját, akkor az Európai Unió Helyzetelemző Központjához (a továbbiakban: EU INTCEN) kell hogy eljussunk. Az EU INTCEN a biztonsági és védelmi szektorban kifejezetten az uniós szintű döntéshozatal támogatására létrehozott egység, amely a közös kül- és biztonságpolitika alatt,[21] a közös kül- és biztonságpolitikai főképviselő (HR/VP)[22] munkaszervén, az Európai Külügyi Szolgálaton[23] (a továbbiakban: EKSZ) belül található.[24] Az EU INTCEN

[19] Intelligence College in Europe 2024.
[20] Counter Terrorism Group.
[21] Common Foreign and Security Policy (CFSP).
[22] High Representative/Vice President. Utóbbi megnevezés a főképviselő Európai Bizottságban betöltött alelnöki tisztségére utal.
[23] European External Action Service (EEAS).
[24] Lásd: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM:foreign_security_policy és https://www.eeas.europa.eu/sites/default/files/documents/2024/2024-10-16%20EEAS%20Org%201.01.pdf

feladatainak általános leírásáról már számos publikáció látott napvilágot, ezért ettől most eltekintek. Egyetértek Björn Fägerstennel, aki szerint a hírszerzési együttműködés fúziós központjaként funkcionáló EU INTCEN integrálódott a leginkább az uniós intézményi struktúrába.[25] Ezt mutatja, hogy az EU INTCEN szervezetileg az EKSZ részét képezi, ahogyan az is, hogy az uniós szintű cselekvések támogatása az elsődleges feladata.[26]

Az eddigiek alapján jól látható, hogy amellett, hogy az uniós és a tagállami hatáskörök elválasztása nem mindig egyértelmű, az Unió biztonságának szavatolásában érdekelt szervek között egymást átfedő hatáskörökkel és nem megfelelően körülhatárolt mandátumokkal szembesülünk. Ez a kihívás az Unió biztonsági ökoszisztémájának egészéről elmondható, de még erőteljesebben jelenik meg az olyan komplex fenyegetések esetén, mint a terrorizmus, ahol az EU INTCEN, a bel- és igazságügyi területen működő szervek és az informális együttműködések is szerephez jutnak.[27] Ez a felismerés az EU INTCEN kötelékén belül is elindított az egységesítési törekvéseket célzó folyamatokat. Ennek tudható be, hogy 2007-ben – különösen az Európai Unió Katonai Törzsének Hírszerzési Osztálya (EUMS INT) felől érkező katonai információk közös kezelésére, a korai előrejelzés és helyzetértékelés kapacitások fejlesztésére – létrehozták az egységes információelemzési kapacitást (*Single Intelligence Analysis Capacity*, SIAC).[28] Később, 2017-ben pedig a hibrid fenyegetések elleni fellépés hatékonyságának növeléseként a hibridfenyegetéses információkat szintetizáló uniós csoport (EU Hybrid Fusion Cell, HFC) felállításáról határoztak.[29]

A geopolitikai turbulencia fokozódása és az elmúlt időszakban tető alá hozott újítások ellenére elmondható, hogy az uniós döntéshozatalt támogató hírszerzés esszenciáját a tagállamok önkéntes hozzájárulása adja, amellett, hogy korlátozott mértékben az Uniónak is a rendelkezésére állnak saját hírszerző jellegű képességek (például műhold program, nyílt forrású információgyűjtést végző egységek, közösségi médiából való információgyűjtést végző egységek, az Európai Bizottság külképviseleteiről beérkező jelentések, az Európai Bizottságon belül keletkező összefoglalók, tájékoztatók stb.).[30] Az már egy másik kérdés, hogy ezzel együtt mennyire tud megvalósulni a tagállamok által megosztott és/vagy a saját erőforrásokból beérkező információk együttes kezelése, fúziója. Az információkezelés metódusa nem képezi kifejezetten e tanulmány tárgyát, de úgy vélem, hogy az eddigi intézkedésekből is világos, hogy van még tere a fejlődésnek.

A hírszerzési szektor hálózatos, kollaboratív természetéből fakadnak az együttműködés legégetőbb kihívásai. Fägersten ezek közül négyet emel ki, nevezetesen, hogy (1) a hírszerzési információk megosztása a tagállamok oldaláról erősen érdekvezérelt, ami az – egyébként gyakran heterogén – érdekek divergenciája okán hézagossá válhat; (2) a tagállamok erőforrásai és képességei eltérők, ami egyenlőtlen helyzetet teremt; (3) tagállamonként különböző bürokratikus akadályokkal kell szembenézni; és (4) hiányos a kooperáció infrastruktúrája.[31] Ezt Fägerstenhez hasonlóan más szerzők is így látják, azzal kiegészítve, hogy a taktikai

[25] Lásd Fägersten 2016.
[26] Fägersten 2016: 1.
[27] Az Európai Parlament 2018. december 12-i állásfoglalása a terrorizmussal foglalkozó különbizottság megállapításairól és ajánlásairól. 2018/2044(INI).
[28] Gruszczak 2022: 140.
[29] Európai Bizottság - Az Unió Külügyi és Biztonságpolitikai Főképviselője 2016.
[30] Conrad 2022.
[31] Fägersten 2016: 3.

szinten (műveleti céllal) folytatott hírszerzési együttműködés szintén csorbát szenved.[32] A tagállamok állam- és kormányfőit tömörítő Európai Tanács 2022-ben elfogadott Stratégiai Iránytű című iránymutatásai szintén erre a következtetésre jutottak. Az Unió legmagasabb szintű politikai döntéshozó testülete több pontban is kifejezte a hírszerzési képességek fejlesztésének, erősítésének a szükségességét.[33]

Nagyvonalakban a fentiek szerint körvonalazható a hírszerzési együttműködés uniós helyzete 2024. év végén. Ezek után csak az a kérdés, hogy ebből az állapotból hogyan jutunk el az „európai CIA-hoz", valamint tényleg ezzel a céllal fogalmazódhattak-e meg a Niinistö-jelentés javaslatai?

Az Európai Unió önálló hírszerzési képességét célzó elképzelések

A Niinistö-jelentés az Unió hírszerzési struktúrájának megerősítéséről ír, továbbá, hogy lépésről lépésre el kell jutni egy teljes értékű uniós hírszerzési együttműködési szerv létrehozásáig. Az Unió fenyegetésekkel szembeni ellenálló képessége érdekében a szerző az uniós szintű hírszerzési információk magasabb fokú kihasználását tűzi ki célul, amelyet a SIAC megerősítésén keresztül tart megvalósíthatónak. Ehhez három feltétel teljesülését látná kívánatosnak. Elsőként, a részben a tagállamoktól érkező, a SIAC-ban kezelt hírszerzési információk strukturálását, ideértve az uniós szintű konkrét műveleti célokhoz igazítását azért, hogy a döntéshozatalhoz szükséges legpontosabb információk álljanak az uniós vezetők rendelkezésére. Másodikként a műveleti célú intézményközi információmegosztás fokozását, a külső biztonságról szóló és a belbiztonsági információk egyesítését, ennek érdekében a SIAC, az Európai Bizottság egységei, valamint a bel- és igazságügyi uniós ügynökségek, például a Frontex és az Europol közötti együttműködés javítását minden szinten. Harmadikként az informális és különböző formátumú hírszerzési együttműködések „uniósítását", azaz formalizálását és uniós jogi szabályozás alá vonásukat.[34]

A célok elérése érdekében konkrét lépésekre tesz javaslatokat. Ilyen a SIAC megerősítése személyzettel, továbbá specifikus adatelemzési és nyelvi képességekkel, valamint egy folyamat kialakítása arra, hogy a SIAC tájékoztatóit a címzettek megfelelő időben és módon megkaphassák. Ezenfelül ide tartozik a SIAC és más releváns uniós aktorok (ideértve az Európai Unió Műholdközpontja,[35] az uniós intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportja [CERT-EU], az Európai Bizottság új Kiberhelyzeti és Elemző Központja, valamint az uniós külképviseletek stb.) között az információáramlás biztosítása. Javasolja még a SIAC és az Európai Bizottság, az EKSZ, a Tanács, valamint más uniós intézmények és a tagállamok közötti koordinációt az egyes kémelhárítási feladatok és az ellenérdekelt hírszerző szolgálatok penetrációjával szembeni fellépés végett.[36]

[32] Gruszczak 2022: 146–147.
[33] European Council – Council of the European Union 2022.
[34] European Commission 2024a.
[35] EU Satellite Centre (SATCEN).
[36] European Commission 2024a: 112–113.

Az eddigiekben felsorolt javaslatok értékelésével arra juthatunk, hogy a Niinistö-jelentés nem feszegeti túlzottan a hálózatos együttműködés kereteit, pusztán annak a fenyegetésspecifikus erősítésére és adaptációjára törekszik. Minden kétségen felül az integráció közös érdeke az uniós intézmények magasabb fokú biztonságiasítása *(sécurisation)*, az uniós entitások közötti információáramlás megkönnyítése és egységesítése, ahogyan a bel- és igazságügyi területen működő uniós szervek információs hálózatba való bekapcsolása is. A legkirívóbbnak talán az uniós vezetők részéről érkező hírigények kiszolgálására irányuló javaslat tűnhet, bár ha jobban belegondolunk, akkor a tájékoztatás kereslethez igazítása egyáltalán nem ördögtől való, ráadásul itt is alkalmazható az önkéntességből fakadó „szűrő", azaz a tagállam eldöntheti, hogy milyen információt csatornáz be a SIAC-ba.

A Niinistö-jelentés azonban a fentieken túl egyéb javaslatokkal is él, amelyekben hosszú távú célként ugyan, de kifejezetten egy, az uniós intézményeket és a tagállamokat egyaránt kiszolgáló teljes értékű uniós hírszerzési együttműködési szerv létrehozását irányozza elő. Minden bizonnyal a jelentésnek a hírszerzés kapcsán ez a pontja a legszembetűnőbb, ezért a szerző azon nyomban le is szögezi, hogy nem célja a tagállami hírszerző és elhárító szolgálatok működésének lemásolása, ahogyan a nemzetbiztonságra vonatkozó hatáskörök megsértése sem, mindössze a SIAC továbbfejlesztését kívánja elérni az uniós szintű fellépések és az uniós vezetés támogatásáért. Egyúttal kifejezi, hogy fontosnak tartja az uniós intézmények defenzív irányú megszilárdítását. Úgy véli, hogy az uniós szintű hírszerzési együttműködés jobban és strukturáltabban szabályozott információmegosztáson keresztül történhet, amely ugyanakkor teljes mértékben tiszteletben tartja a tagállamok hírszerzés terén meglévő előjogait. Az előzőek érdekében a szerző azt tanácsolja, hogy a tagállamokkal közösen dolgozzák ki a teljes értékű uniós hírszerzési együttműködési szervre vonatkozó javaslatot. Ez a szerv szerinte attól volna teljes értékű, hogy a fennálló hiányokat orvosolja, összekapcsolja a külső biztonságot és a belbiztonsági információkat, valamint képes arra, hogy stratégiai és műveleti oldalról szolgálja ki az uniós szintű politikai tervezést és döntéshozatalt.[37]

Mit hoz a jövő?

Összességében, a Niinistö-jelentés elintézhető volna akár annyival, hogy „nincs itt semmi látnivaló", szó sincsen egy „európai CIA" felállításáról, az önálló európai hírszerző szerv a szinte már megszokott újságírói túlzásnak köszönhetően vált újfent a közbeszéd tárgyává. Valójában azonban a gondolat egyáltalán nem a média fantáziálásának tudható be, hiszen politikusok és a témával foglalkozó szakemberek is vissza-visszatérően felvetik az önálló európai hírszerző szerv szükségességét.[38] Az viszont ezekből a felvetésekből általában nem derül ki, hogy egy ilyen szerv mennyiben volna több, vagy mennyiben volna más, mint az EU INTCEN – akár a Niinistö-jelentésben javasoltak mentén való – megerősítése.

John M. Nomikos, az Európai Hírszerzési Akadémia[39] igazgatójának álláspontja az, hogy az Uniónak létre kellene hoznia az Európai Unió Hírszerző Ügynökségét *(EU Intelligence*

[37] European Commission 2024a: 113–114.
[38] Lásd Robert 2015.
[39] Lásd: https://www.euintelligenceacademy.eu/home

Agency). Nomikos úgy látja, hogy erre az EU INTCEN megerősítésével kerülhetne sor, amelynek így a kémelhárításra, a terrorizmus elleni küzdelemre is kiterjedhetnének a feladatai, és az európai hírszerzési együttműködés egységes kapcsolattartó pontjává nőhetné ki magát.[40] Ennél több részletet azonban Nomikos sem osztott meg arról, hogyan is képzeli el az önálló hírszerző ügynökséget. Úgy vélem, hogy az egységes kapcsolattartó pont koncepciója valóban megfontolandó, ahogyan erre a Niinistö-jelentésben is találunk utalásokat, azonban az már kevésbé világos, hogy a kémelhárításra és a terrorizmusra vonatkozó információk akár a jelenlegi keretek között miért ne kerülhetnének a SIAC-ba, feltéve, ha azoknak uniós szintű relevanciája van. José-Miguel Palacios, az EU INTCEN elemzési egységének korábbi vezetője szerint a tagállami hírszerző szolgálatok lelkesen fogadnák a szervezeti önállósodást, az EKSZ-től való függetlenedést.[41] Ez jóval nagyobb autonómiát és láthatóságot adna számukra, valamint szabadságot például a tisztviselői állomány kiválasztásánál. Egyúttal viszont rendezni kellene a jogállamisági követelmények érvényesüléséhez elengedhetetlen garanciák kérdéseit (elszámoltathatóság, demokratikus kontroll stb.). Mindezek mellett kijelenthető, hogy még egy, a jelenleginél jóval erőteljesebb strukturális elkülönüléssel rendelkező európai hírszerző szerv sem válhatna olyan mértékben szupranacionálissá, hogy abszolút elszakítsa magát a tagállamoktól. Ráadásul, tankönyvi értelemben sokkal helyesebb volna önálló európai fúziós központról beszélni, hiszen a klasszikus hírszerzéshez szükséges kapacitások teljességének uniós szintű kiépítése utópia. Bóka János szerint az európai integráció mindig bizonyos célkitűzések megvalósítását tartotta elsődleges céljának, azoknak megfelelően alakította az integrációs intézményeit.[42] A Niinistö-jelentés, amely az Európai Bizottság elnöke általi formális felkérésnek köszönhetően mégiscsak egy közjogi keretek között készült dokumentum, maga tesz finom utalásokat, irányoz elő apróbb lépéseket a hatályos hírszerzési együttműködés határainak kipuhatolására. A geopolitikai realitásokat figyelembe véve aligha kritizálhatók a javaslatcsomag ezen elemei, hiszen az világos és jól felfogott közös érdek, hogy szükség van a preoperatív biztonsági intézkedések fokozására. A másik oldalról viszont nem árt időnként újra és újra megerősíteni, hogy a nemzetbiztonsági céllal folytatott hírszerzés *ab ovo* a nemzetállamok sajátja, és minden bizonnyal a jövőben is az marad. Az Unió biztonsága érdekében folytatott hírszerzés bizonyos mértékig szupranacionalizálódhat ugyan, de tekintettel arra, hogy az Unió a demokratikus legitimációját végső soron mégiscsak a tagállamok szuverenitásából meríti, ezért azoktól sosem különülhet el.

Felhasznált irodalom

Az Európai Parlament 2018. december 12-i állásfoglalása a terrorizmussal foglalkozó különbizottság megállapításairól és ajánlásairól. 2018/2044(INI). 2018. december 12. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52018IP0512

Bóka János – Gombos Katalin – Szegedi László (2019): *Az Európai Unió intézményrendszere*. Budapest: Dialóg Campus.

[40] Nomikos 2014.
[41] Palacios 2020.
[42] Bóka–Gombos–Szegedi 2019: 11.

Borges de Castro, Ricardo (2024): The New Commission Needs Better Mechanisms to Anticipate the Crises to Come. *European Policy Centre,* 2024. szeptember 17. Online: https://epc.eu/en/publications/~5d5c64

Boros, László (2012): *Az EU intézményi és döntéshozatali rendszere.* ELTE Eötvös Kiadó. Budapest.

Cameron, Iain (2020): European Union Law Restraints on Intelligence Activities. *International Journal of Intelligence and CounterIntelligence,* 33(3), 452–463. Online: https://doi.org/10.1080/08850607.2020.1754665

Clark, J. Ransom (2007): *Intelligence and National Security: A Reference Handbook.* Westport: Praeger. Online: https://doi.org/10.5040/9798400670961

Conrad, Gerhard (2022): Situational Awareness for EU Decision-making: The Next Decade. *European Foreign Affairs Review,* 26(1), 55–70. Online: https://doi.org/10.54648/EERR2021006

Európai Bizottság – Az Unió Külügyi és Biztonságpolitikai Főképviselője (2016): Közös közlemény az Európai Parlamentnek és a Tanácsnak. A hibrid fenyegetésekkel szembeni fellépés közös kerete európai uniós válasz. JOIN (2016) 18 final. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:52016JC0018

European Commission (2024a): *Report: Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness.* Online: https://commission.europa.eu/document/5bb2881f-9e29-42f2-8b77-8739b19d047c_en

European Commission (2024b): *Statement by President von der Leyen on the Presentation of the Niinistö Report on Strengthening Europe's Civilian and Military Preparedness and Readiness.* Online: https://ec.europa.eu/commission/presscorner/detail/en/statement_24_5601

European Council – Council of the European Union (2022): *A Strategic Compass for a Stronger EU Security and Defence in the Next Decade.* Sajtóközlemény, 2022. március 21. Online: https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/

Fägersten, Björn (2016): *For EU Eyes Only? Intelligence and European Security.* European Union Institute for Security Studies. Online: http://www.jstor.com/stable/resrep06819

Gruszczak, Artur (2022): Intelligence Fusion for the European Union's Common Security and Defence Policy. *Politeja,* 19(4), 131–150. Online: https://doi.org/10.12797/Politeja.19.2022.79.08

Intelligence College in Europe (2024): *Intelligence College in Europe (ICE) Outreach Event: Intelligence Services and the European Union.* 2024. október 24. Online: https://www.intelligence-college-europe.org/intelligence-college-in-europe-ice-outreach-event-intelligence-services-and-the-european-union

Izsa, Jenő (2009): A hírszerzés céljáról és rendszeréről. *Hadtudomány.* 19. évfolyam. 1–2. szám. 72–83.

Nomikos, John M. (2014): European Union Intelligence Analysis Centre (INTCEN): Next Stop to an Agency? *Journal of Mediterranean and Balkan Intelligence,* 4(2), 5–13.

Palacios, José-Miguel (2020): On the Road to a European Intelligence Agency? *International Journal of Intelligence and CounterIntelligence,* 33(3), 483–491. Online: https://doi.org/10.1080/08850607.2020.1754670

Posaner, Joshua (2024): Create a CIA-Style European Spy Service, von der Leyen is Told. *Politico,* 2024. október 30. Online: https://www.politico.eu/article/europe-spy-service-cia-ursula-von-der-leyen/

Robert, Aline (2015): Verhofstadt Calls for Creation of EU Intelligence Agency. *Euractive,* 2015. november 18. Online: https://www.euractiv.com/section/justice-home-affairs/news/verhofstadt-calls-for-creation-of-eu-intelligence-agency/

Zuleeg, Fabian – Emmanouilidis, Janis A. – Borges de Castro, Ricardo (2021): *Europe in the Age of Permacrisis.* Online: https://epc.eu/en/publications/Europe-in-the-age-of-permacrisis~3c8a0c

NEMZETBIZTONSÁGI SZEMLE
13. évfolyam (2025) 2. szám 62–73. | DOI: 10.32561/nsz.2025.2.5

Erdélyi Ákos[1]

A műveleti pszichológia konceptualizálása, helye és szerepe a pszichológia- és rendészettudományban 1.

A műveleti pszichológia elméleti keretének ismertetése

Conceptualisation, Place and Role of Operational Psychology in Psychology and Law Enforcement Sciences 1.

Introduction to the Theoretical Framework of Operational Psychology

Jelen írás egy kétrészes tanulmány első része, amelynek központi témája a műveleti pszichológia tudományterületi és -elméleti kérdése, valamint annak keretrendszere és meghatározása. Az utóbbi években hazánkban is megfigyelhető a kriminálpszichológiai alkalmazott kutatások és gyakorlati feladatellátás megerősödő tendenciája, ugyanakkor a műveleti pszichológiával kapcsolatos tudományos vizsgálódás kevésbé érhető nyomon ilyen mértékben, már ami a rendészeti és bűnügyi területen megjelenő műveleti pszichológiát illeti, ide nem sorolva a katonapszichológia művelettámogató funkcióit, amelyekről több tudományos közlést találunk. Ennek ellenére azonban úgy vélem, nem kérdés, hogy a műveleti pszichológiának fokozott relevanciája van mind a pszichológia-, mind a rendészettudományban.

Ezen írás célja bemutatni a műveleti pszichológia tudományterületi sokszínűségét, és rávilágítani arra, hogy egy jelenleg kevésbé konceptualizált, alkalmazott, multidiszciplináris alapokkal rendelkező terület milyen módokon szolgálhatja a rendészeti feladatok eredményes ellátását. Szakirodalmi feldolgozással, összefoglaló tanulmány jelleggel dolgozom fel a fentiekben megfogalmazottokat.

Mint az megállapítható, annak ellenére, hogy a műveleti pszichológia jelenleg kevésbé jól definiált és kevésbé meghatározott keretrendszerben működő terület, a szakirodalmi feldolgozás alapján látható, hogy nagymértékben tudná támogatni a rendészeti feladatellátást, általános és speciális területeken egyaránt. A kezdeti bizonytalanság

[1] Pszichológus, kriminológus, PhD-hallgató, egyetemi tanársegéd, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Rendészeti Magatartástudományi és Kriminálpszichológia Tanszék, e-mail: erdelyi.akos@uni-nke.hu

leküzdése érdekében célszerű lenne a kriminálpszichológia mellett a műveleti pszichológia konceptualizálására is figyelmet fordítani, amely kiterjedhetne a viszonyrendszerek és a tudományterületi elhelyezkedés tisztázására is.

Kulcsszavak: *műveleti pszichológia, konceptualizáció, rendszerszemlélet, relevancia, tudományterületi elhelyezkedés*

This article is the first chapter of a two-part study, the central theme of which is organised around the issue of operational psychology and its theoretical framework. In recent years, applied researches and practical task activities in criminal psychology have been strengthened, but scientific, empirical researches and studies related to operational psychology are less available to this extent. Nevertheless, there is no doubt that operational psychology has increased relevance in both psychology and law enforcement. The aim of my article is to present the scientific diversity of operational psychology and to highlight how a currently less conceptualised, multidisciplinary applied field can serve the effective performance of law enforcement tasks. For the above-mentioned points, I analyse the relevant literatures about operational psychology and write a review study. Despite the fact that operational psychology is a less well-defined field and operates within a less defined framework, it is clear from the literature review that this applied psychology could greatly support law enforcement tasks. Although its methodology is also immature, it can nevertheless draw heavily from the methodologies of psychology and related disciplines, which, if successfully integrated, can play an outstanding role as a special operations support field. It would be advisable to pay attention to the conceptualisation of operational psychology in addition to criminal psychology, which could also include clarifying the systems of relationships and the belonging to the scientific field.

Keywords: *operational psychology, conceptualisation, systems approach, relevance, science*

Bevezetés: vissza a kriminálpszichológiáig

Miért van szükség egy műveleti pszichológiai tematikájú írásban a kriminálpszichológiát vizsgálni? – merülhet fel a kérdés. A válasz a két alkalmazott lélektani terület specifikusságában és tárgyában keresendő: mindkét terület szervesen kapcsolódik a rendvédelemhez, a bűnüldözéshez, és bizonyos értelemben a kriminálpszichológia az „őse" valamennyi, a rendészeti feladatellátást támogató alkalmazott pszichológiai területnek.

Popper Péter (1968) a múlt században definiálta és klasszifikálta elsőként hazánkban a kriminálpszichológiát, amely meghatározás és osztályozás a mai napig is sok tanulmány, elméleti keretezés és tudományos diskurzus alapjául szolgál.[2] A popperi értelmezésben a kriminálpszichológia nem más, mint a bűncselekményt elkövető ember lélektana, személyiségstruktúrájának vizsgálata és a struktúra dinamikáinak feltárása, majd így folytatja:

[2] Vilics 2020; Koday 2019; Csernyikné Póth – Fogarasi 2006.

„a kriminálpszichológia a bűnözés és a bűnözővé válás társadalmi és egyéni pszichológiai feltételeivel, valamint a bűnözés elleni harc pszichológiai módszereivel foglalkozó tudomány".[3] Popper, hasonlóan Grosshoz (1905), a kriminálpszichológián belül három alterületet különített el egymástól. A három alterület a bűnnel, a bűncselekménnyel és annak résztvevőivel eltérő aspektusból foglalkozik: míg a kriminológiai pszichológia az elkövetővé és az áldozattá válás kérdéseire keres választ, a kriminalisztikai pszichológia feladata a büntetőeljárások nyomozástámogatása, kezdve a nyomozás elrendelésétől egészen a jogerős ügydöntő határozat kihirdetéséig, mindezt pedig olyan speciális eljárásokkal, mint az elkövetői profilalkotás, a kihallgatás-lélektan, a médiakommunikáció vagy a pszichológiai boncolás. A börtönpszichológia a már büntetés-végrehajtási intézetben letartóztatottként elhelyezett, illetve szabadságvesztésüket töltő fogvatartottakkal foglalkozik, továbbá feladata a személyi állomány pszichikai támogatása és a börtönkörnyezet vizsgálata is.[4]

1. táblázat: A kriminálpszichológia alterületei és feladatuk a popperi felosztás szerint

KRIMINÁLPSZICHOLÓGIA	kriminológiai pszichológia	„A bűnözővé válás társadalmi és egyéni pszichológiai feltételeiről, a bűnelkövetésig súlyosbodó antiszociális magatartásformák mögött meghúzódó személyiségstruktúra és mechanizmusok sajátosságairól szóló szakágazat."
	kriminalisztikai pszichológia	„A bűnüldözés nyomozati és bírói szakágának pszichológiáját tárgyalja. Ezen belül centrális területet jelent az úgynevezett tényállás-diagnosztika, a kihallgatási taktika pszichológiája, különös tekintettel a vallomások lélektanára, egyes speciális eljárások, például nyomozási kísérlet lélektani problémái."
	börtönpszichológia	„A reszocializálás pszichológiai feltételeit és módszereit kutatja. Az eredményes átnevelést biztosító komplex pedagógiai, pszichológiai és szociális gondozói tevékenység számos nevelés-lélektani és klinikai pszichológiai, egyes esetekben pedig egyéni és csoport-pszichoterápiás eljárások alkalmazását igényli."

Megjegyzés: Az idézetek forrása Popper 2014: 15.

Forrás: a szerző szerkesztése

Vilics (2020) kiemeli, hogy a kriminálpszichológia főszabály szerint a beszámítható személyekkel foglalkozik, ugyanakkor bizonyos mértékig a nem, vagy csak korlátozottan beszámítható személyekkel is van feladata, amely megállapításával az Igazságügyi Megfigyelő és Elmegyógyító Intézetben végzett tevékenységre és az igazságügyi pszichológiai szakértésre utal.

A *Rendészettudományi szaklexikon*[5] *kriminálpszichológia* szócikke alatt azt úgy határozza meg, mint az az alkalmazott lélektani terület, amelynek tárgya a bűnelkövetés, a bűnözővé és az áldozattá válás, továbbá a büntető igazságszolgáltatás lélektani kérdéseinek vizsgálata, és amely két alterületre osztható, nevezetesen a kriminológiai pszichológiára és a kriminalisztikai pszichológiára, ezzel felelevenítve a popperi értelemzési keretrendszert.

Ami azonban mind a gyakorlatban, mind a tudományos vizsgálódásban érzékelhető, hogy az 1970-es évekbeli popperi klasszifikáció napjainkra már „túlnőtte" magát: a három

[3] Popper 2014: 11.

[4] Lohner 2024; Vilics 2020; Koday 2019; Popper 2014; Fliegauf 2012; Csernyikné Póth – Fogarasi 2006; Boros–Csetneky 2000.

[5] Boda 2019.

alappillérnek tekinthető kriminálpszichológia-alterület mellett a klasszifikáció nem rendelkezik az olyan további, a kriminálpszichológiával kapcsolatba hozható alkalmazott területekről, mint a műveleti pszichológia, az intézkedéslélektan, a speciális felderítés- és elhárítástámogató pszichológiai eljárásokat magába foglaló területek vagy akár az igazságügyi pszichológia. Ezek a területek – közvetve vagy közvetlenül, de – mindenképpen hatást gyakorolnak napjaink kriminálpszichológiai felfogásának alakítására, ennek apropóján pedig megalapozták nemcsak tudományos, hanem a mindennapi gyakorlatban betöltött relevanciájukat.

Az utóbbi évtizedek során kirajzolódott az a tendencia, amelynek köszönhetően kijelenthetjük: a pszichológia mára a rendészettudomány komplementer tudományává vált. Az elméleti kriminálpszichológia az utóbbi években megerősödött, és a gyakorlatban is integrálódni tudott a rendőri szervezetbe, gondoljunk csak az Országos Rendőr-főkapitányság Bűnügyi Elemző-Értékelő Főosztályán működő Speciális Nyomozástámogató és Viselkedéselemző Csoportra.[6] A kriminálpszichológia ugyanakkor nemcsak az általános rendőrségnél kap fontos szerepet: a speciális rendőrségi feladatokat ellátó szerveknél éppúgy jelen van, igaz más kontextusban és más fókusszal. Ehhez a speciális környezethez és feladatellátáshoz illeszkedhet a műveleti pszichológia, amely terminológia egyelőre kevésbé definiált a hazai gyakorlatban, ugyanakkor kétségtelen, hogy módszertanának, ismeretanyagának köszönhetően releváns területté nőheti ki magát a következő néhány évben, mind a gyakorlatban, mind a tudományos vizsgálódásban.

A műveleti pszichológia konceptualizálása

Ahhoz, hogy meghatározzuk azt a fogalom- és keretrendszert, amelyben a műveleti pszichológia értelmezhető, mindenekelőtt a *pszichológia*, a *művelet* és az *elemző-értékelő tevékenység* szerepét kell tisztáznunk és kontextusba helyeznünk.

A pszichológia vizsgálatának tárgya az emberi viselkedés, célja pedig, hogy „feltárja, leírja, és összefüggéseket állapítson meg a viselkedésünket meghatározó jelenségek között. Olyan kérdéseket tesz fel például, hogy miként képeződik le számunkra a valóság, hogyan szerveződik a tudásunk, mi határozza meg az emberi kapcsolatainkat, az emberi fejlődésnek melyek a törvényszerűségei, illetve mely tényezők befolyásolják viselkedésünk."[7] Noha a legelső pszichológiai tematikájú gondolatok egészen az ókori Hellász filozófusaiig nyúlnak vissza, a pszichológiatudomány megszületése a 19. század második felére tehető, amikor a lipcsei egyetemen Wilhelm Wundt 1879-ben megszervezte az első pszichológiai laboratóriumot.[8] Az azóta eltelt közel 150 év alatt a pszichológiatudomány szerteágazó tudománnyá nőtte ki magát, és alapterületei (szociálpszichológia, személyiségpszichológia, fejlődés- és általános lélektan) mellett olyan alkalmazott területek is kialakultak, mint a sport-, a klinikai, a munka- vagy szervezet-, az evolúciós vagy épp a kriminálpszichológia, amelyek mind kialakították a rájuk jellemző speciális módszertanokat, eljárásokat és

[6] Lohner 2024.
[7] Farkas 2018: 15.
[8] Farkas 2018.

protokollokat, ezzel hozzájárulva az ember és az emberi viselkedés és magatartás komplexebb megértéséhez.

Amikor a rendészet és a pszichológia metszéspontjáról van szó, leggyakrabban a bűnügyi kriminálpszichológiára asszociálunk, ugyanakkor látni kell, hogy a pszichológia más területei is alkalmazhatók, sőt mi több, alkalmazzák is a rendészeti munka során. Kétségtelen, hogy a kriminálpszichológia igen nagy népszerűségnek örvend, és relevanciája megkérdőjelezhetetlen a bűnügyi munka során,[9] de ne feledkezzünk meg a szervezetpszichológia, a tanácsadás, a pedagógiai pszichológia vagy akár a klinikai és igazságügyi pszichológia rendészeti lehetőségeiről sem.[10]

A már idézett *Rendészettudományi szaklexikonban* a *művelet* szócikk alatt a következő meghatározás található:

> „A művelet a felderítés során tervszerűen végrehajtott többszereplős cselekvéssorozat, amely: 1. események célorientált befolyásolásával cselekmények kimenetelét és eredményét alakítja; 2. részeredményeket elérve meghatározza a felderítés további irányait és súlypontját; 3. a művelet során a felderítés eredményei részlegesen vagy teljeskörűen realizálódnak. Továbbá a művelet a műveleti egységek által speciális eszközökkel és taktikák alkalmazásával végrehajtott olyan tevékenység, amely a kiváltó emberi magatartás, helyzet, körülmény, cselekmény, illetve a folyamatban lévő bűncselekmény megszakítására fókuszál, az elkövető(k) elfogásával, valamint – szükséges és indokolt esetben – azok semlegesítésével."[11]

A műveleti pszichológia konceptualizálásához szükséges még egy fogalompár előzetes említése, nevezetesen az elemző-értékelő tevékenység tisztázása. A *Rendészettudományi szaklexikon* az elemző-értékelő tevékenység alatt a megszerzett adatok rendszerezését, a szervezet állandó és időszakos feladatrendszere egyes elemeivel való megfeleltetését, a multiplikációk kiszűrését, az adathiányok azonosítását, a rejtett összefüggések feltárását, az ellenérdekelt tevékenység egészének rekonstrukcióját érti.[12] Az elemző-értékelő tevékenység nem új keletű a rendészetben: mind az általános, mind a speciális rendőrségi feladatokat ellátó szervek, mind pedig a büntetés-végrehajtás végez elemző-értékelő tevékenységet, a specifikusság pedig az egyes szakterületi differencia alapján érhető nyomon (más és más az elemzés-értékelés célja a bűncselekmények, például emberölés felderítésekor, a terrorelhárításban vagy a büntetés-végrehajtásban). A cél ugyan eltérő, de a módszer nagyjából megegyezik: a beszerzett, rendelkezésre álló információhalmazból szisztematikus értékelést végezve egy döntés- és stratégiatámogató, összefoglaló elemzés elkészítése.

A műveleti pszichológia e három aspektus fúziójából, kölcsönös együtthatásából születik meg, aminek ugyanakkor nincs egzakt, konszenzuson alapuló meghatározása. Mégis szükséges valamilyen úton-módon definiálnunk azért, hogy megértsük, pontosan mire és hogyan használható ez a terület. Miután az előző bekezdésekben áttekintettük valamennyi elengedhetetlen szakterület konceptumát, rendelkezésünkre áll minden

[9] Bellavics 2024; Lohner 2024; Lehoczki 2021; Lehoczki – Ronyecz 2021; Pásztor–Mityók–Németh 2009.
[10] Vilics 2020; Pásztor–Mityók–Németh 2009.
[11] Boda 2019: 402.
[12] Boda 2019.

tényező, hogy meghatározhassuk a műveleti pszichológia terminológiáját és elhelyezzük azt a pszichológia- és rendészettudomány rendszerében.

A műveleti pszichológia olyan alkalmazott lélektani terület és elemző-értékelő tevékenység, amelynek célja kettős: egyrészt támogatja a felderítést és a titkos információgyűjtést oly módon, hogy a felderítő tevékenységek végzése során mind OSINT, mind HUMINT forrásból beszerzett információkból pszichológiai szempontú elemzéseket készít, másrészt szupportálja a műveleti és/vagy bűnügyi bevetési egységek célirányos műveleti tevékenységeit, akár már a műveleti terv megtervezésétől egészen a konkrét művelet befejezéséig. Módszerei, eljárásai multidiszciplináris alapokon nyugszanak: a műveleti pszichológia egyaránt merít a pszichológia alap- és alkalmazott területeinek módszereiből, valamint a rendészet- és hadtudomány, a kriminológia és kriminalisztika eljárásaiból. Így többek között eredményesen alkalmazhatja a pszichológiai profilalkotást, a pszichológiai boncolást, a nyílt forrású információk pszichológiai szempontú tartalomelemzését és értékelését, a krízisintervenciót, kríziskezelést és kríziskommunikációt, a kockázatértékelést, valamint a különböző pszichoedukatív tartalmakat, önismereti tréningeket.

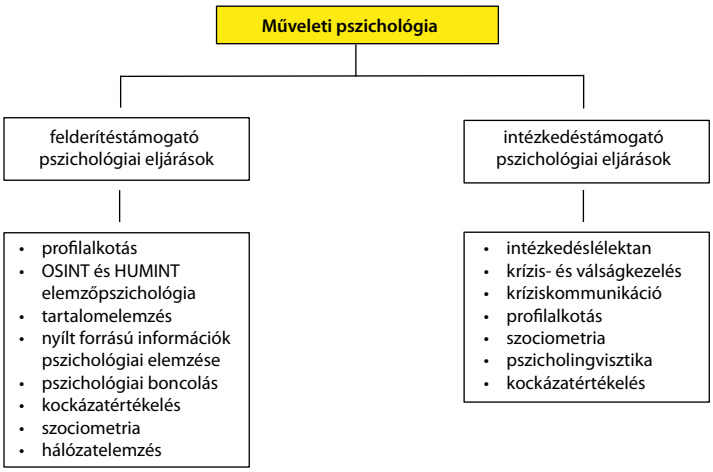
A rendvédelemben végezhető műveleti pszichológiai tevékenység során érdemes tekintettel lennünk arra is, hogy a katonapszichológia már régóta foglalkozik műveleti tevékenységek pszichológiai támogatásával,[13] így a bűnügyi és nemzetbiztonsági célú műveleti pszichológiai eljárások kidolgozásakor, figyelemmel a jelenség komplexitására és multidiszciplinaritására, sokat tanulhatunk a katonapszichológia művelettámogató feladataiból, módszereiből és eredményeiből.

2. táblázat: A műveleti pszichológia alkalmazott eljárásai és módszerei a felderítés és a műveleti szakterületek szemszögéből

MŰVELETI PSZICHOLÓGIA		
	felderítés	**művelet**
felderítéstámogató pszichológiai eljárások	• OSINT-elemzés • HUMINT-elemzés • nyílt forrású információk pszichológiai elemzése • tartalomelemzés • pszichológiai boncolás • pszichológiai profilalkotás • kockázatértékelés • szociometria, hálózatelemzés • narratív pszichológiai elemzés • életútinterjú	
művelettámogató pszichológiai eljárások		• krízis- és válságkezelés • krízisintervenció • kríziskommunikáció • kockázatértékelés • pszichológiai profilalkotás • pszichológiai boncolás • szociometria, hálózatelemzés

Forrás: a szerző szerkesztése

[13] Andó 2024; Sásik 2022; Andó 2020; Schild 2014; Hortobágyi 2010; Markolt 2010.



1. ábra: A műveleti pszichológia sematikus ábrája, feladatellátása alapján
Forrás: a szerző szerkesztése

A 2. táblázat hivatott összefoglalni, hogy a (műveleti) pszichológia milyen eljárásokkal, módszertani megoldásokkal támogatja az egyes műveleti tevékenységeket. Ennek mentén két lényeges differenciát kell tennünk: az egyik fő irányvonalat a felderítő-támogató pszichológiai eljárások alkotják, amelyek valamennyi olyan tevékenységet igyekeznek kiszolgálni, amelyek egy-egy bűncselekmény felderítéséhez, megelőzéséhez, a titkos információgyűjtéshez, a hírszerzéshez köthető folyamatokat szupportálják, míg a másik fő irányvonal a konkrét, célhoz kötött műveletek-intézkedések pszichológiai támogatása, legyen szó válságkezelésről, egy öngyilkossággal fenyegető helyzet kezeléséről vagy bűnügyi realizálás támogatásáról.

Amint látjuk tehát, a rendészeti kontextusban tárgyalt műveleti pszichológia voltaképpen két feladatellátás köré szervezhető: egy felderítést támogató/elemző pszichológiai feladatellátásra fókuszáló és egy intézkedéstámogató/intézkedéslélektani alterületet differenciálhatunk.

Ami a módszertani eljárásokat illeti, számos olyan alkalmazott eljárással találkozunk a műveleti pszichológia kapcsán, amelyek más rendészeti feladatellátás szupportja kapcsán már régóta jól bevettnekszámítanak. Annak ellenére pedig, hogy a műveleti pszichológia mint alkalmazott tudományterület nem rendelkezik mindenki által elfogadott definíciójával, a jogszabályi környezet rendelkezésünkre áll ahhoz, hogy a műveleti pszichológiai feladatellátás kereteit meghatározhassuk.

Ezen a ponton látom szükségesnek leszögezni, hogy jelen írás célja nem az, hogy részleteiben bemutassa a műveleti pszichológia egyes specifikus feladatellátásának részletszabályait és módszertani megoldásait (az majd a második részben érhető el), hanem célja a műveleti pszichológia tudományterületi elhelyezkedésének bemutatása. Így például ugyan a későbbiekben említést teszek a krízisintervencióról és -kezelésről, mint a műveleti pszichológia speciális, szuicid veszélyeztetettség kezelésére fókuszáló eljárásáról és feladatköréről, azonban ennek részletes bemutatása túlmutat a jelen írás keretein. Szintén ez a helyzet a terroristák és különösen a magányos merénylők és a pszichológiai profilalkotás

közti kapcsolattal, a kérdéskör részletes bemutatására terjedelmi okok miatt jelen írásban nincs lehetőség – azt egy másik tanulmány keretein belül szükséges megtenni.

A műveleti pszichológiai tevékenység során esetlegesen figyelembe vehető jogi keretek

A konceptualizálatlanság ellenére azonosítható néhány olyan jogszabály, amelyek alkalmazása szem előtt tartandó a rendvédelmi műveleti pszichológiai tevékenység során. Ezek alapján differenciálható, mely jogszabályok veendők figyelembe a rendőrségi és melyek a büntetés-végrehajtási műveleti pszichológiai tevékenység végzése során. A következőkben ezeket tekintem át.

Műveleti pszichológia és rendőrség

A rendőrség vonatkozásában – akár általános, akár speciális feladatokra szakosodott egységről legyen szó – jól azonosítható jogszabályok adják a műveleti (pszichológiai) tevékenység keretét.

[A *pszichológiai* jelző itt azért kezelendő zárójelben, mivel konkrétan a műveleti pszichológiai tevékenységre vonatkozó jogszabályi vagy egyéb írott norma nem áll rendelkezésre; megjegyzem, hogy általánosságban véve a kriminálpszichológiai tevékenységgel kapcsolatosan sincs írott normánk, hacsak a 2009-es megjelenésű Rendvédelmi bűnügyi-kriminálpszichológiai tevékenység szakmai protokollját[14] nem tekintjük annak, amely pusztán általánosságban fogalmaz meg lehetőségeket és elveket a kriminálpszichológiai tevékenységgel kapcsolatosan.]

Elsők között említendő az egészségügyről szóló 1997. évi CLIV. törvény (a továbbiakban: Eü. tv.), amely meghatároz olyan viselkedés- és magatartásformákat, amelyeknek kiemelt jelentőségük van a műveleti pszichológia vonatkozásában. Ezeket a magatartásformákat az Eü. tv. *veszélyeztető* és *közvetlen veszélyeztető magatartásként* definiálja – ebben az értelemzési rendszerben ilyen magatartásként kezelendő többek között a szuicidium vagy a pszichotikus zavar.

A hatáskör és illetékesség tekintetében kiemelt szabályzók egyike a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól szóló 295/2010. (XII. 22.) Korm. rendelet, amelynek 3. § (2) bekezdés c) pontja alapján a Terrorelhárítási Központ (a továbbiakban: TEK) végzi a rendvédelmi szervek részére kizárólagos hatáskörrel az ön- vagy közveszélyes állapotban lévő személy megfékezését és előállítását, amennyiben a személy a vele szemben foganatosított intézkedés során fegyveresen vagy felfegyverkezve áll ellen, így a műveleti pszichológia, azon belül is a kríziskezelés relevanciája és szerepe e vonatkozásban megkérdőjelezhetetlen. Emellett, mivel a műveleti pszichológia a felderítésben is kaphat szerepet, így többek között a terrorcselekmények és az ahhoz kapcsolódó egyéb bűncselekmények felderítésében és elhárításában is szerepet játszhat, és támogathatja

[14] Pásztor–Mityók–Németh 2009.

a felderítést és elhárítást, amely ugyancsak a TEK esetében releváns, tekintettel arra, hogy az imént már idézett 295/2010. (XII. 22.) Korm. rendelet 3. § (1) bekezdésének, továbbá a Rendőrségről szóló 1994. évi XXXIV. törvény 7/E. § (1) bekezdésének értelmében a Btk. 314–316/A. §-ba ütköző bűncselekmények megelőzésére és felderítésére a TEK rendelkezik hatáskörrel. Míg a felderítés a fentiek alapján a TEK hatáskörébe tartozik, az ilyen jellegű bűncselekmények vizsgálatára már a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet fogalmaz meg részletszabályokat. Eszerint a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 316. §-ába ütköző és aszerint minősülő terrorcselekménnyel fenyegetés bűntettének vizsgálatára a vármegyei rendőr-főkapitányságoknak van hatásköre (kivéve a Repülőtéri Rendőr Igazgatóság hatáskörébe tartozó eseteket), míg a Btk. 314. §-ába ütköző és aszerint minősülő terrorcselekmény bűntettének vizsgálatára már a Készenléti Rendőrség Nemzeti Nyomozó Irodának.

Műveleti pszichológia a büntetés-végrehajtásban

A büntetés-végrehajtási (a továbbiakban: bv.) műveleti pszichológia esetében részben találkozunk már néhány, az imént idézett szabályzókkal, nevezetesen az Eü. tv., valamint a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól szóló 295/2010. (XII. 22.) Korm. rendelet vonatkozó részleteivel. Ugyanakkor a bv. művelet kapcsán bv. szabályzók is rendelkezésünkre állnak.

Mindenekelőtt – és talán a legfontosabb – szabályzó a büntetés-végrehajtási szervezet műveleti egységeinek működéséről szóló 26/2022. (XII. 21.) BVOP utasítás, amely voltaképpen taxatíve sorolja fel a műveleti egység feladatkörébe tartozó eseteket, kitér a képzési-továbbképzési rendszer szerepére és a kiválasztás folyamatára – ezzel kapcsolatban kitér arra is, hogy a speciális fizikai kiválasztásról egy másik BVOP utasítás fogalmaz meg szabályokat. [A rendőrségi műveleti egységek kiválasztásáról egyébként a Rendőrség állományának alkalmasságvizsgálatáról szóló 35/2020. (XII. 23.) ORFK utasítás 22/D pontja fogalmazza meg azt, hogy a KR NNI Műveleti Szolgálat fedett állománya esetén a pszichológiai alkalmasságvizsgálatot első fokon a KR NNI MSZ állományában szolgálatot teljesítő, pszichológus végzettséggel rendelkező munkatárs végzi.]

A veszélyeztető magatartások, illetve az ön- vagy közveszélyes állapotok kapcsán a büntetés-végrehajtás konkrétabb szabályzókat alkotott meg, mint a rendőri szervezet. Mindamellett, hogy az Eü. tv. vonatkozó rendelkezései a bv.-ben is követendők, egyrészt a szuicidium vonatkozásában született a fogvatartotti krízisek, öngyilkossági kísérletek és önártalmak megelőzéséről szóló 18/2020. (V. 29.) BVOP utasítás, másrészt a pszichotikus állapot vonatkozásában figyelembe veendő jogszabály pedig a kényszergyógykezelés és az ideiglenes kényszergyógykezelés végrehajtásáról, valamint az Igazságügyi Megfigyelő és Elmegyógyító Intézet feladatairól szóló 13/2014. (XII. 16.) IM rendelet, amely ugyan nem műveleti céllal született, de találunk benne olyan részeket, amelyek e helyzetek kezelése kapcsán fontos szabályokat fektetnek le.

Kiemelendő pozitívum, hogy a bv. szervezet utasítás formájában szabályozza a (börtön)pszichológusok feladatellátását és szervezeti jogállását. Néhány oldallal fentebb kitértem arra, hogy a bűnügyi-kriminálpszichológiai tevékenység – és ez igaz az alapellátó

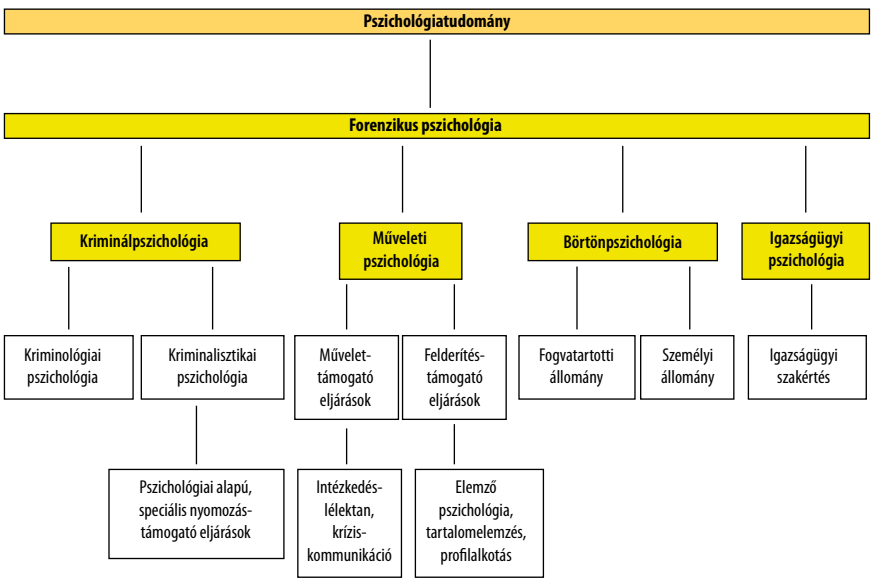
pszichológusokra is – mennyire alulszabályozott a rendőrség életében, ezzel ellentétben a bv.-ben dolgozó pszichológusok munkája – és így közvetve a börtönpszichológiai tevékenység – jóval szabályozottabb környezetben valósul meg, köszönhetően a büntetés-végrehajtási szervezetben szolgálatot teljesítő pszichológusok szervezeti jogállásáról és a fogvatartottakkal végzett tevékenységéről szóló 50/2020. (X. 16.) BVOP utasításnak.

Összegzés

Jelen írásban a műveleti pszichológia témakörét jártam körbe, elsődlegesen annak konceptualizálására, tudományterületi elhelyezkedésére helyezve a hangsúlyt. Amint azt látjuk, a műveleti pszichológia jelenleg kevésbé kidolgozott terminológia, amely ugyanakkor olyan multidiszciplináris elméleti alapokkal rendelkezik, amelyek elősegíthetik e hiányállapot feloldását.

Korábban több fórumon is bemutattam, hogy a 20. századi popperi kriminálpszichológia-klasszifikáció napjainkban már túlnőtte magát, tekintettel arra, hogy számos alkalmazott területtel és szakággal bővült, ami miatt szükséges és indokolt a tudományterület újrastrukturálása, újrakeretezése. Ebbe az új struktúrába célszerű külön is beilleszteni a műveleti pszichológia területét, ahogyan a kriminálpszichológia – börtönpszichológia között már régebb óta fennálló alá-fölérendeltségi viszonyrendszer problematikája[15] is tisztázható lenne.

Az is jól látható, hogy a rendészeti műveleti pszichológia sokat tanulhat a katonapszichológiától.[16] Kétségtelen, hogy a katonai műveletek pszichológiai támogatása mind



2. ábra: A kriminálpszichológia új, alternatív megközelítésének javaslata
Forrás: a szerző szerkesztése

[15] Fliegauf 2012; Boros–Csetneky 2000.
[16] Varga–Gulyás 2023.

gyakorlatban, mind elméletben messze előrehaladott a rendészeti műveleti pszichológiát illetően, éppen ezért az ott szerzett tapasztalatok vizsgálata jó eredménnyel segítené a rendészeti műveleti pszichológia keretrendszerének kidolgozását.

A fentiek lényegében egyetlen gondolatban jól összefoglalhatók: kétségtelen, hogy a rendészetben is lenne lehetőség műveleti pszichológiai feladatellátásról beszélni, és nagyon jó módszereket lehetne integrálni a tágabban értelmezett kriminálpszichológia és a katonapszichológia eljárásaiból, ugyanakkor látni kell azt is, hogy a műveleti pszichológia jelenleg erőteljesen kidolgozásra szükséges állapotban létezik. Ha a kezdeti nehézségeken sikerül túllendülni – már amennyire erre mutatkozik bármilyen igény –, bizonyára egy olyan alkalmazott lélektani területet sikerülne adaptálni a rendvédelmi szervek feladatellátásába, amely minden téren megállná a helyét.

Felhasznált irodalom

Andó Sándor (2020): A fokozott készenléti állapot néhány missziós vonatkozása. *Honvédségi Szemle,* 148(5), 82–95. Online: https://doi.org/10.35926/HSZ.2020.5.7

Andó Sándor (2024): *A Magyar Honvédség 1990. utáni katonapszichológiai szaktevékenységének elemző értékelése.* Doktori (PhD-) értekezés. Budapest: Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola.

Bellavics Mária Zsóka (2024): *Klinikai profilozás és empíria: a kriminalitás és a mentális zavar kapcsolata egy fiatalkorú bűnelkövetői mintában.* Doktori (PhD-) értekezés. Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Doktori Iskola. Online: https://doi.org/10.17625/NKE.2024.050

Boda József főszerk. (2019): *Rendészettudományi szaklexikon.* Budapest: Dialóg Campus.

Boros János – Csetneky László (2000): *Börtönpszichológia.* Budapest: Rejtjel.

Csernyikné Póth Ágnes – Fogarasi Mihály (2006): *Kriminálpszichológia.* Budapest: Rejtjel.

Farkas Johanna (2018): Pszichológia és közszolgálat. In Haller József – Farkas Johanna (szerk.): *Pszichológia a közszolgálatban I.* Budapest: Dialóg Campus, 13–22.

Fliegauf Gergely (2012): A börtönpszichológia elhatárolása a kriminálpszichológiától. *Börtönügyi Szemle,* 31(1), 45–62.

Gross, Hans (1905): *Kriminal-Psychologie.* Lipcse: Verlag von F. C. W. Vogel.

Hortobágyi Miklós (2010): Virtuális kiképzőrendszerek katonapszichológiai vonatkozásai. *Honvédorvos,* 62(1–2), 78–84.

Koday Zsuzsanna (2019): Börtönpszichológia, avagy ami „szabad szemmel" láthatatlan. In Kapitány-Fövény Máté – Koncz Zsuzsa – Varga S. Katalin (szerk.): *Klinikai szakpszichológia a gyakorlatban. Útirányok.* Budapest: Medicina, 231–252.

Lehoczki Ágnes (2021): *A poszt–offenzív szakasz pszichológiai vizsgálata az emberölés profilalkotásában.* Doktori (PhD-) értekezés. Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Doktori Iskola. Online: https://doi.org/10.17625/NKE.2022.008

Lehoczki Ágnes – Ronyecz Csaba (2021): Emberölés nyomozói szemmel és a pszichológiai profilalkotás – esettanulmány. *Belügyi Szemle,* 69(12), 2087–2105. Online: https://doi.org/10.38146/BSZ.2021.12.2

Lohner Klaudia (2024): Speciális nyomozástámogató és viselkedéselemző tevékenység. *Belügyi Szemle,* 72(5), 871–891. Online: https://doi.org/10.38146/BSZ-AJIA.2024.v72.i5.pp871-891

Markolt Norbert (2010): A debriefing: Egy krízisintervenciós módszer bemutatása és alkalmazásának lehetőségei a Magyar Honvédségben. *Honvédorvos,* 62(1–2), 85–95.

Pásztor Attila – Mityók Csaba – Németh Ferenc (2009): A rendvédelmi bűnügyi pszichológiai tevékenység szakmai protokollja. In Gaál Gyula – Hautzinger Zoltán (szerk.): *Tanulmányok „a rendészet kultúrája – kulturált rendészet" című tudományos konferenciáról.* Pécsi Határőr Tudományos Közlemények X., 251–255.

Popper Péter (1968): Kriminálpszichológia. In Lénárd Ferenc (szerk.): *Alkalmazott pszichológia. 2. átdolgozott és bővített kiadás.* Budapest: Gondolat, 300–333.

Popper Péter (2014): *A kriminalitásig súlyosbodó személyiségzavarok pszichikai tényezőinek vizsgálata*. Budapest: Saxum.

Sásik Csaba (2022): Katonai szociális munka harci körülmények között – a harcoló katona komplex humán támogatása. *Honvédségi Szemle,* 150(3), 86–100. Online: https://doi.org/10.35926/HSZ.2022.3.7

Schild Marianna (2014): A katonai létből adódó krízishelyzetek pszichológiai hátterei. *Műszaki Katonai Közlöny,* 24(1), 259–274.

Vajger Éva – Virág László szerk. (2009): *A rendvédelmi pszichológiai tevékenység szakmai protokollja*. Határrendészeti Tanulmányok.

Varga Nóra – Gulyás Géza (2023): Pszichológiai hadviselés a békefenntartó műveletekben. *Lélektan és Hadviselés,* 5(2), 9–24. Online: https://doi.org/10.35404/LH.2023.2.9

Vilics Tünde (2020): Kriminálpszichológia és kriminálpszichológus. *Magyar Rendészet,* 20(4), 219–239. Online: https://doi.org/10.32577/mr.2020.4.14

Jogi források

1994. évi XXXIV. törvény a Rendőrségről

1997. évi CLIV. törvény az egészségügyről

2012. évi C. törvény a Büntető Törvénykönyvről

295/2010. (XII. 22.) Korm. rendelet a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól

25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről

13/2014. (XII. 16.) IM rendelet a kényszergyógykezelés és az ideiglenes kényszergyógykezelés végrehajtásáról, valamint az Igazságügyi Megfigyelő és Elmegyógyító Intézet feladatairól

18/2020. (V. 29.) BVOP utasítás a fogvatartotti krízisek, öngyilkossági kísérletek és önártalmak megelőzéséről

50/2020. (X. 16.) BVOP utasítás a büntetés-végrehajtási szervezetben szolgálatot teljesítő pszichológusok szervezeti jogállásáról és a fogvatartottakkal végzett tevékenységéről

26/2022. (XII. 21.) BVOP utasítás a büntetés-végrehajtási szervezet műveleti egységeinek működéséről

35/2020. (XII. 23.) ORFK utasítás a Rendőrség állományának alkalmasságvizsgálatáról

NEMZETBIZTONSÁGI SZEMLE
13. évfolyam (2025) 2. szám 74–93. | DOI: 10.32561/nsz.2025.2.6

Ambrusz József,[1] Vásárhelyi Örs[2]

A kritikus szervezeti reziliencia és a lakosságfelkészítés nemzetbiztonsági jelentősége a modern fenyegetésekkel szemben

The National Security Importance of Critical Entities Resilience and Citizen Preparedness Against Modern Threats

Napjaink modern hibrid fenyegetései egyre összetettebb kihívások elé állítják a kritikus infrastruktúrákat és az alapvető szolgáltatást nyújtó szervezeteket. Az infrastruktúrák elleni kibertámadások nemcsak gazdasági és politikai instabilitást idézhetnek elő, hanem közvetlen hatással lehetnek a lakosság mindennapi életére is. Jelen tanulmány vizsgálja a kritikus szervezetek és infrastruktúrák védelmének nemzetbiztonsági dimenzióit, és rámutat a CER és a NIS2 uniós irányelvek szerepére az érintett szervezetek védelmének megerősítésében. A tudományos munka emellett párhuzamot von a lakossági felkészültség fokozásának szükségességével, amely az aktív felkészítés és a digitális tájékoztatás révén csökkentheti a krízishelyzetek kialakulását, és elősegítheti a hatékony eseménykezelést. Az esettanulmányokon alapuló kutatás konkrét példákkal mutatja be a hibrid fenyegetések hatásait, különös tekintettel a kritikus szolgáltatások működésére gyakorolt következményekre. A szerzők javaslatokat fogalmaznak meg a katasztrófavédelem digitális eszközökkel való támogatására, beleértve a lakosság katasztrófavédelmi felkészítésének eszközrendszerét is.

Kulcsszavak: *kritikus infrastruktúra, CER és NIS2 irányelvek, hibrid hadviselés, lakosságfelkészítés*

Today's modern hybrid threats pose increasingly complex challenges to critical infrastructure and essential service providers. Cyber and sabotage attacks against infrastructures can not only cause economic and political instability but can also

[1] Egyetemi docens, intézetigazgató-helyettes, tanszékvezető, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Katasztrófavédelmi Intézet, e-mail: ambrusz.jozsef@uni-nke.hu
[2] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: vasarhelyi.ors.laszlo@stud.uni-nke.hu

have a direct impact on the daily lives of citizens. This paper explores the national security dimensions of the protection of critical organisations and infrastructures and highlights the role of the EU CER and NIS2 Directives in strengthening the protection of these organisations. The academic draws parallels with the need to increase citizen preparedness, which through active preparation and digital information can reduce the occurrence of crisis situations and facilitate effective incident management. The case study-based research illustrates the impact of hybrid threats through concrete examples, with a particular focus on the consequences for the functioning of critical services. The authors make suggestions for supporting disaster management with digital tools, including tools for citizen preparedness.

Keywords: *critical infrastructure, CER and NIS2 directives, hybrid warfare, citizen preparedness*

Bevezetés

A modern társadalmak nagymértékben függenek az alapvető szolgáltatásokat nyújtó szervezetektől és a kritikus infrastruktúráktól – legyen szó energiaszolgáltatásról, kommunikációs hálózatokról, közlekedési rendszerekről vagy pénzügyi szolgáltatásokról. *Magyarország Nemzeti Kiberbiztonsági Stratégiája* is hangsúlyozza, hogy az elsődleges cél a megelőzésre épülő hatékony védelmi intézkedések révén a kibertérből érkező fenyegetések és azok kockázatainak kezelése. Ez napjainkban talán aktuálisabb, mint a stratégia megalkotásakor volt, hiszen egyre több konfliktus bontakozik ki világszerte, ezért hazánknak kiemelt figyelmet kell fordítania a biztonságra, így elkerülhetetlen az alapvető szolgálatást nyújtó szervezetek védelmének fokozása. A modern hadviselésben egyre nagyobb szerepet kapnak a hagyományos katonai erők mellett megjelenő aszimmetrikus eszközök és technikák is, mint például a kibertámadások és a dezinformációs kampányok. A kritikus infrastruktúrák és az alapvető szolgáltatást nyújtó szervezetek célpontként történő kiválasztása vonzó, mert ezen szervezetek rendszereinek a kompromittálódása vagy kiesése nemcsak gazdasági károkat okozhat, hanem társadalmi-politikai instabilitást és lakosságvédelmi problémákat is előidézhet. A 2024-es *Microsoft Defense Report* rámutatott annak tényére, hogy a modern hibrid konfliktusok során a kritikus infrastruktúra a fizikai csapások és a kibertámadások egyik fő célpontja. A Microsoft megfigyelte az alapvető szolgáltatást nyújtó szervezetek kritikus folyamatait vezérlő OT-rendszerek elleni támadások növekedését.[3]

Az új típusú szürkezónás hadviselési forma – amely a béke és a háború közötti határon mozgó katonai, gazdasági, politikai és kiberműveletek összessége, célja pedig egy állam vagy egy szervezet destabilizációja nyílt háborús konfliktus kockázata nélkül – relatív alacsony erőforrás-befektetés mellett is súlyos hatásokat képes elérni, ezért a modern társadalom biztonsága szempontjából elengedhetetlenül fontos a kritikus infrastruktúrák és a kritikus szervezetek megfelelő védelme, valamint a lakosság felkészítése a kedvezőtlen események hatásaira.[4] Hazánk nemzetbiztonsági érdeke ezen szervezetek és infrastruktúrák védelme

[3] *Microsoft Digital Defense Report 2024:* 20.
[4] Kiss 2019: 17–37.

és az ezzel összefüggő lakosságvédelem, hiszen ezek biztosítják a társadalom és a gazdaság alapvető működését és stabilitását konfliktushelyzetekben is.

Jelen tudományos munka célul tűzte ki, hogy rávilágítson a lakosság és a kritikus szervezetek rezilienciájának nemzetbiztonsági jelentőségére egy összehangolt hibrid támadással vagy kibertámadással szemben. Továbbá a szerzők célja, hogy bemutassák a CER és a NIS2 irányelv szerepét a kritikus szervezetek és infrastruktúrák 21. századi kihívásokkal szembeni védelmi képességének erősítésében, valamint a lakosság felkészítését az új évszázad kihívásaival szemben, annak technológiai előnyeit felhasználva.

Kutatási módszertan

Jelen tudományos munka elkészítése során a szerzők elsődlegesen szekunder adatokat dolgoztak fel, valamint a CER és a NIS2 irányelv implementációs tevékenységből fakadó új jogszabályok összehasonlító elemzését végezték el, emellett analitikai szempontból vizsgálták a témában megjelent releváns irodalmat. A szerzők azonosították a releváns forrásokat, majd a különböző forrásokból származó adatok egyesítésével összefüggéseket vontak le az adatokban lévő mintázatokból, és következtetéseket fogalmaztak meg. Esettanulmányokon keresztül mutatják be a kritikus szervezetek kitettségét a 21. századi kihívásoknak, valamint górcső alá kerültek a támadásokat követő hatások. A nemzetközi színtér esettanulmányaiból levont következtetések hazai viszonylatban is értelmezhetők. Emellett a szerzők empirikus kutatást is végeztek, amelynek célja az volt, hogy közvetlen információkat szerezzenek a kritikus infrastruktúrák és az alapvető szolgáltatást nyújtó szervezetek rezilienciáját célzó intézkedések gyakorlati alkalmazásáról és kihívásairól, különböző munkaprojektek keretében, valamint az iparági jógyakorlatok vizsgálatával. A szerzők a Shodan keresőmotort alkalmazták annak érdekében, hogy magyarországi sérülékeny ipari rendszerelemeket keressenek a hazai szervezetek potenciális kitettségének alátámasztására.

A kritikus infrastruktúrák sérülékenysége

A kritikus infrastruktúrák, valamint a kritikus szervezetek stabil üzemfolytonos működése alapvető nemzetbiztonsági érdek és érték, mivel azok meghibásodása vagy kompromittálódása a lakosság ellátásának összeomlásához, társadalmi zavarokhoz és gazdasági károkhoz vezethet. Magyarország földrajzi helyzete és energiafüggősége[5] különösen érzékennyé teszi az országot a hibrid és kiberfenyegetésekre, ilyen például az energiaellátási láncok megszakadása, ami gazdasági és társadalmi feszültségeket kelthet.[6] Törekedni kell arra, hogy a hazai kritikus infrastruktúrák a kockázatokkal arányos védelmi képességet alakítsanak ki, és ne rendelkezzenek olyan támadási felületekkel, amelyek célzott fenyegetések látókörébe helyezhetik.

[5] Brucker–Jóna–Szemerédi 2024: 155–182.
[6] Ambrusz–Beke 2023: 638–639.

Hibrid hadviselés keretében a kritikus infrastruktúrák elleni támadások stratégiai eszközzé váltak:

- Fizikai támadások (például energiaellátó hálózatok szabotálása vagy katonai műveletek keretében történő támadása).
- Kibertámadások, amelyek adatvesztéssel járhatnak, továbbá megbéníthatják az üzemfolytonosságot, illetve az ügy- és üzletmenet-folytonosságot.

A kritikus szervezetek az általuk nyújtott szolgáltatástól függően, de jellemzően IT-rendszerek mellett kiberfizikai (OT-) rendszereket is alkalmaznak. Ezeknek a kiberfizikai rendszereknek a szerepe, hogy az egyes ipari folyamatokat irányítsák. Az ipari vezérlőrendszerek segítségével megfelelő felügyeleti kontrollt képesek ezen szervezetek biztosítani folyamataikra. Ugyanakkor fontos megemlíteni, hogy ezen ipari rendszerek jellemzően kevesebb védelmi képességgel rendelkeznek, mint az IT-rendszerek, így amennyiben hálózatra vannak kapcsolva, sérülékenyek lehetnek a kibertérből érkező támadási kísérletekkel szemben. Ezek az ipari vezérlőrendszereket ért sikeres kibertámadások már képesek lehetnek az ipari folyamatokba beavatkozni és akár negatív hatást gyakorolni fizikai világunkra.

Sérülékenységi statisztika

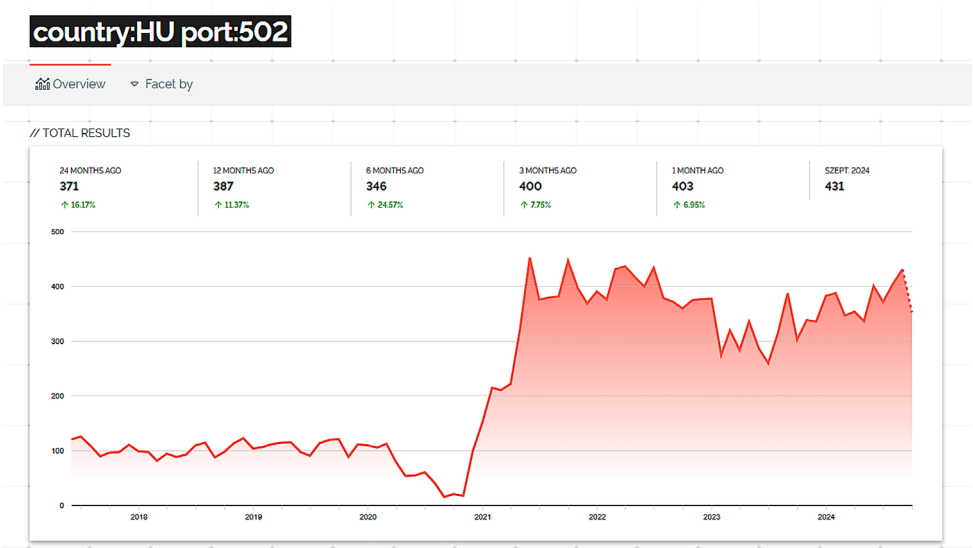
Eltérően a hagyományos keresőktől, a Shodan nem weboldalakra, hanem olyan hálózati eszközökre koncentrál, mint az Internet of Things (IoT) eszközök, szerverek, ipari vezérlőrendszerek, webkamerák és routerek. A keresőmotor az internetre csatlakozó eszközök nyitott portjait és egyéb alapinformációit gyűjti össze, így a biztonsági szakemberek számára értékes adatforrás lehet. Lehetőség van IP-cím, nyitott portok, használt protokollok, szoftververziók és geolokációs adatok alapján keresni.[7]

A Shodan elsősorban etikus hackerek és kiberbiztonsági szakemberek eszköze, amelyet az internetre csatlakozó eszközök biztonsági állapotának vizsgálatára használnak. A nyitott portokon keresztül elérhető eszközök adatai érzékenyek lehetnek, és a jogosulatlan hozzáférés büntetőjogi felelősséggel járhat. A platform segítségével olyan portokat is lehet keresni, amelyek ipari vezérlőrendszerekhez tartoznak, és nyitva vannak az internet felé.

Az ipari hálózatok több olyan portot használnak, amelyek rendszerelemekhez biztosítanak hozzáférést, például vezérlőkhöz, szenzorokhoz és egyéb hálózati eszközökhöz. A tanulmány három olyan nyitva lévő portot mutat be, amely potenciálisan veszélyeztetheti az ipari rendszereket; az adatok anonimizáltak. Az 1., a 2. és a 3. ábra az internet felé nyitott magyarországi portok számát és az elmúlt évek trendjeit (növekedés vagy csökkenés) szemléltetik.

A Modbus TCP/IP egy elterjedt ipari protokoll, és az 502-es portot használja. Gyakran használják ipari vezérlőrendszerekben, és ha nyitva van az internet felé, az veszélyes lehet, így a támadók akár érzékeny adatokat is kiolvashatnak, vagy manipulálhatják a vezérlési parancsokat. Valamint ez a hozzáférés lehetőséget adhat a támadóknak az ipari folyamatok megzavarására, vagy akár a termelési vagy munkafolyamatok leállítására. 2024 szeptemberében 431 darab magyarországi potenciálisan sérülékeny ipari rendszerelem

[7] *What is Shodan?* [é. n.].



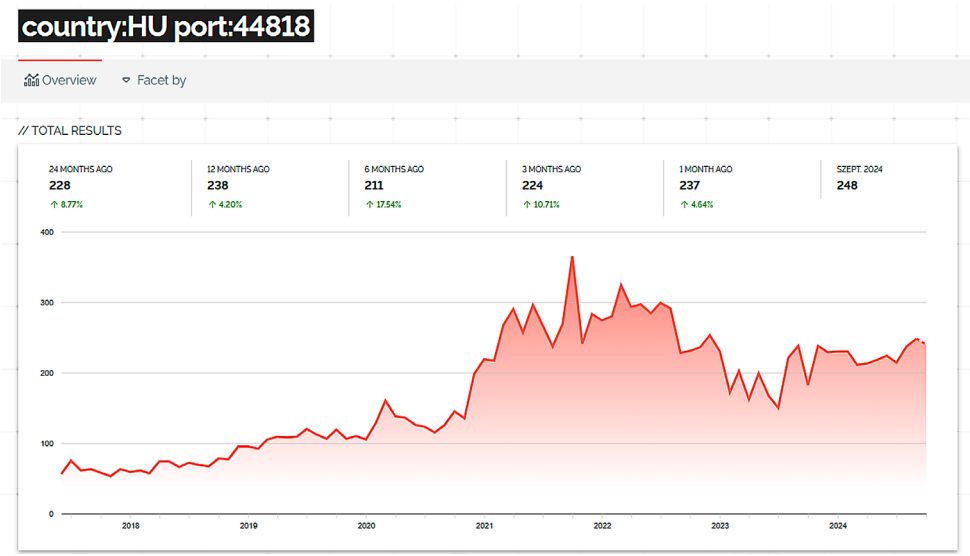
1. ábra: 502-es porton keresztül nyitva lévő magyarországi sérülékeny rendszerelemek számának alakulása
Forrás: Shodan keresőmotor Trends felületének képernyőképe a nyitott 502-es portokkal rendelkező magyar rendszerelemekről, https://www.shodan.io

volt elérhető ezen a nyitott porton keresztül. Az ilyen típusú hozzáférések kockázatait és a lehetséges támadások detektálását mesterséges intelligencia alkalmazásával hazai kutatók vizsgálták egy Modbus-alapú szimulált környezetben, kimutatva, hogy gépi mélytanulási és statikus tanulási módszerek ígéretesek lehetnek hálózati csomagokkal kapcsolatos anomáliák azonosításában.[8]

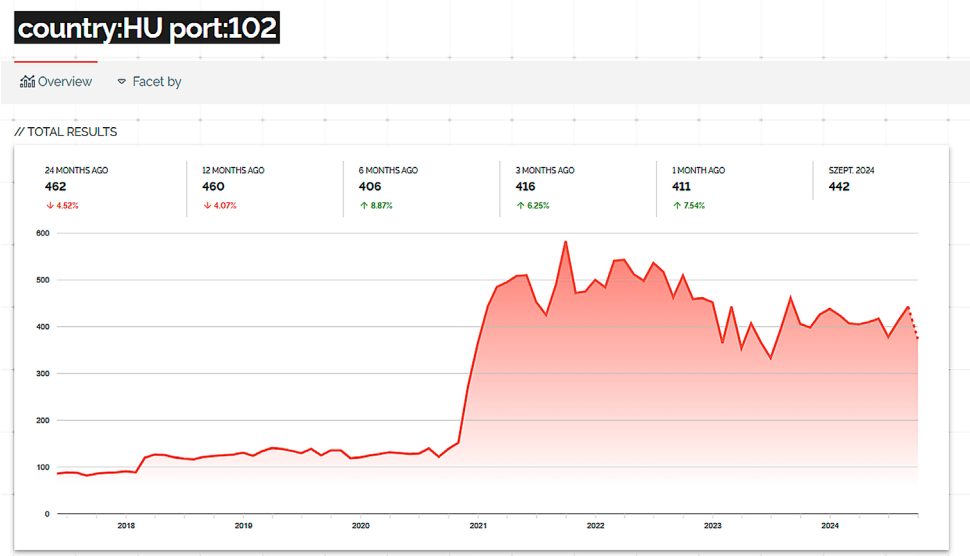
Az internet felé nyitott 44818-as port jelentős biztonsági kockázatot hordoz, mivel az EtherNet/IP protokollt használja, amelyet gyakran alkalmaznak ipari vezérlőrendszerekben, például programozható logikai vezérlőkben (PLC). Ha ez a port védelem nélkül elérhető az interneten, a jogosulatlan behatolók képesek lehetnek hozzáférni a vezérlőkhöz, és így manipulálhatják az ipari folyamatokat, leolvashatják vagy módosíthatják a vezérlési paramétereket, illetve leállíthatják az eszközöket. A szerzők a kutatás idején 248 darab magyarországi potenciálisan sérülékeny ipari rendszerelemet találtak, amelyek ezen a porton keresztül elérhetők voltak.

Az internet felé nyitott 102-es port is rejthet kiberbiztonsági rizikót egy szervezet számára, mivel ezt a portot a Siemens S7 protokoll használja, amelyet gyakran alkalmaznak ipari vezérlőrendszerekben, különösen PLC-k kommunikációjához. Ha ez a port nyitva van és védtelen az interneten, a támadók hozzáférhetnek az ipari vezérlők parancsaihoz és adatfolyamaihoz, lehetővé téve számukra a rendszer működésének manipulálását, a termelési folyamatok megzavarását, túlterhelését vagy leállítását.[9] A kutatás idején

[8] Dobrády–Takács–Hidvégi 2023: 62–68.
[9] CISA 2023a.



2. ábra: A 44818-as porton keresztül nyitott hazai rendszerelemek számának alakulása az elmúlt években
Forrás: Shodan kereső Trends felületének képernyőképe a nyitott 44818-as portokkal rendelkező hazai rendszerelemekről, https://www.shodan.io



3. ábra: A 102-es porton keresztül nyitott hazai rendszerelemek számának alakulása az elmúlt években
Forrás: Shodan keresőmotor Trends felületének képernyőképe a nyitott 102-es portokkal rendelkező hazai rendszerelemekről, https://www.shodan.io

442 darab magyarországi a 102-es porton keresztül nyitott rendszerelem volt megtalálható a Shodan keresőfelülettel.

A nyitott port önmagában nem zárható ki pusztán portokollszintű megoldásokkal, azonban az ipari kommunikáció titkosítása jelentősen csökkenti a támadók által megszerezhető információ értékét. Ezzel a megközelítéssel foglalkozott Antal József és Hidvégi Timót is, akik olyan titkosított ipari kommunikációs protokollt és tesztkörnyezetet dolgoztak ki, amely képes biztosítani a csomagok védelmét az illetéktelen olvasással és manipulációval szemben, még akkor is, ha a hálózati elérés technikailag lehetséges marad a fent bemutatott portokon keresztül. További előnye, hogy ez a kriptográfiai protokoll meglévő rendszerekbe is integrálható.[10]

Esettanulmányok

Colonial Pipeline

A Colonial Pipeline elleni kibertámadás 2021 májusában történt, és az Amerikai Egyesült Államok egyik legnagyobb kritikus infrastruktúra elleni zsarolóvírus-támadása volt, amely nyilvánosságra került. A Colonial Pipeline az Egyesült Államok egyik legjelentősebb olajvezetéke. Ezen keresztül történik az olaj szállítása a Mexikói-öbölből a keleti parti államokba. A támadók, a feltehetőleg kelet-európai kötődésű DarkSide nevű hackercsoport egy virtuális privát hálózathoz (VPN) tartozó jelszó kiszivárgását kihasználva fért hozzá a Colonial Pipeline informatikai hálózatához, ahol 100 GB adatot loptak el, majd zsarolóvírust telepítettek. A támadás több lépcsőben zajlott a Colonial Pipeline informatikai rendszerei ellen. A csővezeték kiberfizikai (OT) rendszerei, amelyek ténylegesen felelnek az olajszállításért, nem kerültek közvetlen veszélybe a támadás során. Azonban a vállalat megelőző intézkedésként leállította az üzemanyag-ellátó rendszert, amelynek kiesése jelentős hiányt és pánikot okozott az Egyesült Államok keleti partján. A vállalat 75 bitcoin (mintegy 4,4 millió dollár) váltságdíjat fizetett a támadóknak a rendszerei és adatai visszaállításáért, azonban a hatóságok később visszaszereztek abból 63,7 bitcoint (körülbelül 2,3 millió dollár).

A DarkSide hackercsoport tagjai nem állami háttérrel működő kiberbűnözők. Állításuk szerint egészségügyi, oktatási, állami és nonprofit szervezetek ellen nem követnek el kibertámadást. Elsődleges működési modelljük az RaaS (Ransomware as a Service), ransomware vírusokat fejlesztenek és terjesztenek más kiberbűnözői szervezetek számára, amelyek aztán önállóan végzik a vírusok telepítését a célpont hálózatokon, a váltságdíjak egy bizonyos százalékát a vírus fejlesztői kapják meg. A DarkSide Ransomware egy olyan RaaS, amely gyakran alkalmaz kettős zsarolási taktikát. A célhálózatba való beszivárgás után az érzékeny adatokat titkosítja, és váltságdíjat követel azok feloldásáért cserébe. Emellett a kiberbűnözők azzal is fenyegetőznek, hogy ha nem fizetik ki a váltságdíjat, nyilvánosságra hozzák a megszerzett adatokat, vagy a dark weben keresztül értékesítik azokat.

A DarkSide az adathalászatot, a gyenge hitelesítő eszközöket és az ismert sebezhetőségeket (például a CVE-2021-20016-ot, a SonicWall SMA100 SSL VPN megoldás

[10] Antal–Hidvégi 2021: 106–112.

SQL-injekcióját) használja fel a rendszerekhez való kezdeti hozzáférés megszerzéséhez. Ezután a kártékony kód rendszergazdai jogosultságokat szerez, megkerülve az UAC-t a CMSTPLUA COM interfész segítségével, így a támadók teljes hozzáférést kapnak az érzékeny adatokhoz, illetve fontosabb műveletek végrehajtásához. A fájlok titkosítására Salsa20 szimmetrikus titkosítási kulcsot használ, majd egy RSA-1024 aszimmetrikus kriptográfiai algoritmus publikus kulcsával titkosítja a Salsa20 kulcsot, így annak feloldása csak az RSA privát kulcsával lehetséges (ez a támadóknál van). Ez a módszer azért hatékony, mert a Salsa20 gyors, míg az RSA-1024 lehetővé teszi a Salsa20 kulcs megfelelő erősségű titkosítását.[11]

A Colonial Pipeline Company elleni kibertámadásnak szinte azonnali hatása volt, hiszen az üzemanyag-ellátás üzemfolytonossága megszakadt, ami számos negatív következménnyel járt. A légi közlekedés esetén számos légitársaságnál, köztük az American Airlinesnál üzemanyaghiány lépett fel, így a keleti parti reptereken korlátozott fennakadások alakultak ki. Emellett az Amerikai Egyesült Államok társadalmi mobilitásának alappillére a személygépkocsik széles körű használata, így a lakosság körében a benzinhiánytól való félelem pánikvásárlást eredményezett, aminek következtében az üzemanyagok ára is jelentősen megnőtt, valamint egyes területeken üzemanyaghiány lépett fel, mivel a fogyasztók a megszokottól eltérően jelentős többletüzemanyagot vásároltak.[12]

A CISA elemzése a Colonial Pipeline elleni 2021-es zsarolóvírus-támadás kapcsán hangsúlyozza az amerikai kritikus infrastruktúrák sebezhetőségét és a kiberbiztonsági intézkedések fontosságát. A támadás nyomán az Egyesült Államok kormánya számos intézkedést hozott, beleértve a Shields Up kampányt, a Joint Ransomware Task Force létrehozását, valamint a CyberSentry kibervédelmi program bővítését. 2021 májusában a Biden-kormányzat végrehajtási rendeletet adott ki, amelyben utasította az amerikai állami szerveket, hogy hajtsanak végre proaktív lépéseket a kiberbiztonság megerősítése érdekében.[13]

Német kórházak elleni támadás

2023. december 24-én több német kórház is kibertámadás áldozatává vált, amely mögött a Lockbit nevű kiberbűnözői csoport állt. A támadók célpontjai a Kelet-vesztfáliai Katolikus Kórházi Szövetség (KHO) intézményei voltak. A Szövetségbe tartozó hat kórházból háromnál történt szolgáltatás-összeomlás a Lockbit 3.0 ransomware támadás következtében. A támadások súlyosan érintették a kórházak működését támogató rendszereket, ezek aztán több sürgősségi ellátás megszakadását is okozták.

A kórházak IT-hálózatához hozzáférve a támadók titkosították az adatokat, az első tesztek alapján egyértelmű volt, hogy ransomware támadás történik. A támadás hatókörébe tartozó rendszerek visszaállítási ideje nem volt előre meghatározható. A kórházak központi IT-osztálya leállította az összes rendszert, és gondoskodott az intézmények értesítéséről. A kórházak kritikus szerepet játszanak az egészségügyi szolgáltatások nyújtásában az adott

[11] Chiscariu 2021.
[12] Kerner 2022.
[13] Easterly 2023.

régióban, így egy, az informatikai rendszereiket érintő kibertámadás súlyos következményekkel járhat az orvosi vészhelyzetben lévő emberek számára.

A KHO közleménye egyértelművé teszi, hogy a betegellátás a normális keretek között folytatódott az érintett kórházakban, és minden klinikai tevékenység továbbra is elérhető volt, bizonyos technikai korlátozásokkal. A biztonsági mentések sikeres helyreállítása révén a betegek alapvető adatai továbbra is hozzáférhetők maradtak. A sürgősségi ellátás azonban a három KHO-kórházban nem volt elérhető, így a sürgős orvosi ellátásra szoruló embereket máshová irányították, ami kritikus késedelmeket okozhatott, valamint általános elégedetlenséget szült az érintett kórházakkal szemben, a német egészségügy feltehetően reputációbéli veszteséget könyvelhetett el.[14]

Nem található arra vonatkozó információ, hogy a támadók hogyan jutottak be a kórházak IT-hálózatába, azonban a Lockbit Ransomware-t (RaaS) használók gyakran a sebezhető Remote Desktop Protocol (RDP) szerverek vagy a dark weben vásárolt, kompromittált hitelesítő adatok használatával szerzik meg a kezdeti hozzáférést. A kezdeti hozzáférési vektorok közé tartoznak még az e-mailek rosszindulatú mellékletei vagy a linkeket tartalmazó adathalász e-mailek, illetve a Fortinet VPN-ek olyan sebezhetőségének kihasználása, mint például a CVE-2018-13379.

A hitelesítő eszközök megszerzésére, valamint a hálózat felderítésére gyakran ingyenesen elérhető, legális eszközöket, szoftvereket használnak fel, ilyen például az AdFind GMER és a Mimikatz, ezek mellett gyakran alkalmaznak penetrációs vizsgálatokhoz használt eszközöket, mint a Cobalt Strike és a Metasploit. A vírus laterális-oldalirányú terjedéssel más, a hálózatban részt vevő rendszerelemeket is képes célba venni.

A LockBit AES és RSA titkosítást használ a fájlok enkriptálására. A vírus csak az első néhány kilobájtot titkosítja a gyorsabb működés érdekében, valamint az érintett fájlhoz egy *.lockbit* kiterjesztést fűz, ezzel jelezve, hogy titkosítva van. Ezt követően a vírus lecseréli az asztali háttérképet egy váltságdíjat követelő üzenetre, amennyiben pedig a megtámadott eszközre vagy hálózatra nyomtatók is csatlakoztatva vannak, a váltságdíjat követelő üzeneteket automatikusan kinyomtatja, hogy az áldozatok biztosan észrevegyék, hogy az adataik kompromittálódtak. Ennél az esetnél nem kerültek nyilvánosságra az utólagos vizsgálat eredményei, így nem derült ki, hogy a kiberbűnözők ellopták-e a betegek adatait vagy más érzékeny információkat.[15]

Az elmúlt években számos kibertámadásért a LockBit Ransomware volt a felelős, aminek megállítása érdekében az Europol, az FBI és a brit Nemzeti Bűnüldözési Ügynökség egy összehangolt nyomozás keretében végül 2024 februárjában elfogta a zsarolóvírust fejlesztő kiberbűnözői banda feltételezett vezetőjét, akit vád alá helyeztek és elítéltek. Természetesen a támadások nem értek véget, hiszen a Lockbit 3.0 zsarolóvírus szolgáltatásként történő értékesítése (RaaS) a mai napig tart. A többi vezető felkutatásáért 10 millió dolláros nyomravezetői díjat tűzött ki az amerikai kormány. A japán rendőrség által kifejlesztett LockBit 3.0 dekódoló elérhető a NoMoreRansom weboldalán, a felhasználásával nagy valószínűséggel a titkosított adatok visszaszerezhetők váltságdíj megfizetése nélkül.[16]

[14] Toulas 2023.
[15] CISA 2023b.
[16] Euronews 2024.

Ez az eset rávilágít arra, hogy az Európai Unió alapvető szolgáltatásokat nyújtó szervezetei ki vannak téve a kibertámadásoknak, amelyek akár emberéleteket is veszélyeztethetnek, valamint zavart kelthetnek a társadalomban. A hatékony megelőzés és védelem kialakítása érdekében az Európai Unió NIS2 és CER direktívái által szorgalmazott védelmi intézkedések megfelelő implementációja csökkentheti az ilyen jellegű támadások sikeres bekövetkezésének valószínűségét.

Dán villamosenergia-rendszer elleni kibertámadás-sorozat

A dán SectorCERT, amely Dánia kritikus infrastruktúrái felett lát el kiberbiztonsági felügyeletet, mint incidenskezelő központ publikált a dán villamosenergetikai szervezeteket ért kibertámadásokról egy részletes tanulmányt. A támadók összesen, két hullámban, 22 sikeres támadást hajtottak végre energiaszektorbéli szervezetek ellen. A jelentés szerint államilag támogatott támadócsoportokról lehet szó, amelyek előre kiválasztott célpontokat vettek célba alaposan előkészített, fejlett technikákkal. Az elkövetők pontosan tudták, mely szervezeteket érdemes megcélozniuk, és milyen sérülékeny rendszerelemeket kell támadniuk. Továbbá a támadásra utaló jeleket igyekeztek elfedni az áldozatok hálózati forgalmában.

A támadások első hulláma 2023. május 10-én kezdődött, a támadók a CVE-2023-28771 sérülékenységet használták ki, amely a Zyxel tűzfalak egyik súlyos biztonsági hibája volt. A sebezhetőség lehetővé tette a támadók számára, hogy egy speciálisan kialakított hálózati csomagot az 500-as porton keresztül küldve teljes irányítást szerezzenek az érintett tűzfal felett, anélkül, hogy felhasználóneveket vagy jelszavakat kellett volna ismerniük. Ez azért különösen súlyos, mert maga a tűzfal az első védelmi vonal a kritikus rendszerekhez való hozzáférés megakadályozásában. Azonban a támadókat leleplezték és még idejében kizárták a megtámadott szervezetek hálózataiból, köszönhetően a SektorCERT, a tűzfal beszállítói és a szervezetek szakemberei együttes erőfeszítéseinek.

A támadássorozat második hulláma 2023. május 22-én kezdődött, ekkor a támadók már új technikákat és eszközöket vetettek be. Az egyik energetikai szervezet tűzfalára egy nem biztonságos kapcsolaton keresztül új szoftvert töltöttek le, ami gyanút keltett. A tűzfal ezután úgy kezdett el viselkedni, mintha egy botnet részévé vált volna, a támadók egy elosztott szolgáltatásmegtagadással járó támadást (DDoS) készítettek elő a rendszerelemek megfertőzésével. A kompromittált szervezet eszköze két célpontot érintő DDoS-támadásban vett részt az Egyesült Államokban és Hongkongban. Ekkor a SektorCERT értesítette az áldozattá vált szervezetet, amely azonnal szigetüzemre állt át, a tűzfal beszállítója pedig segített újrakonfigurálni a kompromittálódott eszközt, valamint meggyőződtek arról, hogy a támadók a DDoS-támadásokon kívül másra nem használták a hozzáférést. Ezt követően ismét hasonló incidens történt a tűzfallal, így a szervezet szigetüzemre állt vissza.

Május 23-án egy másik energetikai szervezet infrastruktúráját kompromittálták, hogy Secure Shell (SSH) kriptográfiai protokollon keresztüli brute-force – vagyis olyan automatizált módszer, amely különböző jelszó- vagy kulcskombinációkat próbál végig

a hozzáférés megszerzése érdekében – támadásban használják fel egy kanadai szervezet ellen, a SektorCERT és a dán cég végül ki tudta zárni a támadókat a kompromittált hálózatból.

Május 24-én a SektorCERT felügyelete alá tartozó négy energetikai vállalat tűzfala kompromittálódott egy MIPSkiller nevű rosszindulatú kódsor miatt (payload) és kezdett el DDoS-támadásokban önkéntelenül részt venni, ameddig meg nem szakították a hackerek irányítását. Egy esetben a tűzfal túlterhelődött és leállt, ami az adott szervezet hálózatának leállását is előidézte. Az egyik szervezet kamerarendszere volt egy Zyxel tűzfal mögött, amit szintén kihasználtak, és a MIRAI Moobot része lett.

A második hullámú támadásoknál feltűnő volt, hogy a támadók olyan sérülékenységekről is tudhattak, amelyeket a Zyxel még nem hozott nyilvánosságra. A SektorCERT a támadások elemzése alapján úgy vélte, hogy a május 11-én észleltektől eltérő típusú támadásról van szó. Ez gyakorlatilag zero-day támadás volt, mert olyan sérülékenységeket használt ki, amelyek nem voltak ismertek akkor, a tűzfal gyártója napokkal később jelentette ezeket (CVE-2023-33009 és CVE-2023-33010).

Május 24-én este a SektorCERT a Sandworm APT csoportra utaló hálózati forgalmat azonosított a riasztás alapján. Az APT csoport jellemzően akkor kezd el műveleteket végrehajtani, ha valamely állam működését politikai vagy katonai megfontolások miatt meg akarják zavarni. A támadók ügyeltek arra, hogy észrevétlenek maradjanak, a kompromittálódás után mindössze egyetlen csomagot küldtek vissza, (egy pinget) a hálózati forgalommal. Jellemzően ezek tesztkapcsolatok a támadó command and control (C2) szerverével vagy egy rejtett azonosító jelzés, amely megerősíti a támadók számára, hogy sikerült kompromittálni a rendszert, és az elérhetővé vált számukra. A Sandworm csoportra utaló jelek megjelenésekor a SektorCERT a dán rendőrségen belül működő Nemzeti Kiberbűnözési Központ bevonása mellett döntött. Az érintett szervezet tűzfalát lefoglalták, hogy a lehető legtöbb bizonyítékot szerezhessék meg. Így a vállalat 6 napig szigetüzemben működött, amíg az addig használt Zyxel tűzfalakat nem cserélték le más márkájúakra.

Másnap egy másik létfontosságú szervezetnél ismétlődött meg a Sandworm-féle támadás, azonban itt már a távoli ipari rendszerek elérhetetlenné váltak a szervezet központi felügyeleti rendszere számára, mert a megtámadott tűzfal belső routerként is működött az OT-hálózatban, ezért az üzemnek manuális irányításra kellett átállnia a távoli helyszíneken is. Párhuzamosan ezzel a támadással másik két biztonsági incidens is volt, a nyomok alapján azonban itt más típusú támadás történt a tűzfalakkal szemben, vélhetően más elkövetők álltak mögötte.

Amint a dán kritikus infrastruktúrák által alkalmazott tűzfal-sérülékenységek nyilvánosságra kerültek, a dán kritikus szervezetek elleni támadási kísérletek száma drasztikusan megnőtt főként lengyel és ukrán IP-címekről, azonban eddigre már ezen IT- és OT-hálózatok tűzfal-sérülékenységeit kijavították, így a támadási kísérletek sem voltak hatásosak. A támadások után az amerikai CISA is felvette a Zyxel tűzfalak sérülékenységeit az aktívan kihasználható sebezhetőségek listájára.[17]

Az esettanulmány rávilágít arra, hogy a dán energetikai infrastruktúrák hatékony és gyors reagálású védekezési képessége a SektorCERT-nek, a beszállítóknak és az adott szervezeteknek az együttműködésével valósulhatott meg. Ennek köszönhetően meg lehetett állítani a további eszkalációt, ami súlyos következményekkel járt volna a szolgáltatás

[17] SektorCERT 2023.

folytonosságára és magára a kiberfizikai rendszerekre nézve is, valamint a dán nemzetbiztonságra. A jövőben gondoskodni kell arról, hogy rendszerszintű sérülékenységek ne forduljanak elő egy-egy ágazat szereplőinek infrastruktúráiban, amelyek kihasználása révén a támadók egy időben tudnak végrehajtani célzott támadásokat valamennyi szereplő ellen. A folyamatos biztonság fenntartása érdekében számos olyan védelmi intézkedést szükséges bevezetni, amely a kockázatokkal arányos módon biztosítja egy-egy szervezet kibervédelmi képességét, ezek tételes ismertetésére a jelentés kitér.

A CER és a NIS2 irányelv szerepe a hazai kritikus szervezetek esetén

Az Európai Unió kritikus szervezeteinek és kritikus infrastruktúráinak fokozott kiberkitettségei és fizikai sebezhetőségei ellen az Európai Parlament és a Tanács még 2022 decemberében kiadta a két irányelvét, hogy előmozdítsa az Unióban lévő fontos és alapvető szolgáltatást nyújtó szervezetek teljes körű rezilienciájának kialakítását.[18] Hazánk kritikus szervezeteire az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedések érvényesek, *az Európai Parlament és a Tanács (EU) 2022/2555 irányelve a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről* (a továbbiakban: NIS2), illetve *az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről* (a továbbiakban: CER) irányelv hazai jogszabályai is vonatkoznak, aminek köszönhetően ezen szervezetek képesek lesznek egy hatékony, a kockázatokkal arányos védelmi képességet kialakítani. A NIS2 irányelv 15 ágazatra terjeszti ki a hatályát, így nemcsak a kritikus infrastruktúrák, hanem egyéb, nemzetbiztonsági szempontból kiemelt szervezetek is a hatókörébe tartoznak. Az egységes uniós szabályozás elősegíti a tagállamok együttműködését, gyorsabbá és hatékonyabbá téve az incidenskezelést. Magyarország számára ez magasabb szintű kiberbiztonsági védelmet, hatékonyabb incidenskezelést és erősebb nemzetközi együttműködést jelent, elősegítve a digitális gazdaság és az ipari szektor biztonságos fejlődését. A hatósági felügyelet, a szigorúbb biztonsági követelmények és auditok ösztönözhetik a szervezeteket a kiberbiztonság folyamatos fejlesztésére, ezáltal növelve a kockázatos ágazatok ellenálló képességét a kibertámadásokkal szemben. Az irányelvet a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény, annak végrehajtási rendelete, valamint a 7/2024 (VI.24.) MK rendelet implementálta a hazai jogrendbe. A jogszabály hatálya alá tartozó szervezetek számára magas szintű kiberbiztonsági követelmények teljesítése szükséges, beleértve a kockázatkezelési keretrendszerek kialakítását, a beszállítói lánc értékelését és a rendszeres biztonságtudatossági képzéseket. A szervezeteknek kiemelt figyelmet kell fordítaniuk az incidensek kezelésére, kivizsgálására, az üzletmenet-folytonosság biztosítására és a gyors helyreállásra. Az üzemeltetőknek biztosítaniuk kell a rendszereik folyamatos felügyeletét, ennek keretében többek között sérülékenységvizsgálatokat kell lefolytatniuk, és független auditokon kell megfelelniük az amerikai NIST 800-53 rev5[19] dokumentumon alapuló 7/2024 MK rendelet követelményeinek. A követelmények számosságát a szervezet

[18] Ambrusz–Dobor–Vásárhelyi 2024: 57–69.
[19] National Institute of Standards and Technology 2020.

rendszereinek száma és azok biztonsági osztályai (alap, jelentős, magas) befolyásolják. Azoknak a szervezeteknek, amelyeket a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) 2025. január 1. előtt nyilvántartásba vett, az idei év végéig kell számot adniuk felkészültségükről az első kiberbiztonsági audit során. Ha egy kritikus szervezet többségi tulajdona az államhoz köthető, annak ellenőrző és felügyeleti hatósága a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI). Amennyiben a szervezet felett egy gazdálkodó szervezet rendelkezik döntő tulajdoni hányaddal, a felügyeleti hatósági szerepkört az SZTFH tölti be.[20]

Magyarország, mint valamennyi tagállam, kijelölt egy nemzeti incidenskezelő központot és nemzeti kiberbiztonsági hatóságot is, mindkét szerepkört az NBSZ NKI látja el. A nemzeti kiberbiztonsági hatóság feladatai közé tartozik a kritikus szervezetek és az ország szempontjából jelentős szervezetek információbiztonsági szabályzatainak továbbítása a nyilvántartó hatóság számára, valamint az elektronikus információs rendszerek biztonságáért felelős személyek (IBF-ek) listájának közzététele. Az SZTFH által biztosított adatok figyelembevételével összeállítja az alapvető és fontos szervezetek jegyzékét, amelyet kétévente felülvizsgál. A hatóság jogosult sérülékenységvizsgálatok elvégzésére, akár hivatalból, akár az érintett szervezet kérésére. A nemzeti kiberbiztonsági hatóság alapvető vagy fontos szervezetként azonosíthatja azon szervezeteket, amelyek eddig valamilyen okból kifolyólag nem jelentkeztek be a hatóságnál, továbbá jogosult a szervezetek rendszereinek biztonsági osztályait felülbírálni.

A nemzeti kiberbiztonsági incidenskezelő központ feladata a kiberfenyegetések és incidensek kezelése, valamint a kritikus infrastruktúrák és szervezetek védelmének támogatása. Valamennyi, a NIS2 hatálya alá tartozó szervezetnek kötelessége haladéktalanul jelenteni minden releváns fenyegetést, incidensközeli helyzetet és kiberbiztonsági eseményt, ideértve az üzemeltetési incidenseket is. A központ proaktív, behatolásmentes sérülékenységvizsgálatokat végez a nyílt interneten elérhető rendszerek biztonsági állapotának felmérése céljából, és szükség esetén egyedi vizsgálatokkal is támogatja a szervezeteket. Emellett részt vesz a kiberbiztonsági stratégiák és szabályozások kidolgozásában, valamint szabványosított gyakorlatokat, ajánlásokat és kötelező érvényű állásfoglalásokat adhat ki az incidensek megelőzésére és kezelésére. A központ szükség esetén működtetheti a kormányzati információtechnológiai és kiberbiztonsági incidenskezelési együttműködési fórumot.

A NIS2 és CER irányelvek egymást kiegészítve erősítik az európai uniós kritikus szervezetek és infrastruktúrák rezilienciáját. A CER irányelv előírja a kritikus szervezetek azonosítását, a kockázatok értékelését, a fizikai védelmi intézkedések biztosítását, továbbá deklarálja a kiberbiztonsági védelmi intézkedések meglétének fontosságát. Magyarország és az EU számára ez megerősíti az ellátási láncok stabilitását, a közszolgáltatások védelmét és az állampolgárok biztonságát. A CER irányelv emellett elősegíti a tagállamok érintett hatóságai közti együttműködést és gyors reagálást válsághelyzetekben, így csökkentve az infrastruktúrákat érintő támadások és katasztrófák hatásait. Hazánk az irányelvet a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény (a továbbiakban:

[20] Marsi–Orosházi 2025, 94. epizód.

Kszetv.), valamint annak végrehajtási rendelete, a 474/2024 (XII. 31.) Korm. rendelet által implementálta a hazai jogrendbe. A jogszabályi keret célja a magyarországi székhellyel rendelkező kritikus szervezetek ellenálló képességének növelése az alapvető szolgáltatások folyamatosságának biztosítása érdekében. Részletesen foglalkozik az egyes ágazatokkal és alágazatokkal, például az energetikai ágazattal. Az új törvény új fogalmakat vezet be, mint például a *kritikus szervezet,* a *kritikus szervezet ellenálló képességéért felelős vezető.* Előírja a kritikus szervezetek ellenálló képességére vonatkozó nemzeti stratégia és nemzeti kockázatértékelés kidolgozását, amely segíti a kritikus szervezetek kockázatértékelési tevékenységeit, és amelyet adott szervezet figyelembe vesz, amikor a saját kockázatértékelését, ellenálló képességi mátrixát és ellenálló képességi intézkedéseit hozza meg. Ennek az új szerepkörnek a betöltéséhez elengedhetetlen az NKE Katasztrófavédelmi Intézete által biztosított kritikusinfrastruktúra-védelmi biztonsági összekötő személy szakirányú továbbképzési szak elvégzése. Az Intézet a vonatkozó hazai jogi környezet figyelembevételével, valamint több mint két évtizedes iparbiztonsági oktatási tapasztalataira építve alakította ki a képzés tananyagát és struktúráját.[21]

A kritikus szervezeteknek ellenálló képességi tervet kell kidolgozniuk, és belső auditokat kell végezniük annak érdekében, hogy megfeleljenek a 474/2024 (XII. 31.) Korm. rendeletben előírt követelményeinek. Az állam az ellenálló képesség kialakítására támogatást nyújthat megfelelő szakmai útmutatók és segédletek kidolgozásával. A szabályozás kiemelten kezeli a határokon átívelő együttműködéseket, és létrehoz egy egyedüli kapcsolattartó pontot, amely az Európai Bizottsággal és más országok egyedüli kapcsolattartó pontjaival működik együtt. Az ellenőrző hatóság jogosult ellenőrzéseket végezni, szükség esetén pedig szankcionálni. Amennyiben a Kszetv.-ben előírtaktól a NIS2 hazai jogszabályai eltérően rendelkeznek, akkor az azokban foglaltak élveznek elsőbbséget. A szabályozás célja a proaktív védelem, vagyis a kockázatok előzetes felismerése és kezelése.

A kritikus szervezeteknek a fent felsorolt követelményeken túl szükséges a törvény végrehajtási rendelete által meghatározott biztonsági követelményeket teljesíteniük attól függően, hogy az általános ágazatkijelölő hatóság a három ellenálló képességi szint közül melyikbe sorolta. Az ellenálló képességi szintbe történő besoroláskor az illetékes hatóság figyelembe veszi az érintett kritikus szervezet által beküldött dokumentumokat, valamint a jogszabály 1. számú melléklete által meghatározott horizontális kritériumok teljesülését. A besorolásról hivatalos értesítést kapnak az érintett szervezetek.

A kritikus szervezetek rezilienciáját szabályzó hazai jogszabályok ezen szervezetek ellenálló képességének növelését célozzák, valamint azon túlmenően hozzájárulnak Magyarország nemzetbiztonságának megerősítéséhez is. A szabályozás meghatározza a szervezetek kijelölésének, ellenálló képességi szintbe sorolásának és kockázatértékelésének kereteit, miközben előírja az ellenálló képességi tervek kidolgozását, bemutatja a hatósági ellenőrzés és felügyelet rendszerét, valamint ismerteti a szintbe sorolástól függően és függetlenül megvalósítandó követelménykatalógus kontrolljait. Azonban ezen jogszabályok nem rendelkeznek az alapvető szolgáltatást igénybe vevő lakosság felkészítéséről, ha ezen infrastruktúrák egyesével vagy csoportosan kompromittálódnak.

[21] Kátai-Urbán – Bleszity – Vass 2025: 220–236.

A lakosságvédelem nemzetbiztonsági aspektusai

Napjaink információs társadalmában már elengedhetetlen, hogy a lakosságvédelmi tájékoztató kiadványok és a lakosságfelkészítő anyagok ne csak nyomtatott formában létezzenek, hanem széles körben, online is elérhetők legyenek. A lakosság digitális platformokon keresztül való felkészítése a válsághelyzetekre csökkenti a nemzetbiztonsági kockázatokat, mert minimalizálhatja azok kialakulásának valószínűségét. Mindez elősegíti az állami erőforrások hatékonyabb felhasználását, lehetővé téve azok célzottabb alkalmazását preventív intézkedésekben és válságkezelésben. Azonban napjainkban a lakosságot a természeti és civilizációs katasztrófák, valamint azok hatásai mellett fel kell készíteni az álhírek kiszűrésére is, ki kell alakítani a lakosság megfelelő médiaműveltségét.[22] Ez segít ellensúlyozni a dezinformációs kampányok és a digitális médián keresztül terjedő álhírek hatásait. Az Európai Unió 2022-ben kiadta a megerősített *Dezinformációs Gyakorlati Kódex*ét,[23] amelynek célja a dezinformáció elleni fellépés és az átláthatóság fokozása; ez egy önszabályzó keretrendszer, a benne foglaltakat az azt aláíró online platformok önként vállalják. Ennek a kódexnek részét képezi a felhasználói tudatosság növelése, valamint független tényellenőrző szervezetek működtetésének (fact-checkers) a lehetősége. Ma a dezinformációs kampányok súlyos nemzetbiztonsági kihívást jelentenek valamennyi állam számára. Ezek ellen a leghatásosabb védelem a lakossági médiaműveltségi programok elindítása. Néhány uniós tagállam ezeket már középiskolás kortól, a közoktatás infrastruktúráját is felhasználva alkalmazza. Jelenleg Magyarországon még nem elterjedtek ezek a médiaműveltségi programok, azonban az Európai Unió honlapján számos magyar nyelvű oktatóanyag és videó is elérhető a témával kapcsolatban.[24] Az EU Külügyi Szolgálata (EEAS) létrehozta az East StratCom Task Force-t, amelynek fő feladata a hamis információk azonosítása, elemzése és cáfolata. Az East StratCom Task Force együttműködik a tagállamok kormányaival, kutatóintézetekkel és médiapartnerekkel dezinformáció elleni fellépés érdekében, eddig változó eredménnyel.[25]

Már több uniós tagállam is bevezetett veszélyhelyzet-kezelő és/vagy -értesítő okostelefon-alkalmazást. Németországban a lakosság számára elérhető egy ingyenes mobilapplikáció, amely széles körű funkcionalitással bír. A Német Szövetségi Polgári Védelmi és Katasztrófavédelmi Hivatal (BBK) által fejlesztett NINA (Notfall-Informations- und Nachrichten-App) nevű alkalmazás lehetőséget biztosít arra, hogy a felhasználók az aktuális tartózkodási helyük alapján figyelmeztetéseket és riasztásokat kapjanak telefonjukra hang- és fényjelzésekkel egybekötve, miközben nem tárolja a felhasználó helyadatait. A NINA célja, hogy megbízható és gyors információkat nyújtson a lakosságnak a veszélyhelyzetek kezeléséhez, és elősegítse a megfelelő felkészülést és viselkedést különböző katasztrófahelyzetekben. A felhasználóknak lehetőségük van vészhelyzeti tippeket olvasniuk, amelyek kategorizálva vannak a természeti és ipari katasztrófatípusoknak megfelelően. Az eseményleírás mellett cselekvési ajánlásokat is megfogalmaztak számukra. Továbbá az adott veszély típusának megfelelő hatóság elérhetőségét és hivatalos honlapját is feltüntették az esetek leírásánál.[26]

[22] Európai Bizottság 2024.
[23] European Commission 2022.
[24] Európai Unió [é. n.].
[25] European Union External Action 2021.
[26] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe [é. n.].

Hazánkban jelenleg okostelefonokra az Országos Katasztrófavédelmi Főigazgatóság (BM OKF) által fejlesztett ingyenes mobilalkalmazás érhető el iOS és Android operációs rendszeren, a neve VÉSZ (Veszélyhelyzeti Értesítési Szolgáltatás). Az applikáció segítségével a felhasználók képesek valós időben tájékozódni veszélyhelyzetekről, például közlekedési balesetekről, tűzesetekről vagy időjárási riasztásokról. Az alkalmazás olyan kiegészítő funkciókkal rendelkezik, mint a felolvasási lehetőség és a nagykontrasztos mód. Valamint lehetőséget biztosít a helyalapú értesítések beállítására, így a felhasználók a tartózkodási helyükhöz kapcsolódó riasztásokat is megkaphatják. A VÉSZ célja, hogy megbízható, gyors és pontos információkkal segítse a lakosságot a veszélyhelyzetek elkerülésében és kezelésében. Azonban az applikáció a lakosság felkészítését jelen formájában nem támogatja, nincsenek felkészítéssel kapcsolatos funkciói.[27]

Fejlesztési lehetőségek a hazai katasztrófavédelmi rendszerben

Javasolt lenne a hazai katasztrófavédelem rendszerében nagyobb hangsúlyt fektetni olyan lehetőségek kihasználására, amelyeket a közösségi média és a rövid videók megosztására specializálódott platformok nyújtanak. Ezek a digitális felületek hatékonyan támogathatják az aktív lakosságfelkészítést, hiszen a figyelemfelkeltő és könnyen érthető tartalmak gyorsan eljuthatnak a célközönséghez. Amennyiben az adott tartalom terjedését segítő faktorokat is megfelelően kihasználjuk (például aktuális trendeknek megfelelő tartalom, hashtagek használata, aktív kommentelési lehetőség stb.), akkor a videó még szélesebb tartalomfogyasztó körökhöz is eljuthat. A különböző közösségimédia-platformok a célzott hirdetési eszközökkel lehetővé teszik, hogy a tartalomkészítők demográfiai, földrajzi és viselkedési adatok alapján szűkítsék és optimalizálják célközönségüket. A digitális oktatás, úgymint az e-learning, hatékony eszköz lehet a lakosság felkészítésében, mert lehetőséget teremt a rugalmas, interaktív és széles körben elérhető oktatási anyagok biztosítására. Olyan ingyenesen elérhető digitális platformot javasolt kialakítani, amely bármikor alkalmazható, visszanézhető oktatási anyagokat és feladatokat tartalmaz. A digitális tananyagok segíthetnek a lakosságnak elsajátítani a vészhelyzetkor alkalmazandó óvintézkedéseket és magatartási szabályokat, például áramszünetek, kibertámadások vagy természeti katasztrófák esetén. További előnyei az online biztosított képzéseknek, hogy gyorsan frissíthetők a tananyagok, és különböző társadalmi csoportokhoz igazíthatók, továbbá hozzájárulhatnak a lakosság ellenálló képességének növeléséhez. A VÉSZ mobilapplikáció is fontos szerepet kaphat a digitális oktatás eszköztárában, ennek az alkalmazásnak a kiegészítése különböző veszélyhelyzet-kezeléshez kapcsolódó információkkal hasznos lehet olyan katasztrófahelyzetek esetén, ahol a lakosság is érintett.

Javasolt megfontolni a lakossági felkészítési programok és oktatási anyagok kiegészítését az energiaellátásban, az infokommunikációs és vízkezelő rendszerekben, valamint a rendszerelemekben jelentkező zavarok kezelésének ismereteivel. Ezek a kritikus infrastruktúrák közvetlen hatással vannak a mindennapi életre, így a lakosság alapvető

[27] BM OKF [é. n.].

tájékozottsága hozzájárulhat egy esetleges incidens hatékonyabb kezeléséhez, a bizonytalanság és a pánikhelyzet kialakulási kockázatának a csökkentéséhez. A célzott és könnyen érthető oktatási anyagok segíthetnek a lakosság tudatos felkészítésében, erősítve ezzel a közösségi ellenálló képességet és az önálló problémamegoldás lehetőségét.

A helyi szintű lakossági tájékoztató kiadványok nem biztosítanak a lakosság számára megfelelő információkat a településen lévő alapvető szolgáltatást nyújtó szervezetekről, valamint azok átmeneti vagy tartós kiesése esetén az alkalmazandó óvintézkedésekről és követendő magatartási szabályokról, annak ellenére, hogy a lakosságfelkészítés fő célja, hogy megismertesse a polgárokkal a településükre és annak közvetlen környezetére jellemző kockázatokat, valamint a veszély vagy riasztás esetén alkalmazandó magatartási szabályokat.[28] Míg a veszélyes anyagokkal foglalkozó üzemek által veszélyeztetett területen élők rendszeres és kérés nélküli tájékoztatást kapnak az adott veszélyes üzem működési sajátosságából fakadó kockázatokról és azok hatásairól, addig a kritikus szervezetek nem képezik ezen kiadványok részét. A lakosság tájékoztatása során kiemelt figyelmet kell fordítani arra, hogy ne kerüljenek nyilvánosságra olyan nem publikus információk, amelyek a kritikus szervezetek rendszereinek működésével kapcsolatban potenciális támadási felületek lehetnek. A tájékoztatás és a felkészítés célja nem a kritikus infrastruktúra működésének ismertetése, hanem a zavarok és a kiesések következményeinek bemutatása, valamint a megfelelő reagálási formák elsajátítása. A lakosság ez irányú tájékoztató kiadványai, illetve oktatási anyagok összeállításakor javasolt lehet bevonni a település szempontjából releváns kritikus szervezetek ellenálló képességért felelős vezetőit.[29]

Összegzés

A nemzetbiztonság, a lakosságvédelem és a kritikusinfrastruktúra-védelem szoros összefüggése megköveteli az integrált stratégiai megközelítést. Az utóbbi években, különösen nemzetközi színtéren is bekövetkezett változások miatt a kritikus szervezetek ellen elkövetett célzott kiber- és fizikai támadások száma jelentősen megnőtt, amelyekből három esetet mutattak be a szerzők. A CER és NIS2 irányelvek előrelépést jelentenek uniós és hazai szinten is ezen üzemek védelmében, de a lakosság rezilienciájának kérdéskörére nem terjednek ki. A lakosság felkészítése az alapvető szolgáltatást nyújtó szervezetek elleni támadásokat követő hatásokra, valamint a dezinformációs kampányokkal szemben szintén egy fontos és időszerű lépés annak érdekében, hogy a kritikus szervezeteink mellett a magyar lakosság is teljes körű ellenálló képességgel rendelkezzen. A passzív és aktív lakosságtájékoztatás és felkészítés hagyományos eszközei mellett a 21. század által kínált platformok is rendelkezésre állnak, amelyek révén az információk gyorsan és hatékonyan eljuttathatók, a felkészítésbe pedig szélesebb társadalmi rétegek is bevonhatóvá válnak.

[28] Ambrusz 2017: 33–39.
[29] Bonnyai 2013: 58–73.

Felhasznált irodalom

Ambrusz, József (2017): An Overview of Disaster Preparedness Training in Hungary, With Special Regard to Public Administration Leaders. *Ecoterra – Journal of Environmental Research and Protection,* 14(1), 33–39.

Ambrusz József – Beke Zoltán (2023): A lakossági tájékoztatás feladatai. In Szabó Csaba (főszerk.): *A katasztrófavédelem lakosságfelkészítési feladatai*. Budapest: Pytheas Könyvmanufaktúra, 603–725.

Ambrusz József – Dobor József – Vásárhelyi Örs (2024): Létfontosságú rendszerek,-rendszerelemek rezilienciájának fejlesztési lehetőségei az Európai Unió direktíváinak tükrében. *Polgári Védelmi Szemle,* 16(különszám), 57–69. Online: https://mpvsz.hu/pv_szemlek/pvszemle2024/index.html

Antal, József – Hidvégi, Timót (2021): Test Environment for Special Protocols for Industry Computer Systems. In Abonyi-Tóth, Andor – Stoffová, Veronika – Zsakó, László (szerk.): *Proceedings of XXXIV. DidMatTech 2021 Conference New Methods and Technologies in Education, Research and Practice*. Budapest: Eötvös Loránd University (ELTE) Faculty of Informatics, 106–112.

BM OKF [é. n.]: *VÉSZ*. Online: https://www.katasztrofavedelem.hu/37/vesz

Bonnyai Tünde (2013): A lakosságfelkészítés lehetséges módszertana a létfontosságú rendszerek és létesítmények védelmének rendszerében. *Hadmérnök,* 8(3), 58–73. Online: http://hadmernok.hu/133_07_bonnyait.pdf

Brucker Balázs – Jóna László – Szemerédi Eszter (2024): Magyarország energiapiacának átfogó elemzése az Európai Unió változó prioritásainak tükrében. *Tér és Társadalom,* 38(1), 155–182. Online: https://doi.org/10.17649/TET.38.1.3516

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe [é. n.]: *Warn-App NINA*. Online: https://www.bbk.bund.de/DE/Warnung-Vorsorge/Warn-App-NINA/warn-app-nina_node.html

Chiscariu, Radu Emanuel (2021): DarkSide Ransomware Behavior and Techniques. *Keysight,* 2021. május 18. Online: https://www.keysight.com/blogs/en/tech/nwvs/2021/05/18/darkside-ransomware-behavior-and-techniques

CISA (2023a): Siemens Multiple Denial of Service Vulnerabilities in Industrial Products. *Cisa.gov,* 2023. január 13. Online: https://www.cisa.gov/news-events/ics-advisories/icsa-22-349-03

CISA (2023b): Understanding Ransomware Threat Actors: LockBit. *Cisa.gov,* 2023. június 14. Online: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

Dobrády, Zoltán – Takács, Szilárd L. – Hidvégi, Timót (2023.). Use of AI in Operational Technology Networks and Packet-Based Attacks Detection. Varbanov, Petar S. – Wang, Bohong – Kapustenko, Petro: *Széchenyi István University Proceedings of Sustainable Development Research*. Győr: Universitas-Győr Nonprofit Kft., 62–68. Online: https://doi.org/10.62897/COS2023.1-1.62

Easterly, Jen (2023): The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. *Cisa.gov,* 2023. május 7. Online: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Európai Bizottság (2024): *Médiaműveltség.* Online: https://digital-strategy.ec.europa.eu/hu/policies/media-literacy

Európai Unió [é. n.]: *Éberség az interneten: fel tudja Ön ismerni az információmanipulációt?* Online: https://learning-corner.learning.europa.eu/learning-materials/how-spot-and-fight-disinformation_hu

European Commission (2022): *Strengthened Code of Practice on Disinformation*. Online: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

European Union External Action (2021): Questions and Answers about the East StratCom Task Force. *Eeas.europa.eu,* 2021. október 27. Online: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11234

Kátai-Urbán Lajos – Bleszity János – Vass Gyula (2025): A kritikus infrastruktúra védelmi felsőoktatási tapasztalatok a kritikus szervezetek ellenállóképességéről szóló szabályozás tükrében. *Polgári Védelmi Szemle,* 17(különszám), 220–236. Online: https://mpvsz.hu/pv_szemlek/pvszemle2025/index.html

Kerner, Sean Michael (2022): Colonial Pipeline Hack Explained: Everything You Need to Know. *TechTarget,* 2022. április 26. Online: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Kiss Álmos Péter (2019): A hibrid hadviselés természetrajza. *Honvédségi Szemle,* 147(4), 17–37. Online: https://honvedelem.hu/images/media/5f58be696dc30542944535.pdf

Marsi Tamás – Orosházi Dávid (2025): Új fejezet a kiberbiztonságban: a 2024. évi LXIX. törvény [aktuális]. *Kibertámadás! Podcast,* 94. epizód. Online: https://nki.gov.hu/podcast/

Microsoft Digital Defense Report 2024. Online: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

Most „Harmful" Hacker Network LockBit Disrupted by Global Police Operation. *Euronews,* 2024. február 20. Online: https://www.euronews.com/2024/02/20/most-harmful-hacker-network-lockbit-disrupted-by-global-police-operation

National Institute of Standards and Technology (2020): *Security and Privacy Controls for Information Systems and Organizations.* Online: https://doi.org/10.6028/NIST.SP.800-53r5

SektorCERT (2023): *The Attack Against Danish Critical Infrastructure.* Online: https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

Toulas, Bill (2023): Lockbit Ransomware Disrupts Emergency Care at German Hospitals. *BleepingComputer,* 2023. december 27. Online: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupts-emergency-care-at-german-hospitals/

What is Shodan? [é. n.] Online: https://help.shodan.io/the-basics/what-is-shodan

Jogi források

2024. évi LXIX. törvény Magyarország kiberbiztonságáról
2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről
418/2024 (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
474/2024. (XII. 31.) Korm. rendelet a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról
1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve 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 (NIS2 irányelv)
Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről

NEMZETBIZTONSÁGI SZEMLE
13. évfolyam (2025) 2. szám 94–107. | DOI: 10.32561/nsz.2025.2.7

Szabó Hedvig,[1] Solti István,[2]
Mezei József,[3] Drusza Tamás,[4] Dobák Imre[5]

A Z generáció munkahelyválasztási preferenciái a nemzetbiztonság területén

A nemzetbiztonsági pálya iránti érdeklődés című online, kérdőíves kutatás 1.

Job Choice Preferences of Generation Z in the field of National Security

Interest in National Security Careers Online Survey 1

A 21. század egyik legfontosabb munkaerőpiaci kihívása a nemzetbiztonsági szolgálatok esetében is a különböző generációk, különösen a Z generáció munkavállalói elvárásainak megértése. A Z generáció nemcsak munkavégzési preferenciákban, hanem életstílusban, technológiai jártasságban és munkahelyi lojalitásban is jelentős eltéréseket mutat az előző korosztályokhoz képest. A globális gazdasági és társadalmi változások, a digitalizáció, valamint a mesterséges intelligencia használata tovább erősíti ezt az átalakulást, amely különös jelentőséget kap a nemzetbiztonsági szolgálatok toborzási és állománymegtartási stratégiáiban. Az ezzel összefüggésben felmerülő kérdéseknek – vagy legalább azok egy részének – sikeres megválaszolása érdekében a Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézete egy online, kérdőíves kutatást hajtott végre az elmúlt hónapokban. A kutatás eredményeit kétrészes publikáció keretében tárjuk az érdeklődő olvasóközönség elé, amelynek első részét tartja kezében most.

Kulcsszavak: *Z generáció, pályaválasztás, preferencia, nemzetbiztonság*

[1] Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, e-mail: szabo.hedvig@uni-nke.hu
[2] Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, e-mail: solti.istvan@uni-nke.hu
[3] Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, e-mail: mezei.jozsef@uni-nke.hu
[4] Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, e-mail: drusza.tamas@uni-nke.hu
[5] Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, e-mail: dobak.imre@uni-nke.hu

One of the most important labour market challenges of the 21st century for the national security services is to understand the expectations of different generations of employees, especially Generation Z. Generation Z differ significantly from previous generations not only in their work preferences, but also in their lifestyle, technological proficiency and workplace loyalty. Global economic and societal changes, digitalisation and the use of artificial intelligence are further reinforcing this transformation, which is of particular importance in the recruitment and retention strategies of national security services. In order to successfully answer some or all of the questions that arise in this context, the Institute of National Security of the Ludovika University of Public Service has conducted an online survey in recent months. The results of this research are presented to the interested public in a two-part publication, the first part of which you are now holding in your hands.

Keywords: *generation Z, career choice, preference, national security*

Bevezetés

A Z generáció, amely az 1996 és 2007 között született fiatalokat foglalja magában, a „digitális bennszülöttek" generációjaként ismert.[6] Tagjaik egy olyan világban nőttek fel, amelyet alapvetően meghatároz az állandó online jelenlét, a közösségi média uralma, valamint az azonnali és közvetlen kommunikációs igények. Ez a korosztály olyan készségekkel és ismeretekkel rendelkezik, amelyek meghatározók a 21. századi információs társadalomban. Ugyanakkor figyelemreméltó, hogy a munkához való viszonyulásuk, értékrendjük és lojalitásuk jelentős kihívások elé állítja a munkáltatókat.[7] Emiatt indokolt külön kutatás keretében vizsgálni, hogy ez a generáció hogyan tekint az olyan szigorúan szabályozott, speciális szervezetekre, mint a nemzetbiztonsági szolgálatok, amelyek elengedhetetlenek az ország biztonsága és stabilitása szempontjából.

A téma aktualitását az adja, hogy a nemzetbiztonsági szolgálatok számára kulcsfontosságú a legtehetségesebb és legmegbízhatóbb munkavállalók toborzása és hosszú távú megtartása. A Z generáció tagjai azonban nem feltétlenül tekintenek értékként a hagyományos karrierutakra, és sokkal inkább az önmegvalósítást, a gyors visszajelzést, az innovatív munkakörnyezetet, valamint a munka és a magánélet egyensúlyát helyezik előtérbe.[8] Ezen túlmenően a globális kihívások, a kiberbiztonsági fenyegetések, a nemzetközi terrorizmus és az információs hadviselés olyan újfajta kompetenciákat és hozzáállást igényelnek, amelyekben a Z generáció erősségei – például a multitasking, a technológiai tudatosság és a gyors problémamegoldó képesség – jelentős előnyt hozhatnak. A tanulmány célja, hogy feltárja a Z generáció nemzetbiztonsági szolgálatokkal kapcsolatos karrierdöntési, továbbá szervezetben maradási motivációit és attitűdjeit. Kutatásunk arra kereste a választ, hogy milyen tényezők befolyásolják ezen generáció tagjainak elköteleződését és lojalitását egy ilyen különleges szakterületen. Emellett arra is választ kívánunk adni, hogy

[6] Prensky 2001.
[7] Balogh – Kardos – Bácsné Bába 2021.
[8] Waworuntu–Kainde–Mandagi 2022.

a nemzetbiztonsági szolgálatok hogyan alakíthatják át szervezeti kultúrájukat és toborzási stratégiáikat annak érdekében, hogy vonzók legyenek a Z generáció számára, miközben megőrzik az elvárt szakmai színvonalat és biztonsági követelményeket. Jelen vizsgálat során a főiskolai, egyetemi képzésben aktuálisan részt vevő személyeket szólítottuk meg. Ennek oka elsődlegesen az volt, hogy a magyar nemzetbiztonsági szolgálatok a kialakult gyakorlatnak megfelelően a felsőfokú végzettséggel rendelkező munkavállalókat keresik a legnagyobb számban. Ebbe az irányba mozdította el gondolkodásunkat a polgári nemzetbiztonsági szolgálatok személyi állományának jogállásáról szóló 2024. évi LXX. törvény is,[9] azonban érdemes lehet a kutatást további területekre is kiterjeszteni, ami a terveink között szerepel.

A kutatás nemcsak a nemzetbiztonsági szféra jövőbeli fejlődését segítheti elő, hanem hozzájárulhat ahhoz is, hogy szélesebb körű betekintést nyerjünk a Z generáció munkavállalói magatartásának motivációiba és azok társadalmi-gazdasági tényezőibe, ezzel támogatva a munkaerőpiaci trendek mélyebb megértését és közvetve a nemzetbiztonsági szolgálatok stratégiai célkitűzéseit.

Ezen első tanulmány keretében a kutatás módszertanát, a kutatási minta alapvető jellemzőit és a kutatás négy fő részterületéből egy-egy releváns tényező elsődleges eredményeit tárjuk az olvasó elé. A vizsgálat részletes ismertetésére a második részben kerül sor.

A kutatás módszertana

A kutatás célja a Z generációs embereket, elsősorban egyetemi hallgatókat megszólító felmérésen keresztül a nemzetbiztonsági szféra iránti érdeklődés tényezőinek, valamint a pályán maradás elemeinek feltárása volt. A kutatás során online kérdőíves módszert[10] használtunk, amelynek linkje a Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézetének (NKE NBI) honlapján szabadon hozzáférhető volt. Ezt lehetett megosztani és terjeszteni az adatgyűjtés 2024. október 15. és 2024. december 15. közötti időszakában. Az NKE viszonyainak jobb ismerete révén a felmérés lehetősége itt szélesebb körben jutott el a hallgatókhoz, aminek eredménye, hogy a válaszadók 58,3%-a az NKE hallgatója volt. A kérdőívet összesen 549 fő töltötte ki, ami alapján a mintavétel relatíve átfogónak tekinthető. Ugyanakkor hangsúlyozni kell, hogy a mintavétel nem valószínűségi módszerrel történt, hanem elérhetőségi alapon valósult meg, így a kutatás nem reprezentatív, az eredmények kizárólag a vizsgált mintára vonatkoztathatók. A kérdőív összesen 55 kérdést tartalmazott, amelyek többsége zárt végű volt, elősegítve az adatok könnyebb feldolgozását és értékelését. Nyitott kérdéseket csak akkor alkalmaztunk, amikor a válaszadóktól önálló megfogalmazást vártunk.

A kérdéseket több témakörre bontottuk, amelyek a következőket foglalták magukban:

- Anonim demográfiai adatok: A válaszadókat életkoruk (18–22 év, 23–25 év, 26–29 év), nemi hovatartozásuk (férfi, nő, nem nyilatkozom), valamint iskolai végzettségük és oktatási intézményük megjelölése alapján csoportokba soroltuk. A kérdőív

[9] 2024. évi LXX. törvény, 88. §.

[10] Anonim, személyes adatokat nem gyűjtő űrlap, amely kizárólag a kutatás időszakában volt kitölthető.

a településtípust is vizsgálta, így a válaszadók fővárosi, megyei jogú városi, városi vagy községi lakosként jelölhették meg magukat.

- Személyes és szakmai jellemzők: A válaszadók humán vagy reál beállítottságát, munkatapasztalatuk mértékét (nincs, 0–2 év, 2–5 év, 5 évnél több) is beillesztettük a szempontok közé.
- Nemzetbiztonsági pálya iránti érdeklődés: A kutatás célja volt a nemzetbiztonsági szféra ismertségének és megítélésének vizsgálata. A válaszadók véleményt nyilvánítottak arról, hogy dolgoznának-e ilyen szférában.
- Motivációs tényezők: Részletesen vizsgáltuk, hogy milyen tényezők befolyásolhatják a nemzetbiztonsági pályaválasztást. A tényezők között szerepelt a hazaszeretet, családi hagyomány, harmadik személy ajánlása, jó kereseti lehetőség, megkeresték a szolgálattól, szakmai kihívások, kiszámítható karrier, különleges feladatok, szakmai fejlődés lehetősége, nemzetbiztonsági szolgálatok társadalmi megítélése, magas szintű technológia, nemzetközi kapcsolatokban való részvétel, nyelvi érdeklődés, rugalmas időbeosztás, jó munkahelyi közösség, érdekes, nem mindennapi munkahely. Célunk volt feltárni azt is, hogy mely tényezők befolyásolták azokat a résztvevőket, akik nem választanák munkahelynek a nemzetbiztonsági szolgálatokat. A felajánlott választási lehetőségek: kevés az információm a nemzetbiztonsági munkáról ahhoz, hogy dönteni tudjak/akarjak, nem érdekel ez a munka/munkakör, szigorúbb magánéleti kötöttségek, munkahely és magánélet egyensúlya, stresszes munkakör, titoktartási kötelezettség, szakmai fejlődés, nemzetbiztonsági szolgálatok társadalmi megítélése, államigazgatási ágazat, fizetés/pénzügyi juttatások.
- A pályán maradás preferenciái: A kutatás fel kívánta tárni, hogy a válaszadók milyen elvárásokat támasztanak, amelyek hatására megfontolják a munkahely melletti hosszú távú elköteleződést. Ennek keretében számos tényezőt vizsgáltunk (lásd a kutatás során használt kérdőívet tartalmazó 1. táblázatot).

1. táblázat: A kutatás során használt – a szerzők által összeállított – kérdőív

Sorszám	Kérdés
1.	Válassza ki, melyik korcsoporthoz tartozik!
2.	Melyik nemhez tartozik?
3.	Milyen iskolai végzettséggel rendelkezik?
4.	Melyik egyetemen tanul vagy tanult?
5.	Milyen településen él?
6.	Humán vagy reál beállítottságú, vagy mind a kettő?
7.	Van már munkatapasztalata?
8.	Milyen forrásból tájékozódik a munkahely választásánál?
9.	Egyéb
10.	Rendelkezik-e ismerettel a nemzetbiztonsági szféráról?
11.	Mi a véleménye a titkosszolgálatok tevékenységéről?
12.	Dolgozna-e nemzetbiztonsági szolgálatnál?
13.	Folytatni kívánja a kitöltést?

Nemzetbiztonsági irányultságú pályaválasztásnál a jelzett alábbi tényezők mennyire befolyásolnák a választását?	
14.	Hazaszeretet
15.	Családi hagyomány
16.	Mások ajánlása
17.	Jó kereseti lehetőség
18.	Megkeresnének a szolgálattól
19.	Szakmai kihívások
20.	Kiszámítható karrier
21.	Nemzetbiztonsági szolgálatok társadalmi megítélése
22.	Magas szintű technológia
23.	Nemzetközi kapcsolatokban való részvétel, nyelvi érdeklődés
24.	Rugalmas időbeosztás
25.	Jó munkahelyi közösség
26.	Érdekes, nem mindennapi munkahely
27.	Egyéb
Miért nem (vagy inkább nem) dolgozna nemzetbiztonsági szolgálatnál?	
28.	Kevés az információm a nemzetbiztonsági munkáról ahhoz, hogy dönteni tudjak/akarjak
29.	Nem érdekel ez a munka/munkakör
30.	Szigorúbb magánéleti kötöttségek
31.	Munkahely és magánélet egyensúlya
32.	Stresszes munkakör
33.	Titoktartási kötelezettség
34.	Szakmai fejlődés
35.	Nemzetbiztonsági szolgálatok társadalmi megítélése
36.	Államigazgatási ágazat
37.	Fizetés/pénzügyi juttatások
38.	Egyéb
Ha elhelyezkedne nemzetbiztonsági szolgálatnál, mely tényezők alapján maradna hosszú távon is a szolgálatnál (mely tényezőket mennyire tartja fontosnak)?	
39.	Versenyképes fizetés
40.	Egyéb juttatások
41.	Munka-magánélet egyensúlya
42.	Etikai, morális elvek érvényesülése
43.	Szervezet társadalmi elismertsége
44.	Modern, inspiráló munkahely
45.	Jó munkahelyi hangulat
46.	Szakmai fejlődés lehetősége, munkakörök változatossága, új kihívások megléte
47.	Képzések, továbbképzések, mentorálás, coaching megléte
48.	Rugalmas munkaidő, rugalmas időbeosztás
49.	Lehetőség a munkahelyi előrelépésre
50.	Munkavégzés alternatív formáinak lehetősége (home office, távmunka)
51.	Társadalmi felelősségvállalás, közösségi szerepvállalás, környezettudatos működés megléte
52.	Technológiai innovációra való nyitottság, modern technológia és digitális eszközök használata
53.	Szakmai kapcsolatépítés, konferenciákon való részvétel lehetősége
54.	Egyéb
Ha nemzetbiztonsági szervezetnél dolgozna, az előmenetel során inkább a rövid időnkénti, de kisebb szintű előrelépési rendszert preferálná, vagy a hosszabb időközönkénti jelentősebb előlépési rendszert?	

Forrás: a szerzők szerkesztése

Az adatokat a JMP Pro 18 statisztikai program segítségével elemeztük. Az elemzés során alapvető leíró statisztikákat készítettünk, amelyek segítségével áttekintettük a válaszadók jellemzőit és az egyes kérdésekre adott válaszok gyakorisági eloszlását, valamint meghatároztuk az átlagokat és a mediánokat. Ezek az adatok biztosították a kutatás kiindulópontját, és lehetőséget adtak az adatok egyszerű, áttekinthető bemutatására. Ezt követően kereszttáblás elemzéseket végeztünk, hogy megvizsgáljuk, milyen kapcsolat mutatható ki a demográfiai jellemzők – például nem, életkor és iskolai végzettség – és a nemzetbiztonsági pálya iránti érdeklődés között. Ez a módszer lehetővé tette, hogy azonosítsuk az egyes demográfiai csoportok közötti eltéréseket, valamint az érdeklődést befolyásoló mintázatokat.

További elemzésként korrelációs vizsgálatot alkalmaztunk annak érdekében, hogy feltárjuk a motivációs tényezők és a nemzetbiztonsági pályaválasztási szándék közötti kapcsolat erősségét. Ez a megközelítés segít azonosítani, hogy mely tényezők játszanak meghatározó szerepet a válaszadók döntéseiben. Az elemzés utolsó szakaszában faktorelemzést alkalmaztunk, amely lehetővé teszi a motivációs tényezők csoportosítását és a főbb befolyásoló faktorok azonosítását. Ezzel a módszerrel az egyes tényezők közötti rejtett összefüggések is feltárhatók, ami hozzájárul a nemzetbiztonsági pályaválasztási preferenciák mögötti komplexebb struktúra megértéséhez. Az elemzési módszerek kombinációja pedig átfogó képet nyújt az adatokban rejlő összefüggésekről és a kutatási kérdések megválaszolásáról.

A kutatási minta alapjellemzői

A válaszadók túlnyomó többsége (77,6%) a 18–22 éves korcsoportba tartozott. A 23–25 éves korosztály aránya 16,2%, míg a 26–29 éveseké 6,2%. A nemek közötti megoszlás kiegyensúlyozott, a nők aránya 50,1%, míg a férfiaké 49,4%, ami megfelelő reprezentációt biztosít a nemek közötti különbségek vizsgálatához.[11] A válaszadók 82,5%-a középfokú végzettséggel rendelkezik. A felsőfokú végzettséggel rendelkezők aránya jelentősen kisebb (BSc: 15,7%, MSc: 1,5%). A válaszadók legnagyobb része városban él (31,5%), míg a megyei jogú városok és a főváros aránya egyaránt közel 24%. A községekben élők aránya 20,4%, ami jelzi, hogy a kutatás földrajzilag is széles körű reprezentációt biztosított. A résztvevők több mint fele (58,3%) humán beállítottságú, míg a reál beállítottságúak aránya mindössze 12,8%. A mindkét terület iránt érdeklődők aránya pedig közel 29%.

A válaszadók több mint fele (58,3%) az NKE hallgatója, ami a mintavétel helyének dominanciáját mutatja. A többi egyetemhez való kapcsolódás jelentősen alacsonyabb, csak a Széchenyi István Egyetem (12%) és a Pécsi Tudományegyetem (9,5%) emelkedik ki. Ezen terület részletes adatait a 2. táblázat tartalmazza.

[11] 0,5%-uk nem válaszolt a kérdésre.

2. táblázat: A kérdőívet kitöltők egyetemek szerinti megoszlása

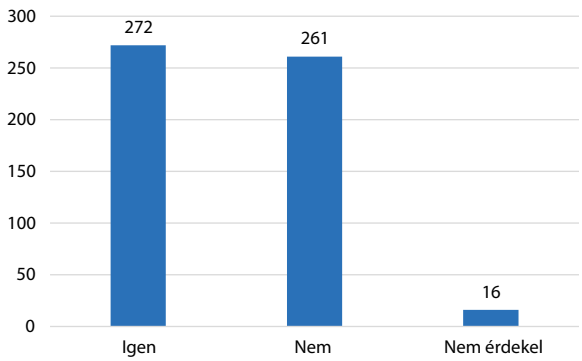
Egyetem	Fő	Arány (%)
Budapesti Corvinus Egyetem	4	0,7
Budapesti Műszaki és Gazdaságtudományi Egyetem	12	2,2
Debreceni Egyetem	18	3,3
Eötvös Loránd Tudományegyetem	17	3,1
Károli Gáspár Református Egyetem	4	0,7
Nemzeti Közszolgálati Egyetem	320	58,3
Óbudai Egyetem	6	1,1
Pázmány Péter Katolikus Egyetem	5	0,9
Pécsi Tudományegyetem	52	9,5
Széchenyi István Egyetem	66	12,0
Szegedi Tudományegyetem	35	6,4
Egyéb	4	0,7
Nem tanultam/tanulok felsőoktatásban	4	0,7
Nem kívánok nyilatkozni	2	0,4

Forrás: a szerzők szerkesztése

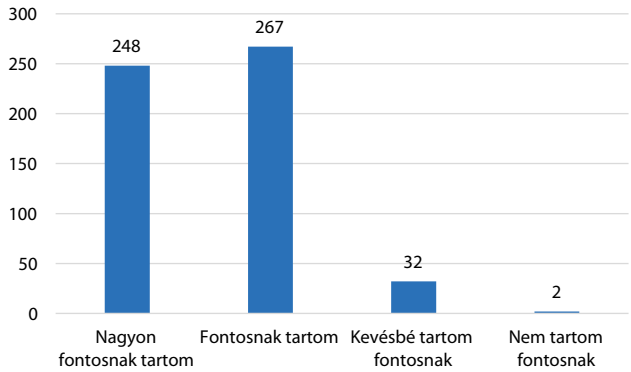
A kutatás elsődleges eredményei

a) Rendelkezik-e ismerettel a nemzetbiztonsági szféráról? Mi a véleménye a titkosszolgálatok tevékenységéről?

A kérdőíves vizsgálat eredményéből láthatóvá vált, hogy a válaszadók felének volt ismerete a nemzetbiztonsági szféráról, és közel ugyanilyen arányban nyilatkozták, hogy nem ismerik az ágazatot, míg a teljesen elutasítók aránya minimálisnak (3%) tekinthető (1. ábra). Az elsődleges ismeretek ellenére az 549 válaszadó 94%-a tartotta fontosnak, illetve nagyon fontosnak a titkosszolgálatok tevékenységét (2. ábra).



1. ábra: A Rendelkezik-e ismerettel a nemzetbiztonsági szféráról? kérdésre adott válaszok száma (fő), megoszlása (549 kitöltő)
Forrás: a szerzők szerkesztése



2. ábra: A Mi a véleménye a titkosszolgálatok tevékenységéről? kérdésre adott válaszok száma (fő), megoszlása (549 kitöltő)
Forrás: a szerzők szerkesztése

b) Dolgozna-e nemzetbiztonsági szolgálatnál?

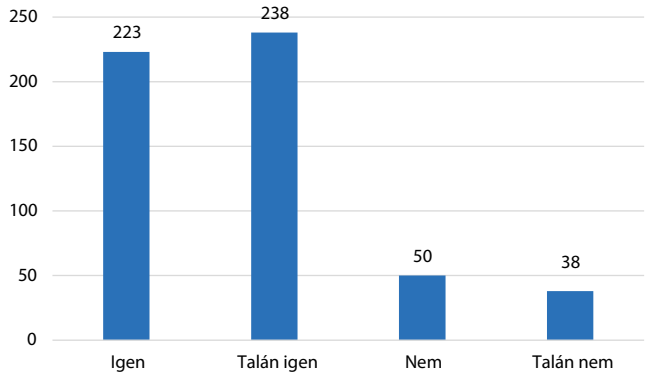
A kutatás egyik fontos célja volt annak megállapítása, hogy a Z generációhoz tartozó személyek milyen arányban dolgoznának valamely magyar nemzetbiztonsági szolgálatnál. Az ezen irányultság megismerése érdekében egy egyválaszos, zárt kérdést tettünk fel: *Dolgozna-e nemzetbiztonsági szolgálatnál?* A válaszadók a lehetséges válaszokon keresztül jelölhették ez irányú szándékuk erősségét (igen; nem; talán igen; talán nem). Ezt mutatja be a 3. táblázat.

3. táblázat: A Dolgozna-e nemzetbiztonsági szolgálatnál? kérdésre adott válaszok nemenkénti bontásban

	Melyik nemhez tartozik?			
Dolgozna-e nemzetbiztonsági szolgálatnál?	*Férfi*	*Nem nyilatkozom*	*Nő*	*Összesen*
Igen	120	1	102	223 fő
				40,62%
Nem	24	1	25	50 fő
				9,11%
Talán igen	109	1	128	238 fő
				43,35%
Talán nem	18	0	20	38 fő
				6,92%
Összesen:	271 fő	3 fő	275 fő	549 fő
	49,36%	0,55%	50,09%	

Forrás: a szerzők szerkesztése

A kérdésre a felmérésben részt vevő összes személy, mind az 549 fő válaszolt. Közülük 223 választotta az „igen” opciót, ami az összes válaszadó 40,62%-a. Ebből 120 férfi, 102 nő, míg 1 fő nem nyilatkozott a nemi identitásáról. A vizsgálatban részt vevő összes férfi



3. ábra: A Dolgozna-e nemzetbiztonsági szolgálatnál? kérdésre adott válaszok száma (fő), megoszlása (549 kitöltő)

Forrás: a szerzők szerkesztése

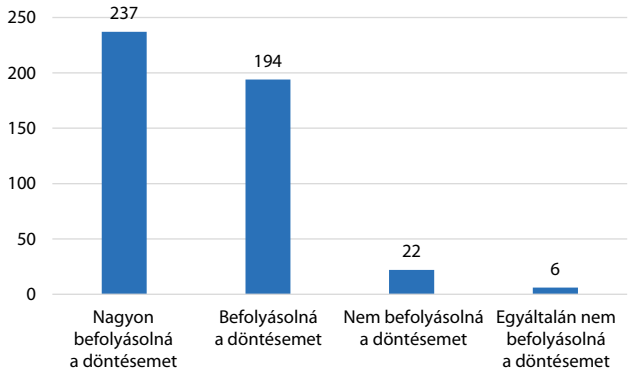
(271 fő) esetében az arány 44,28%, míg az összes nő (275 fő) esetében 37,09%. A válaszadók 43,35%-a, 238 fő a „talán igen" lehetőséget jelölte meg. Ebből 109 férfi, 128 nő, 1 fő pedig nem nyilatkozott a nemi identitásáról. A vizsgálatban részt vevő összes férfi esetében ezen válasz esetén az arány 40,22%, míg a nők esetében 46,55%. A válaszok eloszlását a 3. ábra szemlélteti.

A kérdőívet kitöltő 549 főből 461 fő, vagyis 83,97% jelölte meg azt, hogy dolgozna („igen", illetve „talán igen" válaszok) nemzetbiztonsági szolgálatnál, ami jelentős aránynak tekinthető. Ebből a nők aránya 41,9%, míg a férfiaké 41,71%. A „nem" válaszokra rátérve az 549 főből mindössze 50 fő, tehát 9,11% gondolta úgy, hogy biztosan nem dolgozna nemzetbiztonsági szolgálatnál. Amennyiben ehhez hozzáadjuk a „talán nem" válaszok számát is, ami 38 volt, akkor is az összes válaszadónak a 16,03%-a jelölte azt, hogy nem dolgozna nemzetbiztonsági szolgálatnál. A férfi és női megoszlásban nincs szignifikáns eltérés, a férfiaknak 15,5%-a, a nők 16,3%-a elutasító az ágazat irányában. Összességében kijelenthető, hogy a Z generáció alapvetően nyitott arra, hogy valamely nemzetbiztonsági szolgálatnál helyezkedjen el.

A vizsgálatban minél pontosabb választ szerettünk volna kapni arra is, hogy melyek azok a tényezők, amelyek pozitívan hatnak a vizsgált generáció tagjaira abban a tekintetben, hogy nemzetbiztonsági szolgálatnál helyezkedjenek el, és ezen tényezők mennyire befolyásolják ez irányú döntésüket.

c) Nemzetbiztonsági irányultságú pályaválasztásnál a jelzett alábbi tényezők mennyire befolyásolnák választását: jó munkahelyi közösség, nemzetbiztonsági szolgálatok társadalmi megítélése?

Az egyes kérdésekre adott válaszok száma 458 és 460 között volt. Az adatok alapján a vizsgált tényezők közül a *jó munkahelyi közösség* az, amelyről a legtöbben, a válaszadók 93,9%-a jelölte azt, hogy befolyásolja a döntését abban, hogy nemzetbiztonsági szolgálatnál helyezkedjen el, tehát ez a Z generáció tagjai számára az egyik legfontosabb tényező



4. ábra: A Befolyásolná-e a pályaválasztását a jó munkahelyi közösség? kérdésre adott válaszok száma (fő), megoszlása (459 kitöltő)
Forrás: a szerzők szerkesztése

a pályaválasztás során. Az ezen kérdés kapcsán megadott válaszlehetőségeket és az azokra adott válaszok számát a 4. ábra mutatja.

Ezen kérdéssorban a válaszok alapján a lista végén a *nemzetbiztonsági szolgálatok társadalmi megítélése* áll 34,34%-kal. A nemzetbiztonsági szolgálatok a társadalom egésze biztonságának fenntartásáért dolgoznak. Ennek tükrében figyelmet érdemel, hogy a válaszoló 459 főből mindössze 158 személy nyilatkozott úgy, hogy befolyásolná vagy nagyon befolyásolná a döntését a nemzetbiztonsági szolgálatok társadalmi megítélése.

d) Ha elhelyezkedne nemzetbiztonsági szolgálatnál, mely tényezők alapján maradna hosszú távon is ott (mely tényezőket mennyire tartja fontosnak): szervezet társadalmi elismertsége, lehetőség a munkahelyi előrelépésre? Ha nemzetbiztonsági szervezetnél dolgozna, az előmenetel során inkább a rövid időnkénti, de kisebb szintű előrelépési rendszert preferálná, vagy a hosszabb időközönkénti jelentősebb előlépési rendszert?

A kutatás célja volt annak felmérése is, hogy a Z generáció tagjai számára mely tényezők azok, amelyeket számításba vesznek hosszabb idejű munkavállalás esetén, vagyis melyek azok a területek, amelyek akár már az elhelyezkedést is segíthetik. Ezen generációs igények felméréséhez 15 különböző tényezőre vonatkozó kérdést tettünk fel.

A nemzetbiztonsági szolgálatok eredményes működése szempontjából fontos, hogy a társadalom tagjai elismerjék, támogassák tevékenységüket. Az ezen részterületen vizsgált tényezőkre adott válaszok alapján általánosan kijelenthetjük, hogy a társadalmi elismertségnek fontos szerepe van a generáció megtartásában és hosszú idejű foglalkoztatásában is, hiszen mind azok körében, akik szívesen dolgoznának a nemzetbiztonsági ágazatban, mind pedig azok körében, akiknél elképzelhető, hogy itt vállaljanak munkát, többségben vannak azok, akik nagyon fontosnak gondolják, hogy olyan szolgálatoknál dolgozzanak, amelyekről a társadalomban pozitív kép alakult ki. Ha ehhez még hozzávesszük azokat is, akik alacsonyabb szinten, de ugyanúgy szempontként tekintenek a társadalmi elismertségre, akkor már mindkét vizsgált körben jelentős többségben vannak, akiknél ez a szempont megjelenik.

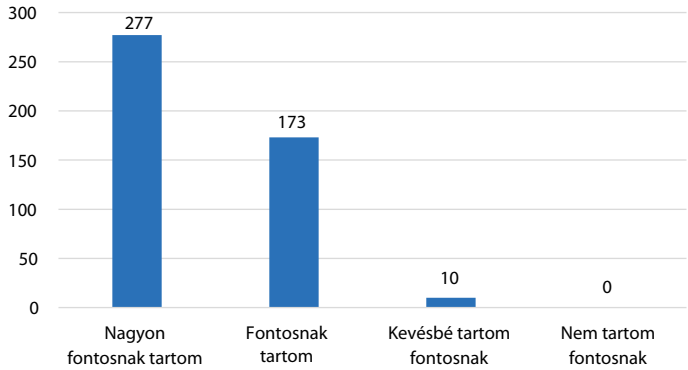
A válaszadói halmazt, 459 főt vizsgálva azok közel 57,5%-a, vagyis 264 fő számára van jelentősége ennek, amely arány akkor sem változik számottevően (60,5%), ha csak a nem NKE-s azon hallgatók 100 fős csoportját nézzük, akik elhelyezkednének nemzetbiztonsági szolgálatnál. Azt is kijelenthetjük, hogy viszonylag alacsony azok száma – mindössze 33 fő, a válaszadók 7,19%-a –, akiknél egyáltalán nem számít a szolgálatok társadalmi megítélése.

A férfi-női eloszlás vizsgálata esetén azt látjuk, hogy a nők sokkal érzékenyebbek ezen szempont iránt, hiszen a válaszadó férfiak közel 12%-a (27 fő), míg a nőknek csupán 2,6%-a (6 fő) nyilatkozott úgy, hogy egyáltalán nem tartja fontosnak a szervezet társadalmi elismertségének szempontját. A fenti majd kétharmados arányból azt a következtetést vonhatjuk le, hogy a Z generáció tagjainak hosszú vagy hosszabb távú elköteleződésére csak olyan nemzetbiztonsági szféra számíthat, amelynek léte és tevékenysége a társadalom számára elfogadott, és nem övezi őket széles körű elutasítottság. Vagyis a fiatalok számára fontos, hogy olyan helyen dolgozzanak, amely a köz részéről is megbecsülésnek örvend, és amely miatt a későbbi életszakaszaikban nem kell számítaniuk hátrányos megkülönböztetésre sem a munkaerőpiacon, sem pedig a magánéletükben. Ugyanakkor érdemes rámutatni, hogy a társadalmi elfogadottság abszolút értékben fontos, viszont relatíve mégis a legkevésbé fontos tényező azok közül, amelyeket a kérdőívben megfogalmaztunk. A további 14 szempont közül ugyanis egyrészt a második legkevésbé fontos szempont az előző kérdéssel kapcsolatban lévő, a *társadalmi, közösségi szerepvállalás, környezettudatos működés,* amely 323 főnek, a válaszadók 70,68%-ának volt fontos, másrészt az összes többi tényező 80% és 90% feletti támogatottságot ért el. Vagyis a fiatalok kilátásait, kezdve a munka és a magánélet megfelelő egyensúlyától egészen a szakmai kapcsolatépítés lehetőségeinek meglétéig, lényegesen jelentősebben befolyásolják, mint az előzőkben bemutatott elismertségi tényező. Ennek következtében azonban a fenti kijelentést is árnyalnunk szükséges, hiszen amellett, hogy már önmagában is szerepet játszik a Z generáció hosszú távú elképzeléseiben, számos olyan szempont van, amit nem szabad a szolgálatoknak figyelmen kívül hagyniuk.

Az adatfelvételt megelőző ismereteink szerint a hosszú távú foglalkoztatás szempontrendszere között fontos szerepet játszik a munkahelyi előrelépés lehetősége. Ennek további tanulmányozásához, amellett, hogy megvizsgáltuk a fiatalok számára a munkahelyi előmenetel szükségességének mértékét, arra is kíváncsiak voltunk, hogy milyen típusú előmenetelt részesítenek előnyben. Ennek során azt állapítottuk meg, hogy a Z generáció körében a legfontosabb szempont a munkahely megtartásában egy stabil és tervezhető előmeneteli rendszer biztosítása. Ugyanis a válaszadók közel kétharmada (277 fő) nagyon fontosnak, több mint egyharmada (173 fő) pedig fontosnak jelölte az előrelépés lehetőségét, mindösszesen 10 fő volt, aki kevésbé fontosnak tartja e szempontot pályája során. A jelentőséget abból is érzékelhetjük, hogy senki nem választotta a „nem tartom fontosnak" lehetőséget (5. ábra).

Ráadásul azt is kimutattuk, hogy nincs jelentős eltérés a nemek között a hangsúlyokat tekintve sem, hiszen néhány százalék eltéréssel mondják azt a nők és a férfiak, hogy nagyon fontos számukra az előrejutás pályafutásuk során.

Ha településszerkezet szerint vizsgáljuk a populációt, akkor két véglet jelenik meg. A fővárosiak kivétel nélkül úgy nyilatkoztak, hogy fontos vagy nagyon fontos az előrejutás, és csak a községekből jövők esetében vannak többen (ez is csak 6 fő, ami a községből érkezők 6,3%-a), akik kevésbé tartják fontosnak e tényezőt. Viszont még az ő esetükben is több mint 53% azok aránya, akik nagyon fontosnak tartják az előmenetelt, a városiak esetében ez az érték



5. ábra: A lehetőség a munkahelyi előrelépésre kérdésre adott válaszok száma (fő), megoszlása (460 kitöltő)
Forrás: a szerzők szerkesztése

pedig 60% körül van. Érdekes módon a legalacsonyabb értéket a fővárosiak esetében (60%) mértük, amit alig előz meg a városból érkezők eredménye (61%), viszont annál inkább a megyei jogú városból jövők aránya (65%). Szintén jellemző adat, hogy a reál beállítottságúak, vagy a 90-es évek végén születettek, vagy a mesterdiplomával rendelkezők, vagy az 5 évnél több munkatapasztalattal rendelkezők, a budapesti vezető egyetemeken végzettek közül senki nem nyilatkozott úgy, hogy kevésbé tartja fontosnak az előrejutást. Ráadásul ezen fiatalok 71%-a még csak nem is fontos, hanem nagyon fontos szempontnak jelölte meg.

A Z generáció tagjai abban már megosztottak, hogy a munkahelyi előrelépés mely formáját részesítik előnyben. A felmérés utolsó kérdése arra vonatkozott, hogy egyébként a fiatalok a munkahelyi előmenetel mely formáját tekintik ideálisnak, mennyi idő elteltével várják el a szervezettől a karrier következő lépcsőjét. A kérdésre adott válaszok (459 válasz) alapján általánosságban azt mondhatjuk, hogy a fiatalok többsége (263 fő, 57,3%) elvárja, hogy gyakran léptessék elő, viszont ebben az esetben megelégszik kisebb lépésekkel, míg szintén nagy részük (197 fő, 42,8%) elfogadja a hosszabb idejű, de a munkakörben érzékelhető változást hozó előléptetést. Ha mindezt a nemek szerint vizsgáljuk, a nők esetében közel fele-fele az arány, ellenben a férfiak több mint 60%-a inkább a folyamatos előrejutást preferálja. A mért adatok esetében a mesterdiplomával és az alapdiplomával rendelkezők között látható szignifikáns eltérés, hiszen míg az MSc-fokon végzettek (6 fő) esetében pont 50% mindkét lehetőség értéke, addig a BSc-diplomával rendelkezők (77 fő) majd kétharmada a rövid, de gyors előrejutást preferálja.

Megítélésünk szerint a munkahelyi előmeneteli rendszerrel szemben támasztott generációs követelmények azt jelentik, hogy a következő belépő generáció megtartása érdekében a nemzetbiztonsági szolgálatoknak is érdemes kialakítaniuk egy érzékelhető és valid karriert biztosító rendszert, mivel ennek hiányában a Z generáció tagjai viszonylag rövid idő után új munkahelyet fognak keresni az előrelépés érdekében. Ezek alapján azt is mondhatjuk, hogy önmagában a nemzetbiztonsági szolgálatoknál való munka lehetősége nem jelent elegendő vonzóerőt a fiatalok számára. Az erre a tényezőre való odafigyelés fontosságát alátámasztja az is, hogy a nemzetbiztonsági szolgálatok olyan, magasan kvalifikált és nyelvvizsgával rendelkező fiatalokat invitálnak a szervezetbe, akik a munkaerőpiacon is versenyképes végzettséggel és diplomával rendelkeznek.

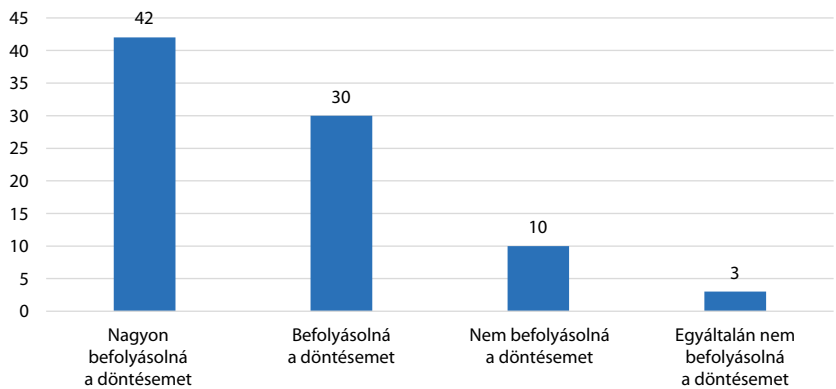
e) Miért nem (vagy inkább nem) dolgozna nemzetbiztonsági szolgálatnál? – Szigorúbb magánéleti kötöttségek.

A vizsgálatban részt vevők közül 85 fő válaszolta azt, hogy nem érdekli a nemzetbiztonsági pálya. Az ezzel összefüggésben vizsgált tényezők közül a szigorúbb magánéleti kötöttségek 84,7%-os elutasítási aránnyal a legfontosabb visszatartó tényezőként jelent meg. Ez jelzi, hogy a személyes szabadság és a magánélet fontosabb sok válaszadó számára, mint a nemzetbiztonsági karrier lehetősége. Az ezen tényezőre adott válaszokat a 6. ábra mutatja.

Hasonlóan magas arányban jelezték elutasításuk indokaként a megkérdezettek a *munkahely és magánélet egyensúlya* tényezőt (83,53%). Kevésbé befolyásoló tényezőként jelentek meg az olyan szempontok, mint a *nemzetbiztonsági szolgálatok társadalmi megítélése* (33,33%) és az *államigazgatási ágazat jellege* (48,23%).

A nemzetbiztonsági szolgálatok feladatellátása kapcsán az egyik kiemelten fontos tényező, hogy titkosszolgálati eszközöket alkalmazhatnak, amivel összefüggésben azt követően alapvetően egész életükben titoktartási kötelezettség terheli őket. Ennek függvényében figyelmet érdemel, hogy a nemzetbiztonsági pályát elutasítók közül mindössze 52,94%-ot nem vagy egyáltalán nem befolyásolna a titoktartási kötelezettség, ami arra utal, hogy a titoktartás kevésbé jelent akadályt a legtöbb potenciális jelentkező számára.

Amennyiben a válaszokat például nemek szerinti bontásban vizsgáljuk, akkor a férfiak inkább a szakmai és szervezeti tényezőket (például az államigazgatási jelleget és a titoktartást) jelölték meg elutasítási okként, míg a nőknél a magánélet és a munka egyensúlya, valamint a munkakör stressz-szintje váltott ki nagyobb ellenérzést. A munkahely és magánélet egyensúlyának hiánya a nők 65%-ánál, míg a férfiak 35%-ánál volt erősen elutasító tényező. A szigorúbb magánéleti kötöttségeket a nők 62%-a, a férfiak 38%-a ítélte nagyon befolyásolónak, míg a stresszes munkakörrel kapcsolatos elutasítás is magasabb volt a nőknél (58%) a férfiakhoz képest (42%).



6. ábra: Miért nem (vagy inkább nem) dolgozna nemzetbiztonsági szolgálatnál? – „Szigorúbb magánéleti kötöttségek" kérdésre adott válaszok száma (fő), megoszlása (85 kitöltő)
Forrás: a szerzők szerkesztése

Befejezés

A vizsgálat hiánypótló, sőt mondhatjuk azt is, hogy unikális, hiszen Magyarországon ilyen kutatásra ez idáig a nemzetbiztonság területén nem került sor. A munkaerőpiacon jelen lévő generációk közötti különbségek, az új generációk integrálása és megtartása a hivatásos szolgálati viszony alapján működő szervezetekben napjainkban komoly kihívást jelent. Az ezen kutatás keretében megszületett válaszok feldolgozásának eredményei azonban hatalmas segítséget adhatnak a magyar nemzetbiztonsági szolgálatok vezetése és humán szakterületei számára stratégiai döntéseik meghozatalához.

Felhasznált irodalom

2024. évi LXX. törvény a polgári nemzetbiztonsági szolgálatok személyi állományának jogállásáról

Balogh Renátó – Kardos Magdolna Valentina – Bácsné Bába Éva (2021): Az Y és Z generáció munkahelyválasztásának szempontjai. *Jelenkori Társadalmi és Gazdasági Folyamatok,* 16(1–2), 59–67. Online: https://doi.org/10.14232/jtgf.2021.1-2.59-67

Prensky, Marc (2001): *Digital Game-Based Learning.* New York: McGraw-Hill.

Waworuntu, Evi C. – Kainde, Sandra J. R. – Mandagi, Deske W. (2022): Work-Life Balance, Job Satisfaction and Performance Among Millennial and Gen Z Employees: A Systematic Review. *Society,* 10(2), 384–398. Online: https://doi.org/10.33019/society.v10i2.464

Tartalom