NEMZETBIZTONSÁGI SZEMLE

Kiemelt közlemények

Horváth Ferenc: ***Új oktatási módszerek alkalmazásának tapasztalatai a Nemzetbiztonsági Szakszolgálatnál***

Mustafa Burak Şener:
The Collapse of the Ottoman Empire: An Evaluation on the Impact of Milestones in Europe

12. évf. (2024)
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: Deli Gergely rektor
Olvasószerkesztők: Bujdosó Hajnalka, Nagy Judit, Resofszki Ágnes
Tördelőszerkesztő: Kőrösi László

Tartalom

NEMZETBIZTONSÁGI SZEMLE
12. évfolyam (2024) 2. szám 3–17. | DOI: 10.32561/nsz.2024.2.1

Mustafa Burak Şener[1]

The Collapse of the Ottoman Empire: An Evaluation on the Impact of Milestones in Europe

One of the largest empires in world history, the Ottoman Empire had its golden age in the 16th century. However, in this period, when the Ottoman Empire was the strongest and unbeatable, some problems began to occur. The empire, which could not keep up with the developments and innovations in the world required by the period, collapsed over the centuries due to its weak internal structure. In the meantime, Europeans found new trade routes and colonised many places with geographical discoveries, advanced in science, art, and technology with the Age of Enlightenment, mechanised with the Industrial Revolution, and democratised with the French Revolution. While all those developments took place in Europe, the Ottoman Empire could not provide the necessary modernisation. In this direction, with its weakened internal structure in the military, economic, political, administrative, and educational fields, it could not prevent that process. Thus, it gradually became a state that fall behind in every area from Europe over the centuries and eventually collapsed. Accordingly, this study has comprehensively analysed the Ottoman disintegration process, which had started in the 16th century, by considering the significant historical developments in Europe and the gradually weakening Ottoman internal structure.

Keywords: *Ottoman Empire, collapse, disintegration, downturn period, decline paradigm*

Introduction

The Ottoman Empire was one of the largest empires of the period and history, which ruled on three continents and continued its existence for 623 years from the Middle Ages to the Modern Ages.[2] The Ottoman Empire, which became the most powerful empire in the world in the 16th century, expanded its territory to Eastern Europe, Southwest

1 PhD student, Eötvös Lóránd University, Doctoral School of History, e-mail: buraksener1626@gmail.com
2 Sultana–Sharif 2019: 37–38.

Asia and North Africa in this period and eventually reached its widest borders in 1683.[3] Nevertheless, such a great empire has fallen apart and collapsed, as has happened to all empires in history. Therefore, it is essential to analyse the collapse of this great empire to understand the importance of not being able to withstand time like other empires in history, and the position of states in the future international system.

However, the main reason for the disintegration of this empire is not an event that happened suddenly or occurred within a certain period of time. The period that begins with the Treaty of Yas, which the Turkish education curriculum calls the period of collapse of the Ottoman Empire, and ends with the Treaty of Sèvres, describes the period of collapse of the Ottoman Empire chronologically, not the reasons for the collapse of the Ottoman Empire.[4] In the literature, it is seen that the collapse of the Ottoman Empire is discussed more frequently, but there is a quantitative deficiency in the studies that comprehensively discuss the reasons behind the collapse of the Ottoman Empire.[5] Although these studies are very valuable and have made great contributions to the literature, it is necessary to increase the number of studies that deal with the causes.

Therefore, this study will analyse the reasons behind the collapse of the empire instead of analysing the last periods of it. For this reason, it would be appropriate to examine the collapse of the Ottoman Empire from the 16th century, when the basis of systemic deterioration began, and external factors began to take effect. Instead of examining periodic events, the article will focus on the results and analyse how these situations affected the collapse of the Ottoman Empire. In this direction, the article will deal with the reasons behind the collapse, together with critical historical developments, depending on internal and external factors.

External factors

The factor that makes an empire strong is that it is ahead of its time. Yet this should be considered as a sum of all factors, not just a single factor. Empires that are not ahead of their time become open to external factors because they do not have a feature that distinguishes them from other powers.

The main external factor that caused the collapse of the Ottoman Empire was the inability to follow the developments in Europe. The Ottoman Empire, which dominated a considerable area in Europe, was constantly competing with Europe since it was never seen as a European civilization. On the other hand, Europeans entered many bloody wars among themselves, and even though they caused the First and Second World Wars, they were permanently affected by the developments in each other and integrated themselves in this direction. At the beginning of the 17th century, Maximilien de Béthune, Duc De Sully's[6] "Christian European Council" and the "Great Design" idea, which formed the foundations of the European Union, aimed to exclude and to establish a military unit

3 Hürriyet 2019.
4 See: www.ktb.gov.tr/TR-96255/turk-kulturu.html
5 See also Reid 2000; Hanioğlu 2010; İnalcık–Quataert 1994.
6 He was an advisor to King Henry IV of France as Chief Minister in 1589 and 1611.

against the Ottoman Empire.[7] Thus, while the European Union was formed as a result of centuries of integration, Turkey, the successor of the Ottoman Empire, has been left out of the union for many years.[8]

While the Ottoman Empire was living its new age and creating its own classical period from 1299 to 1579, Europe was living in the darkness of its own medieval period. However, from the 16th century onwards, the historical process began to work in reverse. As a result of this, while Europe was entering its new age with its new dynamic actors formed by individual-mind-science and even nation-centred scientists, philosophers, and merchants by creating a new alternative from its own Medieval Age, the Ottomans continued on their way with their old system, as they could not create new alternatives and new actors from their own system, and in a way prepared their own Middle Ages and got into it.[9]

Geographical discoveries

All of the factors in Europe's overtaking of the Ottoman Empire, which will be examined under the subtitle of external factors, are interrelated. However, geographical discoveries form the basis of all these factors.

The time interval of the period, which is called the period or epoch of geographical discoveries in world history, is accepted from 1400 to 1600. This period covers when Europeans began to explore new trade routes, raw materials and uninhabited lands by sea. It is seen that Portugal, which is a small state in terms of the area it covers and located at the southwestern tip of Europe in particular, is the locomotive state in geographical discoveries, and respectively, followed by Spain, France, the Netherlands and England in this process.[10] Although the missionary aims to spread Christianity were dominant in the 14th century, as the main reason for geographical discoveries, economic purposes began to dominate from the 15th century.[11] Thus, in the 15th century, Europe, which was left behind in economic, political and social terms, began to seek ways to go to the East, which is considered the centre of wealth, without intermediaries.[12]

Geographical discoveries had very adverse effects on the Ottoman Empire. As can be seen from Figure 1, the most negative impact on the Ottoman Empire was that the Mediterranean began to lose its importance. In particular, the Mediterranean was an important route for products such as silk, paper, spices, and porcelain to reach Europe via the Silk Road. Alternative routes to the Mediterranean were found through new discoveries, and the Ottoman Empire lost an important source of tax revenue.[13] As the Mediterranean lost its importance, the people living on this route became unemployed with the decrease in the number of traders passing through the trade routes on the Mediterranean route. The Ottoman Empire started to give capitulations to the European states in order to revive

7 Sully et al. 1909: 78–81.
8 See Pagden 2002.
9 Hocaoğlu 2004: 54–55. Kodaman 2007: 12.
10 Arnold 1995: 13–15.
11 Gürbüz 2018: 6.
12 Uluerler 2018: 49.
13 Gürbüz 2018: 9; Uluerler 2018: 73.

the trade routes. Although this situation initially stimulated trade in the Mediterranean, over time, it became a tool for the exploitation of the empire by the European states.[14]

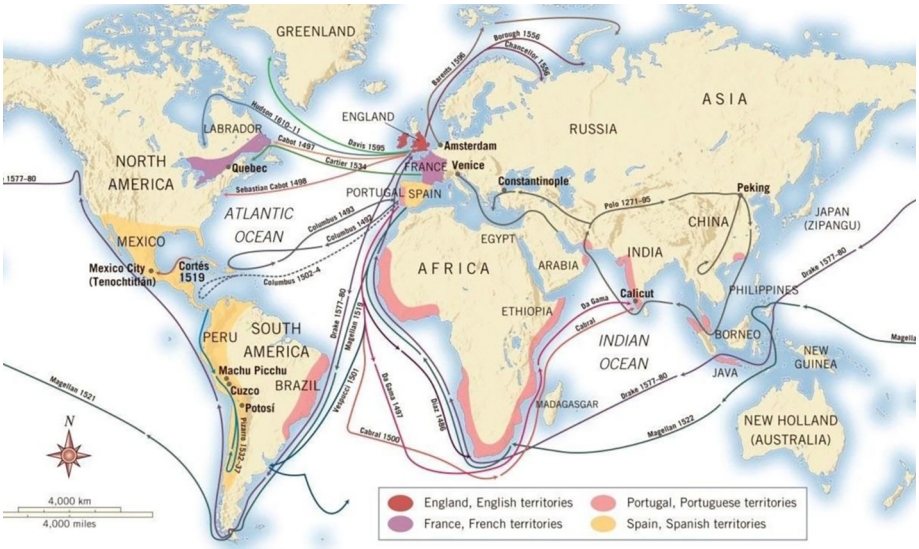


Figure 1: New trade routes and inhabited lands with the Age of Discovery
Source: www.studentsofhistory.com/routes-of-famous-european-explorers

In addition, the abundant gold and silver metals transported to Europe, especially from America, overthrew the monetary economy, and inflation began to occur in the Ottoman Empire.[15] Thus, gold and silver entering the Ottoman markets caused devaluations. For instance, as shown in Table 1 below, the silver gram ratio decreased steadily from 1.181 grams per hundred Dirhams in 1431 to just 0.323 grams by 1600. Likewise, Table 2 below illustrates how the ducat equivalent of mites surged from 45 in 1477 to 120 in 1586.[16]

Table 1: Effect of devaluation on silver in the empire

Year	Pieces of a hundred Dirhams	Silver gram ratio
1431	260	1.181
1460	330	0.931
1480	400	0.768
1491	420	0.731
1572	450	0.682
1585	800	0.384
1600	950	0.323

Source: compiled by the author based on Gürbüz 2018: 17.

14 Türkmen 1995: 332, 334, 335.
15 Uluerler 2018: 74.
16 Gürbüz 2018: 18.

Table 2: Effect of devaluation on gold in the empire

Year	Ducat equivalent of Mites
1477	45
1488	49
1510	54
1523	55
1548	57
1550	60
1566	60
1575	60
1586	120

Source: compiled by the author based on Gürbüz 2018: 18.

Also, European states began to gain strength "thanks to" the lands they colonised as a result of "discoveries". Thus, Europeans began to dominate in areas where Muslims lived densely, such as Indonesia, Malaysia, India and the Persian Gulf. Considering that the Ottoman Empire was an Islamic state and held the caliphate, this situation negatively affected the Ottoman's influence in the Islamic geography. The ineffectiveness of the caliphate in Islamic geography over the centuries will also be effective in the start of the Arab revolts with the effect of increasing nationalism.[17]

Finally, the European States, which were enriched by the lands they colonised as a result of the discoveries, became increasingly influential.[18] With these discoveries, Europe found ways of discovering both nature, matter and society and their laws, thus producing knowledge. As a result of this, Europe advanced, especially in military technology and science, gained power, wealth, knowledge, and gained the upper hand against the Ottomans.[19] Moreover, the bourgeois class, which got rich due to the discoveries in Europe, gained power and found new markets for European goods, and these developments triggered the Industrial Revolution.[20] Finally, in my opinion, due to the discoveries, Europe's development in the field of science and the understanding that "the world is round" and the absolute trust in the church was shaken, and the geographical discoveries also laid the groundwork for the Age of Enlightenment.

Age of Enlightenment

The foundations of the Age of Enlightenment, a science-based view of reason and divine concepts in Europe, are based on the Renaissance and Reformation movements. Later, this process accelerated with the increasing wealth of geographical discoveries.[21] Thus, the Age of Enlightenment emerged as an innovation movement based on rationality,

17 For the Arab Revolt 1916–1918 please see Fargo 1969.
18 Uluerler 2018: 74.
19 Kodaman 2007: 12.
20 Gürbüz 2018: 8.
21 Zariç 2017: 52.

which started in England in 1688 and was influential in all European countries, especially France. The new discoveries made in the scientific field at that time caused the church's authority to be shaken.[22]

As a matter of fact, this rationalist view, which started in Europe, reached its zenith with the French Revolution in 1789.[23] The French Revolution is one of the most important historical events that affected the collapse of the Ottoman Empire. This situation will be examined in the next part of the article.

Moreover, scientific and technological developments in the Age of Enlightenment contributed to the formation of the Industrial Revolution. Likewise, the social change and prosperity experienced with the Industrial Revolution contributed to the development of this age.[24] The Industrial Revolution is one of the other significant historical developments that was effective in the collapse of the Ottoman Empire, just like the French Revolution. In addition to the interaction of the Age of Enlightenment with two important events that played a role in the collapse of the Ottoman Empire, such as the French Revolution and the Industrial Revolution, the Age of Enlightenment negatively affected the Ottoman Empire in many ways. In this period, developments based on rationality and science enabled Europe to develop in the field of technology. As a result of this, it is seen that Europe, which has developed considerably in the field of new weapon technology, is ahead of the Ottoman Empire. The Europeans started to win the wars against the Ottomans with the new weapons they invented, which caused the collapse of the empire over time.[25] In this period, the understanding of colonialism gained momentum as a result of the power of Europe and the increasing need for raw materials with new technological developments.[26] Thus, the power gap between the Ottoman Empire and Europe gradually widened.

However, it should be noted here that the phenomenon of modernisation after the developments in the Age of Enlightenment undoubtedly affected the modernisation of the Ottoman Empire. However, this attempt could not go beyond imitating the Western European Civilization. As a positive result of the Ottoman modernisation process, we can see the establishment of the Modern Turkish Republic and Atatürk's reforms.[27] However, the Turkish Grand National Assembly, representing the new Turkish state established as a result of this modernisation, abolished the sultanate in 1922 and officially ended the Ottoman Empire, which was effectively ended with the Treaty of Sèvres in 1920.[28] In my opinion, although this is the official collapse of the Ottoman Empire, it is a positive development as it requires a republic and democracy, not a sultanate in the modern age. Although the Age of Enlightenment brought the end of the Ottoman Empire in the long run, I think it contributed to the modern Turkish Republic in this sense.

22 Zarıç 2017: 35.
23 Usta 2018: 75.
24 Eren 2017: 117.
25 Starkey 2003: 35, 176, 182.
26 Starkey 2003: 137, 186.
27 Gümüşlü 2008: 130.
28 Türkiye Büyük Millet Meclisinin, hukuku hâkimiyet ve hükümraninin mümessili hakikisi olduğuna dair. 1 November 1922, No 308, Grand National Assembly of Turkey, Ankara.

Industrial Revolution

The Industrial Revolution in England that took place after the second half of the 18th century and the great political revolution in France caused significant changes in the social structures of societies in Europe. With the Industrial Revolution, machines were invented, steam power was discovered, electrical energy was put into service in a way that people could use, and thus the rapid development of mechanisation shook the situation of artisans and masters working with manual power.[29]

The Ottoman Empire was incapable of predicting the results of this great transformation, and, therefore, in keeping up with this transformation. The source of this inadequacy was based on a long process dating back to geographical discoveries, long before the revolution.[30]

In addition, the Ottoman Empire could not realise the agricultural and population revolution. Accordingly, the empire fell behind in this matter, could not keep up with the Industrial Revolution. As can be seen in Table 3, the increase in agricultural products, the increase in the workforce employed in agriculture, and more importantly, the productivity of labour has increased since the beginning of the 16th century in England, where the Industrial Revolution began. This increase in output and productivity has allowed a larger population to be fed. These developments in the British agricultural sector have been one of the factors that directly affected England's being the leading country in the Industrial Revolution.

Table 3: England 1381–1700 annual production, labour and labour productivity growth rates in agriculture

Years	Output growth	Labour supply	Labour productivity
1381–1522	0.01	–0.01	0.2
1522–1700	0.38	0.25	0.13
1700–1759	0.79	0.22	0.57
1759–1801	0.85	0.44	0.41

Source: Broadberry et al. 2010: 367.

Besides, both domestic and foreign markets in the Ottoman Empire were under the protectionist and interventionist attitude of the state. Thus, the main purpose of the administration was to perpetuate the political order with economic balances. However, this situation prevented an economic and social transformation.[31] Besides, the Ottoman bureaucrats believed that agricultural production and agricultural society should be protected by the state.[32] Agricultural production was equivalent to approximately 65% of the national income in the last centuries of the state. It is seen that 80% of the total working population was employed in the agricultural sector in the last periods of the Ottoman Empire. These statistical data also show that the Ottoman Empire was an agricultural country, and it was not possible at that time to achieve industrialisation at the standards of European countries.[33]

29 Keleş 2019: 172.
30 Uluerler 2018: 73.
31 Akşin 1997: 194.
32 İnalcik–Quatert 2000: 189–190.
33 Keleş 2019: 172.

For these reasons, the Ottoman Empire could not keep up with the innovations brought by the Industrial Revolution. However, after the revolution, the countries with developed industries started colonial activities in search of raw materials and markets. With the opening of the political, military, and economic differences between the industrialising states and the Ottoman Empire, it became a market. Eventually, as a result of the Industrial Revolution, the Ottoman Empire became a semi-colonial state[34] with the 1838 Balta Liman Trade Agreement with Britain.[35] Furthermore, the Ottoman Empire had to make these agreements with other European states in the 19th century. The Ottomans made such trade agreements to get the support of western states against internal rebellions and potential land losses. In addition, it aimed to provide a partial expansion in its economy through foreign trade.

Table 4: Amounts of imports and exports in the Ottoman Empire in 1838 and 1870

Years	Import (m £)	Export (m £)
1838	4.4	6.2
1870	17.4	22.5

Source: compiled by the author based on Erdem 2016: 23.

As can be seen in Table 4, the Ottomans were able to achieve a partial opening with these agreements. However, in the long run, products of European origin dealt a great blow to the Ottoman domestic market. The domestic Ottoman industry, which could not keep up with the Industrial Revolution and had difficulties maintaining its comparative superiority in international markets as a result of these agreements, suffered greatly, foreign capital became stronger, foreign trade balances deteriorated more, and the country was forced to borrow rapidly.[36]

The Ottoman Empire, which could not pay its foreign debts, established the *Düyun-u Umumiye* (General Obligations Administration) with the pressures of the European states. Accordingly, the essential revenue sources of the state were left to the western creditor states. Thus, the Ottoman Empire completely lost its economic independence, and it became more challenging to keep up with the Industrial Revolution.[37]

French Revolution

As a result of this movement, which is defined as the rebellion of the people in France under the leadership of the intellectuals against the oppression of the king, the people put an end to the monarchy-based theocratic state structure in France and a new era began in the history of Europe and the world. With the French Revolution, concepts such

[34] See for details: https://web.archive.org/web/20131216025543/www.urunlu.com/BelgeOku2.aspx?y-kod=66
[35] Erdem 2016: 31–35.
[36] Erdem 2016: 23.
[37] Izol–Cingöz 2020: 392; Karaman 2018: 66.

as human rights, democracy, nationalism, freedom, justice, and equality emerged.[38] This revolution had a significant impact on the Ottoman Empire in two respects. The first was nationalist revolts and the second was democratisation movements.

Under the influence of the French Revolution, the absolutist kingdoms came to an end with the 1830 and 1848 revolutions in Europe. Formations such as the democratic state and social order, the secularisation of the state, and the nation-state structure gained momentum. Emerging concepts and structures affected not only Europe but the whole world.[39] Multinational empires such as the Ottoman Empire and Austria-Hungary were shaken by these nationalist movements. These nationalist uprisings in the Ottoman Empire were supported by the dominant powers to achieve their goals. In particular, Russia embarked on pan-Slavic movements in order to descend to the warm seas and instilled the idea of rebellion in the Serbs, Bulgarians and Greeks.[40] As can be seen, the increasing nationalism movement was used by the great powers. As a matter of fact, when these nations gained their independence, they could not go beyond the influence of these great powers. However, the revolts of these nations for independence played an important role in the collapse of the Ottoman Empire.

On the other hand, intellectuals who opposed the empire through concepts such as equality, freedom, justice and law emerged. These intellectuals forced the Ottoman Empire to make western-style reforms and democratise. In the developing process, the Ottoman Empire made some reforms. Eventually, it was governed by a constitutional monarchy instead of an absolute monarchy with the first Constitutionalism and the second Constitutionalism.[41] I would also like to point out that although this is seen as a positive development, it caused many internal problems and unrest, such as the 31 March incident,[42] since the sultans were reluctant to give their absolute powers. Therewithal, as this desire for revolution among the intellectuals could not find a response in the people, there was no mass revolution like in France. In particular, the intellectual group that called itself Young Turk among Ottoman officers was decisive in the establishment of constitutionalism. In my opinion, the Young Turks' taking power is directly related to the collapse of the Ottoman Empire. Because, instead of the balance policy[43] that the Ottoman sultans had applied for centuries, the empire collapsed at the end of the war, with the aggressive attitude of the Young Turks that dragged the Ottomans into the First World War.

Domestic reasons

For an important part of the history of the Republic of Turkey, politicians have tended to associate the problems experienced in the country with foreign powers. They were trying

38 Loules–Kaya 1992: 291; Karaman 2018: 66.
39 Aladağ 2007: 64–65.
40 Ketenci 2018: 351.
41 Karaman 2018: 72.
42 It is an attempted uprising and coup by those who oppose the Committee of Union and Progress and the sharia supporters after the proclamation of the Second Constitutional Era. Sultan Abdulhamid II, who was held responsible for the riots, was dethroned.
43 It is the name given to the alliances that the Ottoman Empire established with European states in order not to lose more land in the 19th and 20th centuries.

to convince the public that there is no problem in their administration and declared that almost every problem is caused by external forces, not internal ones. In fact, since this situation has become a habit, only external factors have been highlighted among the factors that were effective in the decadence of the Ottoman Empire by most people. Nonetheless, it is effective in the collapse of a state in problems that are internal as well as external. Hence, the Ottoman Empire did not feel external developments in its heyday due to its enormous systematic structure. However, as there were ruptures in the empire, it became open to external factors. Under this title, these internal reasons that were effective in the collapse of the empire will be examined.

Deterioration of the military organisation

One of the most important factors in the collapse of the Ottoman Empire was the deterioration of the military system. As a matter of fact, the empire, which dominated three continents for centuries, achieved this thanks to its strong and systematic military structure. The deterioration of the military system can be added to the loss of wars due to the backwardness of weapon technology from Europe and, accordingly, demoralisation. Since this situation has been analysed under the above title, it will not be mentioned again. The reasons for the deterioration of the military system are quite detailed and should be the subject of another study. Under this title, the deterioration of the timar cavalry and the janissary corps, which were the heart of the Ottoman Empire, will be analysed in a general way and its effects on the collapse of the Ottoman Empire will be mentioned.

Timar holders/cavalries are military units that are responsible for collecting taxes in the area given to them by the state. During the war, they had to provide all war materials and the number of cavalrymen to the empire, according to the tax revenue they collected, together with the taxes they collected here. In this way, the state met the need for soldiers without any money coming out of its treasury, and even the taxes collected by the cavalries contributed to the treasury.[44] However, corruption in the timar system occurred as a result of the illegal auctioning of timar lands and the loss of land due to wars.[45]

Also, the Ottomans kept the tax they received from the timar owners at the same level, despite the depreciation of money, which started with geographical discoveries in the 16th century. The reason for this was to compete with the developing armies of Europe with the Industrial Revolution. However, as a result of this, a significant part of the timar holders, whose income decreased significantly, had to leave their timar voluntarily.[46] Thus, the number of timar cavalry gradually reduced. As a result of this, the security of the empire weakened in the areas where the timar cavalry lands were located, and as a result of the deterioration of the system, the empire suffered a significant tax loss, and its economy was damaged. Moreover, feudal structure was formed by the emergence of *ayans*[47] in the lands where the fiefs remained vacant. While Europe was destroying the feudal system,

44 Gündoğdu 2021: 193–194.
45 Ceylanli 2011: 159.
46 Ceylanli 2011: 160.
47 It refers to the local landlords who gained power in a certain region during the Ottoman period.

a feudal structure was formed in the Ottoman Empire.[48] Gibb and Bowen state that sipahis, whose number was 200,000 at the time of Kanuni, decreased to 25,000 in the 18th century and they were used for back services in wars.[49] The dwindling timar cavalries were tried to be replaced by the janissaries.

The Janissary Corps comprised the majority of the infantry part of the Kapikulu Hearths affiliated to the Sultan, which was formed by raising children aged 10-15, gathered from Anatolia and Rumelia by the devshirme method.[50] Until it was abolished entirely in 1826, it went through a period of deterioration due to various reasons such as the deterioration of the devshirme system, irregularities in admissions to the quarry, uncontrolled increase in the quarry, shortage of treasury, bribery, favour and the negative effects of inflation, especially as a result of geographical discoveries at the end of the 16th century.[51]

The reasons listed above are directly related to the increase in the number of janissaries. There are many reasons for this situation. First of all, as mentioned before, due to the deterioration of the timar system, the number of cavalrymen with timar gradually decreased and the number of janissaries was increased to compensate for this.[52] In addition, the number of janissaries began to increase as the Ottomans failed to achieve their former successful results in the wars at the end of the 16th century, in connection with the backwardness of weapon technology.[53] Since the devshirme system was insufficient to meet the increasing number of janissaries, many Turks entered the hearth, the regular training period of the janissaries was shortened and people entered the hearth by bribery.[54] However, due to their ignorance and incompetence, the newly recruited personnel did not increase the combat power of this hearth, on the contrary, it destroyed the peace, discipline, and regular education.[55] Moreover, as the number of janissaries increased, the uprisings against the sultan also increased. The janissaries, who did not want to fight and were dissatisfied with the state administrators or the sultan, frequently rose up, causing the Ottomans to have a hard time.[56] The number of uprisings of the Janissaries, especially dissatisfied with their salaries, is incalculable. So much so that often the gold and silver items in the palace were melted and turned into *akçe* (coin), and the salaries of the janissaries were paid.[57] This situation deeply affected the military, political and economic power of the Ottoman Empire.

Economic, social and administrative disorders

It should be accepted that external reasons were mainly effective in the deterioration of the economic, social, and political system in the Ottoman Empire. While the technology and system of the European armies were developing, the deterioration in the Ottoman

48 Kodaman 2007: 13.
49 Gibb–Bowen 1951: 188–190; Ceylanli 2011: 161.
50 Kodaman 2007: 8.
51 Elibol 2009: 23.
52 Ceylanli 2011: 161.
53 Ceylanli 2011: 163.
54 İnalcik 1980: 289.
55 Ceylanli 2011: 163.
56 Elibol 2009: 39.
57 Ceylanli 2011: 166.

army forced the loot from the conquests to stop and the empire to pay compensation as a result of the lost wars. However, with the loss of importance of the Mediterranean with geographical discoveries, there was a loss of income, and inflation was experienced as gold and silver entered the markets. Moreover, with the capitulations, the Ottoman domestic industry, which could not compete with European goods, went into decline.[58] In addition, with the Industrial Revolution, it became impossible for the Ottoman economy, which was based on agriculture, to compete with the mechanised European economy. In the external factors part of the study, since the effects of those situations on internal factors are examined in detail, it will not be discussed again. In this part, the weak internal position of the Ottoman Empire, which made it open to external factors, will be discussed.

All this failure had a negative impact on the people and the army, causing frequent revolts, and as a result, the rulers and even the sultans had to change frequently.[59] Hence, these adverse developments had become triggers for each other. Disobedience has emerged in the military, ulama[60] and bureaucracy.[61] The rulers, who were constantly changed by military pressure, refrained from making reforms. In fact, generally pro-military administrators were brought to power and acted in their interests.[62] Managers, who were changed frequently in the corrupted system, started to take bribes by taking advantage of this opportunity. Particularly, it can be said that bribery has dominated all state mechanisms since the end of the 16th century. Thus, people who give a lot of money are appointed to public services and state administration, not people with merit. In fact, this situation deteriorated so much over time that even the bandits began to bribe the rulers with some of the goods and money they robbed.[63]

So much so that bribery and favouritism caused the collapse of the Ottoman justice system. Thus, favouritism, bribery and nepotism took the place of justice. Bribery and corruption, which started in the 16th century, increased gradually until the last period of the Ottoman Empire. The biggest factor for this is the deterioration in economic, administrative, military and social fields.[64]

Deterioration of the education system

For the professorship cadres, which were already few in the Ottoman classical period madrasah system, an examination was held among those who were candidates for it, and the most qualified ones could be placed in these cadres. However, with the deterioration that started at the end of the 16th century, the system of the professorship cadres was changed due to factors such as bribery, favouritism, and nepotism. The requirement of graduating from the madrasah for being a professor was abolished, and the people of state or sultan started to appoint the people they were influenced by as professors. Therefore,

58 Kodaman 2007: 13.
59 Ceylanli 2011: 163.
60 It is the name given to state officials engaged in religious, judicial, and educational affairs during the Ottoman period.
61 Kodaman 2007: 13.
62 Ceylanli 2011: 164–166.
63 Daşçioğlu 2005: 20.
64 Daşçioğlu 2005: 24.

uneducated professors started to be appointed to madrasahs. Over time, these uneducated people opposed the reforms to be made in education and argued that the reforms were against religion.[65]

Parallel to this, the madrasa was no longer able to scientifically confirm the facts, produce new ideas, discover or invent. Because it had tended to look for the subject and object of education in the metaphysical world and neglected the job of solving worldly and human problems by using the mind, creating technology by discovering the laws of nature, and thus the method of producing technologies that would increase material power and welfare. As a result, the scholastic mentality dominated the Ottoman intellectuals and education and prevented entry into the age of reason and science, where new ideas, new knowledge, and new technology could be produced.[66] Therefore, reason and science, which form the basis of Islamic belief, could not find the opportunity to guide the Ottoman madrasah education and intellectual life. For this reason, while Europe was establishing universities and institutes to produce science and knowledge, the Ottomans could not prevent the deterioration of the madrasahs instead of reforming them according to the new conditions.[67]

Conclusion

Depending on external factors, the Ottoman Empire weakened over the centuries as a result of geographical discoveries, the age of enlightenment, the industrial revolution, the French Revolution, and the effects they brought. Therewithal, corruption within the state in the army, economy, social, political and educational fields were also factors that accelerated this collapse.

In this study, it was seen that all external and internal factors are interrelated. Each problem triggered another, and thus the empire came to an end. Among these, the Ottoman Empire took its place in the pages of history when the internal structure of the empire, which was weak against external problems, was combined.

This study has shown us that disintegration does not specifically cover a time period. The 16th century, when the Ottoman Empire was at its strongest, was actually the year when the problems started. As these problems accumulated over the centuries and triggered other problems, as historians have stated, the Ottomans entered from a period of development to a period of stagnation, decline and collapse.

However, although the empire fell, it left its legacy to its successor, the modern Republic of Turkey. Although history never repeats itself, it is full of many similarities. Turkey should learn from the collapse of the Ottoman Empire, and should not make the country open to external factors by having a solid internal structure.

65 Aşkın 2019: 341–342.
66 Kodaman 2007: 14.
67 Kodaman 2007: 14.

References

Aladağ, Özgür (2007): Fransiz Devriminin Evrenselliği Üzerine. *Muhafazakâr Düşünce Dergisi,* 3(11), 55–70.

Arnold, David (1995): *Coğrafi Keşifler Tarihi.* Transl. Osman Bahadır, İstanbul: Alan Yayıncılık.

Aşkın, Deniz (2019): Osmanlı'da Kurumsal Eğitim Sisteminin Bozulması ve Sosyolojik Boyutları. In Polat, İrfan – Öntürk, Tolga – Yabalak, Halit (eds.): *Uluslararası Türkoloji Araştırmaları Sempozyumu,* 26–28 Eylül 2019, 339–346.

Akşin, Sina – Yurdaydin, Hüseyin G. – Faroqhi, Suraiya – Kunt, Metin – Ödekan, Ayla – Toprak, Zafer (1997): *Türkiye Tarihi 3: Osmanlı Devleti, 1600–1908.* İzmir: Cem Yayınevi.

Broadberry, Stephen et al. (2010): *British Economic Growth: 1270–1870.* Cambridge: Cambridge University Press. Online: https://doi.org/10.1017/CBO9781107707603

Ceylanli, Şahin (2011): Osmanlı Ordusunun Bozuluşu ve Çöküşü. *Istanbul Journal of Sociological Studies,* (22), 159.

Daşçioğlu, Kemal (2005): Osmanlı Döneminde Rüşvet ve Sahtekârlık Suçları ve Bunlara Verilen Cezalar Üzerine Bazi Belgeler. *Sayıştay Dergisi,* 59 20–25.

Elibol, Ahmet (2009): Yeniçeriler ve İktidar Bağlamında Osmanlı Sisteminin Dönüşümü. *Gazi Akademik Bakış,* 3(5), 21–40.

Erdem, Ekrem (2016): Sanayi Devriminin Ardindan Osmanlı Sanayileşme Hamleleri: Sanayi Politikalarinin Dinamikleri ve Zaafiyetler. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* (48), 17–44.

Eren, Leyla Gizem (2017): Mitlerin kendini yeniden üretimi: Aydınlanma felsefesinden aydınlanma projesine. *Başkent Üniversitesi Ticari Bilimler Fakültesi Dergisi,* 1(1), 115–129.

Fargo, Mumtaz Ayoub (1969): *Arab-Turkish Relations from the Emergence of Arab Nationalism to the Arab Revolt, 1848–1916.* PhD Dissertation. The University of Utah.

Gibb, H. A. R. – Bowen, Harold (1951): *Islamic Society and the West.* London: Oxford University Press.

Gümüşlü, Bedi (2008): Aydınlanma ve Türkiye Cumhuriyeti. *Hacettepe Üniversitesi Türkiyat Araştırmaları (HÜTAD),* 8, 123–144.

Gündoğdu, İsmail (2021): Tımarlı Sipahilere Hazineden Borç Verilmesi Meselesi: IV. Murat'ın Bağdat Seferi Örneği. *Akademik İncelemeler Dergisi,* 16(2), 191–210. Online: https://doi.org/10.17550/akademikincelemeler.931646

Gürbüz, Yüksel (2018): *Osmanli Devletinin Ekonomik Yapısı ve 16. Yüzyılda Gerçekleşen Devalüasyonun Nedenleri.* Akademik Kaynak. Online: www.akademikkaynak.com/wp-content/uploads/2018/09/Osmanl%C4%B1-Devletinde-Deval%C3%BCasyon-Yuksel-Gurbuz.pdf

Hanioğlu, M. Şükrü (2010): *A Brief History of the Late Ottoman Empire.* Princeton: Princeton University Press.

Hocaoğlu, Durmuş (2004): İlerleme Üzerine Bir Tahlil Denemesi. *Köprü,* 78, 36–60.

Hürriyet (2019): Osmanlı Devleti ne zaman kuruldu? *Hürriyet.com,* 20 November 2019. Online: www.hurriyet.com.tr/gundem/osmanli-devleti-ne-zaman-kac-yilinda-kuruldu-41378299

İnalcik, Halil (1980): Military and Fiscal Transformation in the Ottoman Empire, 1600–1700. *Archivum Ottomanicum,* 6, 283–337.

İnalcık, Halil – Quataert, Donald (1994): *An Economic and Social History of the Ottoman Empire, 1300–1914*. Cambridge: Cambridge University Press.
İnalcık, Halil – Quatert, Donald (2000): *Osmanlı İmparatorluğu'nun Ekonomik ve Sosyal Tarihi (1300–1600)* (Cilt 1). İstanbul: Eren Yayıncılık.
Izol, Ramazan – Cingöz, Murat (2020): Merkantalizm ve Sanayi Devrimi Sürecinde Osmanli Devleti'nin Konumu. *Akademik Hassasiyetler,* 7(14), 379–398.
Karaman, Mehmet Ali (2018): Fransız İhtilali'nin Osmanlı İmparatorluğu'na Etkileri. *Süleyman Demirel Üniversitesi Fen-Edebiyat Fakültesi Sosyal Bilimler Dergisi,* (44), 62–79.
Keleş, Bahattin (2019): *Sanayi Devriminin Osmanli Ekonomisi Üzerindeki Etkisi ve Cumhuriyet Dönemi Ekonomik Politikalarina Yansimalari (1876–1938).* International Congress on Economic and Administrative Sciences, Şırnak.
Ketenci, Ayşegül (2018): Panslavizm ve Başarısızlık Sebepleri. *Akademia Sosyal Bilimler Dergisi,* (1), 345–352.
Kodaman, Bayram (2007): Osmanlı Devleti'nin Yükseliş ve Çöküş Sebeplerine Genel Bakış. *Süleyman Demirel Üniversitesi Fen-Edebiyat Fakültesi Sosyal Bilimler Dergisi,* (16), 1–24.
Loules, Dimitris – Kaya, Selda (1992): Fransız Devriminin Yunanistan Üzerindeki Etkisi. *Tarih Araştırmaları Dergisi,* 15(26), 291–296. Online: https://doi.org/10.1501/Tarar_0000000034
Pagden, Anthony ed. (2002): *The Idea of Europe: From Antiquity to the European Union*. Cambridge: Woodrow Wilson Center Press – Cambridge University Press. Online: https://doi.org/10.1017/CBO9780511496813
Reid, James J. (2000): *Crisis of the Ottoman Empire: Prelude to Collapse 1839–1878*. Stuttgart: Franz Steiner.
Starkey, Armstrong (2003): *War in the Age of Enlightenment, 1700–1789*. Westport, CT: Greenwood Press.
Sully, Maximilien de Béthune, duc de, 1559–1641 – Mead, Edwin D. (Edwin Doak) – Hale, Edward Everett (1909): *The Great Design of Henry IV: From the Memoirs of the Duke of Sully, and the United States of Europe.* Boston: Ginn and Company.
Sultana, Summer – Sharif, Muhammad Amin (2019): The Role of Turkish Women in the Politics of Ottoman Empire. *Pakistan Journal of International Affairs,* 2(2), 37–49. Online: https://doi.org/10.52337/pjia.v2i2.60
Türkiye Büyük Millet Meclisinin, hukuku hâkimiyet ve hükümraninin mümessili hakikisi olduğuna dair. 1 November 1922, No 308, Grand National Assembly of Turkey, Ankara. Online: https://www5.tbmm.gov.tr/tutanaklar/KANUNLAR_KARARLAR/kanuntbmmc001/karartbmmc001/karartbmmc00100308.pdf
Türkmen, Zekeriya (1995): Osmanlı Devleti'nde Kapitülasyonlarin Uygulanılışına Toplu Bir Bakış. *Osmanlı Tarihi Araştırma ve Uygulama Merkezi Dergisi (OTAM),* 6(6), 325–341. Online: https://doi.org/10.1501/OTAM_0000000251
Uluerler, Sıtkı (2018): Coğrafi Keşifler ve Avrupa'nın Yayılması. In Özkan, Selim Hilmi (ed.): *Yeni ve Yakın Çağ Tarihi.* İstanbul: İdeal Kültür Yayıncılık, 45–78.
Usta, Ayşe (2018): Aydınlanma Düşüncesine Kısa Bir Bakış. *Kastamonu İletişim Araştırmaları Dergisi,* (1), 74–90.
Zariç, Sami (2017): Tarihsel Kökeninden Ülkelere Göre Türlerine Aydinlanma Felsefesi (Çağı) ve Türkiye Cumhuriyeti. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* (28), 33–54.

NEMZETBIZTONSÁGI SZEMLE
12. évfolyam (2024) 2. szám 18–37. | DOI: 10.32561/nsz.2024.2.2

Szénási Imre[1]

Kritikus rendszerelemek jellemzői, azok kijelölése, valamint azok védelme

Characteristics of Critical Infrastuctures, their Designation and Protection

Globalizált világunkban a kritikus rendszerelemek vagy más néven a kritikus infrastruktúrák védelme egyre nagyobb figyelmet kap. A tanulmányban megvizsgálom a kritikus infrastruktúrák védelmére a 21. században létrejött szabályozást az Amerikai Egyesült Államok, az Európai Unió, az Észak-atlanti Szerződés Szervezete és Magyarország szempontjából. A kritikus rendszerelemek védelme hazánkban alapvetően a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóságának hatáskörébe tartozik, azonban lehetnek olyan esetek, amikor nem a Belügyminisztérium, hanem a Magyar Honvédség látja el ezeket a feladatokat. Az őrzés-védelmi feladat e formája egyáltalán nem könnyű. Napjainkban megjelentek néhány évtizeddel ezelőtt még egyáltalán nem létező nyílt információforrások. Segítségükkel az őrzött kritikus infrastruktúra elleni támadás viszonylag egyszerűen megtervezhető, akár amatőrök számára is. A tanulmányban az orosz–ukrán háborúból származó példákat mutatok be arra, hogy egyszerű felhasználók is milyen hatékonyan támogathatják a hadseregek harcát, hogyan igazolhatják vagy cáfolhatják a propaganda állításait kizárólag az internet felhasználásával. Megfogalmaztam egy javaslatot az aktív és tartalékos katonák információtudatosságra való felkészítésére. A kutatásom során nyílt forrásokra támaszkodtam, a témához tartozó szakirodalom, a sajtóban megjelent források, valamint a jogszabályok analízisét és elemzését végeztem el.

Kulcsszavak: *kritikus rendszerelem, orosz–ukrán háború, nyílt információ, információtudatosság*

In today's globalised world, the protection of critical system components, also known as critical infrastructure, is receiving increasing attention. In this paper I will examine the regulation of critical infrastructure protection in the 21st century

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: imre.szenasi81@gmail.com

from the perspective of the United States of America, the European Union, the North Atlantic Treaty Organisation and Hungary. In Hungary, the protection of critical system elements is basically the responsibility of the National Directorate General for Disaster Management of the Ministry of the Interior. However, there may be cases where the Hungarian Defence Forces, rather than the Ministry of the Interior, carry out these tasks. The task of guarding and protecting is not an easy one, as open sources of information have emerged that did not exist a few decades ago, making it relatively easy for even amateurs to plan an attack on such guarded critical infrastructure. In this paper, I will present examples from the Russian war in Ukraine of how ordinary users can effectively support the armies' war effort and verify or refute propaganda claims using only the Internet. I have formulated a proposal for information literacy training for active and reserve soldiers.

Keywords: *critical infrastructure, Russian-Ukrainian war, open information, information awareness*

Bevezetés

Napjaink globalizált világában a kritikus rendszerelemek vagy más néven a kritikus infrastruktúrák védelme egyre nagyobb figyelmet kap. Hazánkban sincsen ez másképp.

Tanulmányomat a kapcsolódó fogalmak ismertetésével kezdem, majd rátérek a kritikus rendszerelemek jellemzőire és azok kialakulásának rövid történetére. Megvizsgálom a kritikus infrastruktúrák védelmére a 21. században létrejött szabályozást az Amerikai Egyesült Államok, az Európai Unió, az Észak-atlanti Szerződés Szervezete és Magyarország szempontjából.

A kritikus rendszerelemek védelme hazánkban alapvetően a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóságának hatáskörébe tartozik, azonban lehetnek olyan esetek, amikor nem a Belügyminisztérium, hanem a Magyar Honvédség látja el ezeket a feladatokat. Az aktív katonák létszámuknál fogva képtelenek lennének minden kijelölt kritikus infrastruktúra védelmére. A tartalékos rendszer kiegészíti a reguláris fegyveres erők képességeit, ezért ez a tevékenység megjelenik az Önkéntes Területvédelmi Tartalékosok feladatrendszerében is, összhangban a Magyar Honvédség Magyarország Nemzeti Katonai Stratégiájában[2] megfogalmazott küldetésével.

Az egyszerűnek tűnő őrzés-védelmi feladat azonban napjainkban egyáltalán nem könnyű. Néhány évtizeddel ezelőtt még egyáltalán nem létező, nyílt forrásúnak tekinthető információforrások jelentek meg, amelyek segítségével az őrzött kritikus infrastruktúra elleni támadás viszonylag egyszerűen megtervezhető, akár amatőrök számára is, az interneten fellelhető különböző applikációk és a közösségi média használatával.

Dolgozatomban az orosz–ukrán háborúból származó példákat mutatok be arra, hogy egyszerű felhasználók is milyen hatékonyan támogathatják a hadseregek harcát, hogyan igazolhatják vagy cáfolhatják a propaganda állításait, akár saját otthonukból a karosszékükben helyet foglalva, kizárólag az internet felhasználásával. A hipotézisem

[2] A Kormány 1393/2021. (VI. 24.) Korm. határozata Magyarország Nemzeti Katonai Stratégiájáról.

az, hogy a kritikus rendszerelemek védelme érdekében az azok őrzés-védelmét ellátó katonáinkat fel kell készíteni az internet és a közösségi portálok biztonságos használatára. A tanulmány végén javaslatot fogalmazok meg az aktív és tartalékos katonák információtudatosságra való felkészítésére. A kutatásom során nyílt forrásokra támaszkodtam, a témához tartozó szakirodalom, a sajtóban megjelent források, valamint a jogszabályok analízisét és elemzését végeztem el.

Kritikus infrastruktúrák, avagy kritikus rendszerelemek és azok jellemzői

Mielőtt megkezdem a kritikus infrastruktúra vizsgálatát, meghatározom az infrastruktúra szó jelentését. Az infrastruktúra:

> „közvetett módon, a szükséges feltételek, pl. infrastrukturális létesítmények, eszközök, speciális szaktudással rendelkező személyek megteremtésével járul hozzá a gazdasági-társadalmi szféra működéséhez. Két alapvető ágazata a termelői infrastruktúra (a gazdasági jellegű feltételek biztosítója) és a szociális infrastruktúra (a társadalmi jellegű feltételek biztosítója)."[3]

Amennyiben az infrastruktúrákat a fontosságuk szempontjából vizsgáljuk meg, akkor megkülönböztethetünk kritikus és sebezhető infrastruktúrákat. Tevékenységük alapvető fontosságú a gazdasági-társadalmi szféra működéséhez. Működésképtelenné válásuk esetén, ami megtörténhet valamilyen külső vagy belső beavatkozás következtében, az adott ország biztonsága kerülhet veszélybe, és ez beláthatatlan következményekkel járhat.[4]

Az infrastruktúra rövid bemutatása után rátérek a kritikus rendszerelemek fogalmának ismertetésére. A kritikus infrastruktúra fogalma Gőcze István szerint:

> „Magyarországon található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése, e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna."[5]

Gőcze István Magyarország szemszögéből vizsgálja ezt a területet, de az Európai Unió is foglalkozik a kérdéssel. A kritikus infrastruktúra fogalma az Európai Parlament és a Tanács 2022/2557 Irányelve[6] szerint: „olyan eszköz, létesítmény, berendezés, hálózat vagy rendszer, vagy valamely eszköz, létesítmény, berendezés, hálózat vagy rendszer része, amely szükséges az alapvető szolgáltatás nyújtásához."[7]

---

3 Közszolgálati Online Lexikon: infrastruktúra.
4 Haig–Kovács 2012: 45–46.
5 Közszolgálati Online Lexikon: kritikus infrastruktúra.
6 Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről.
7 A Tanács 2008/114/EK irányelve, 3.

A fogalmak meghatározása után ismertetem a kritikus infrastruktúra kialakulásának rövid történetét. A kritikus infrastruktúra nem új fogalom. Korábban nem pont ezen a néven illették, azonban a rendelkezésünkre álló írott történeti forrásokból kiderül, hogy a történelem során minden állam megvédte a gyenge pontjait. Gondoskodott azon infrastruktúrájának védelméről, amely a működéshez elengedhetetlen volt. Napjainkban ezeket már kritikus rendszerelemeknek is nevezik. Az ókori birodalmakban és a középkori államokban ezek elsősorban közlekedési és élelmiszer-ellátási útvonalakat vagy anyagi erőforrásaikat jelentették. Mindamellett a közigazgatási központok is a kritikus infrastruktúra elemei közé tartoztak.[8] A két világháború és a hidegháború alatt jött létre az, amit ma „kritikus infrastruktúrák védelme" elnevezéssel illetünk.[9]

Az emberi fejlődés dinamikus folyamata magával hozta az infrastruktúrák változását is. A folyamatból kiemelkedik az ipari forradalmak időszaka és a világháborúk kora, amelyek hatására robbanásszerű fejlődés következett be a technológiában és az infrastruktúrában. Az elektromosság felfedezése és elterjedése, a távközlési rendszerek kialakulása, a közlekedés új formáinak (például a vasút, a gépjárművek, a polgári repülés) megjelenése, az ipar tömegtermelésre való áttérése, valamint a kémiai-fizikai-biológiai tudományos felfedezések mind-mind könnyedebbé tették az emberek hétköznapi életét és lakhatóbbá a környezetet. Az új találmányok, a nagy technikai áttörések, a napjainkban megjelenő új fizikai és virtuális infrastruktúrák – egyesével és együttesen is – a rendszerek iránti függőség, az egymásrautaltság és a komplexitás veszélyét hordozzák magukban.[10]

A fentiekben megfogalmazottak miatt meghatározó jelentőségű, hogy feltérképezzük és pontosan behatároljuk a kritikus infrastruktúrákat. A kritikus rendszerelemek Haig Zsolt szerint alapvetően három fő típusra oszthatóak. Az első típus biztosítja a nélkülözhetetlen javak előállítását, szállítását és a társadalom számára alapvető fontosságú szolgáltatások folyamatos elérhetőségét. A második típusú kritikus infrastruktúrák teszik lehetővé az egymással való összeköttetést és az együttműködés képességét. A világháló és a különböző zárt kommunikációs és számítógép-hálózatok kötik össze és gyakran azokon keresztül irányítják és hangolják össze a társadalom és a gazdaság többi infrastruktúráját; ezeket kritikus információs infrastruktúráknak nevezik. A harmadik típusú kritikus infrastruktúrák járulnak hozzá az ország köz- és külső biztonságának megteremtéséhez. A kritikus infrastruktúrák védelme és működésének fenntartása a nemzetbiztonság szempontjából minden kormányzat meghatározó és létfontosságú feladata.[11]

A kritikus infrastruktúrákat fenyegető veszélyek

Az infrastruktúrára nyomást gyakorló fenyegetések a természetes és az épített környezetre is jelentős hatást gyakorolhatnak. Milyen, az infrastruktúrára leselkedő veszélyek vannak napjainkban?

A veszélyek megkülönböztethetőek a formáik szerint. Az ártó szándékú cselekedetek alapvető formái azok a szándékos károkozás céljából végrehajtott cselekmények, amelyek

8 Babos 2007: 14.
9 Babos 2016: 6.
10 Bonnyai 2019: 29.
11 Haig–Kovács 2012: 46.

nemcsak a keletkezett anyagi kár miatt jelentősek, hanem az egész társadalomra gyakorolt pszichológiai hatásuk is rendkívüli lehet. Az ártó szándékú cselekményeknek több típusa is létezik. Ide sorolhatók a klasszikus háborús cselekmények, a fegyveres összeütközések, a hibrid támadások, a terrorcselekmények, a kibertámadások, a társadalmi eredetű események (például zavargások), fegyveres konfliktusok kirobbantása, valamint a gazdasági, politikai okkal elkövetett visszaélések.[12]

Másik formaként a katasztrófajellegű eseményeket említhetjük – természeti, ipari vagy civilizációs katasztrófák –, amelyek bekövetkezési valószínűsége és gyakorisága csak nagyon csekély mértékben jelezhető előre, azonban bekövetkezésük jelentős következményekkel járhat.

Elsőként áttekintem a természeti eredetű veszélyeket, amelyek lehetnek hidrológiai események (ár-, bel- és villámárvíz, cunami), meteorológiai események, geológiai események (földrengések, földcsuszamlások), nagy kiterjedésű vegetációs tűzesetek, napkitörések. Az ipari eredetű veszélyek lehetnek valamilyen, az alkalmazott technológiában keletkező hibák, helytelen emberi beavatkozás vagy baleset miatt az ipari létesítményekben, illetve azokkal kapcsolatosan bekövetkező veszélyhelyzetek. A következőképpen jelenhetnek meg: veszélyes anyagokkal foglalkozó üzemben vagy egyéb ipari létesítményekben bekövetkező esemény, veszélyes áru szállításakor történt közlekedési baleset, környezetkárosodással járó esemény, nukleáris létesítményben bekövetkező esemény. A civilizációs katasztrófák a korunkbeli társadalom jellegzetességein alapuló olyan események, amelyek az alkalmazott rendszerek és a társadalom működőképességére egyformán kifejthetik a hatásukat. A civilizációs katasztrófák lehetnek: informatikai, kommunikációs vagy navigációs rendszerek rongálódása, humánegészségügyi és állategészségügyi epidémiák, táplálékhiány és vízkészletekért folyó fegyveres küzdelem vagy az infrastruktúrák kapacitásának kimerülése.[13]

Korunk ipari és gazdasági fejlettsége, a társadalom rétegei között tapasztalható egyre növekvő különbségek, a radikális vallási és politikai nézeteket valló csoportok számának folyamatos emelkedése és azok időszakos megerősödése, a világ terrorveszélyeztetettségének exponenciális növekedése mind okot szolgáltatnak arra, hogy a prevenciós szemlélet erősödjön.[14]

A kritikus rendszerelemek védelmére vonatkozó szabályozás fejlesztése

Amerikai Egyesült Államok

A prevenció szükségességét az Amerikai Egyesült Államokban is felismerték 1997-ben: az elnök kérésére egy tudományos testület (Federation of American Scientists) jelentést készített, amelyben felhívták a figyelmet a kritikus infrastruktúra sebezhetőségére,

12 Bognár–Bonnyai–Vámosi 2019: 33–35.
13 Bognár–Bonnyai–Vámosi 2019: 33–35.
14 Bognár–Bonnyai–Vámosi 2019: 33–35.

valamint ajánlásokat is megfogalmaztak azok védelmére.[15] A 2001. szeptember 11-i kritikus infrastruktúra elleni terrortámadás (World Trade Center és Pentagon)[16] után alkották meg a Nemzetbiztonsági Törvényt,[17] majd 2006-ban annak kiegészítését, a Nemzeti Infrastruktúra-védelmi Programot.[18] Az Egyesült Államok 16 kritikusinfrastruktúra-ágazatot azonosított, ezek a vegyipari, kereskedelmi létesítmények, hírközlési, kritikus termelési egységek, gátak, védelemipari, sürgősségi szolgáltatások, energia-, pénzügyi szolgáltatási, élelmiszeripari és mezőgazdasági, kormányzati létesítmények, egészségügyi és közegészségügyi, informatikai, nukleáris reaktorok, anyagok és hulladékok, közlekedési rendszerek, valamint a víz- és szennyvízrendszerek ágazata.

Európai Unió

Az Európai Unió (EU) 2004-ben kezdett el mélyrehatóbban foglalkozni a kritikus infrastruktúrával, az Európai Tanács júliusban átfogó stratégia kidolgozására kérte fel a Bizottságot a kritikus infrastruktúrák védelme javításának érdekében. Az Európai Unió Bizottsága ebben az évben hozta nyilvánosságra első javaslatát, a Létfontosságú Infrastruktúrák Védelmére Vonatkozó Európai Programot.[19] Ez alapján dolgozták ki az úgynevezett Zöld könyvet.[20] Az EU jogalkotási folyamatának eredményeként hirdették ki az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló irányelvet.[21] Az irányelv csak az energia- és a közlekedési ágazatra, valamint a kritikus infrastruktúrák védelmére összpontosított. Az irányelv alkalmazásában az európai kritikus infrastruktúra[22] fogalma:

> „a tagállamokban található olyan kritikus infrastruktúra, amelynek megzavarása vagy megsemmisítése jelentős hatással lenne legalább két tagállamra. A hatás jelentőségét a horizontális kritériumok alapján kell értékelni. Ide tartoznak azok a hatások is, amelyek az egyéb típusú infrastruktúrákkal fennálló, ágazatokon átnyúló kölcsönös függőségből erednek."[23]

Meghatározta a tagállamok részére, hogy 2011. január 12-ig meghozzák azokat az intézkedéseket, amelyekkel megfelelnek az irányelvnek. A 2008/114/EK irányelv 2024. október 18-ával hatályát veszti, és helyébe az Európai Parlament és a Tanács (EU) 2022/2557 irányelve lép, amelyet 11 ágazatra[24] kell alkalmazni.[25] 2016-ban az Európai Unió elfogadta

15 *Critical Foundations* 2007: 15.
16 The White House 2003: 15.
17 The USA PATRIOT Act 2001.
18 Mógor–Földi–Solymosi 2008: 15–27.
19 European Programme for Critical Infrastructure Protection, lásd: https://eur-lex.europa.eu/legal-content/EN-HU/TXT/?from=EN&uri=LEGISSUM%3Al33260
20 Zöld könyv COM(2005) 576.
21 A Tanács 2008/114/EK irányelve.
22 European Critical Infrastructure (ECI).
23 A Tanács 2008/114/EK irányelve, 3.
24 Energia, közlekedés, banki szolgáltatások, pénzügyi piaci infrastruktúra, digitális infrastruktúra, közigazgatás, világűr, egészségügy, ivóvíz, szennyvíz, valamint élelmiszer-előállítás, -feldolgozás és -forgalmazás.
25 (EU) 2022/2557 irányelv.

az Európai Parlament és a Tanács (EU) 2016/1148 számú, hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelvét (NIS).[26] Az első olyan átfogó szabályozás volt ez az információbiztonság területén, amely hálózati és információs rendszerek magas biztonsági szintjét kívánta biztosítani a közösségen belül. Az irányelv egyformán szabályozta az alapvető szolgáltatásokat biztosító szereplőket, valamint a digitális szolgáltatókat is.[27] Az irányelv a technológia fejlődésnek köszönhetően hamarosan elavulttá vált. Helyébe az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.), az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS 2) szóló irányelv[28] lépett 2023. január 16-án, amely korszerűsítette a jogi keretet a megnövekedett digitalizációhoz és a kiberbiztonsági fenyegetések változó környezetéhez való alkalmazkodás érdekében. A NIS 2 irányelv a kiberbiztonsági szabályok hatályát új ágazatokra és szervezetekre is kiterjesztette, valamint javította az Unió egészének kiberbiztonsági rezilienciáját.

Észak-atlanti Szerződés Szervezete

A NATO[29] elsődleges feladata 1949-es megalakulása óta a szövetség területének és a tagállamok népességének védelme a szerződés 5. cikkelye alapján. A Szövetség a hidegháború alatt nem hajtott végre semmilyen e cikkely hatálya alá eső műveletet, de felkészült arra, az esetleges vészhelyzetekre vonatkozó gyakorlatok végrehajtása során. Az 5. cikkely szerinti segítségnyújtást a 2001. szeptember 11-i, az Egyesült Államok elleni terrortámadás után aktiválták először.[30]

A kritikus rendszerelemek szempontjából azonban jóval fontosabb az Észak-atlanti Szerződés 3. cikkelye, amely kimondja: „A jelen szerződésben kitűzött célok hathatósabb elérése érdekében a Felek külön-külön és együttesen, folyamatos és hathatós önsegély és kölcsönös segítség útján, fenntartják és kifejlesztik egyéni és kollektív védelmi képességüket fegyveres támadással szemben."[31] Kijelenthető, hogy a NATO védelmi struktúrájában a civil mellett a katonai képesség biztosítására helyezi a fő hangsúlyt, amely csak abban az esetben teljesül, ha a tagországok rugalmasak és ellenállóak a fentiekben már felsorolt ártó szándékú cselekményekkel és katasztrófajellegű eseményekkel szemben. Az ellenálló képesség a NATO szerint az az egyéni és kollektív képesség, amely lehetővé teszi a tagállamok számára a sokkhatásokra és a zavarokra történő felkészülést, az ellenállást, az azokkal szemben alkalmazott válaszlépéseket, valamint az azokból történő gyors helyreállítást,

26 Network and Information Systems (NIS). Az Európai Parlament és a Tanács (Eu) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

27 Mógor–Angyal 2022: 119.

28 Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről.

29 Észak-atlanti Szerződés Szervezete.

30 NATO 2022a.

31 Az Észak-atlanti Szerződés, Washington DC, 1949. április 4.

és biztosítja a Szövetség működésének folytonosságát.[32] A fentiekben megfogalmazottak miatt a polgári védelem („olyan össztársadalmi feladat-, eszköz- és intézkedési rendszer, amelynek célja katasztrófa, illetve fegyveres összeütközés esetén a lakosság életének megóvása, az életben maradás feltételeinek biztosítása, valamint a lakosság felkészítése azok hatásainak leküzdése és a túlélés feltételeinek megteremtése érdekében")[33] a NATO nemzeti és kollektív ellenálló képességének egyik központi pillére és a kollektív védelem egyik kritikus eszköze, amely létfontosságú a társadalmak és a közös értékek védelme szempontjából.[34] A Szövetség támogatja a tagállamokat az ellenálló képesség megerősítésében. 2007-ben pedig készített egy összefoglalót a kritikus infrastruktúrák védelméről és az Európai Unióval történő együttműködésről.[35] A 2016-os varsói csúcstalálkozón a NATO tagországainak állam- és kormányfői megállapodtak abban, hogy fokozzák a Szövetség ellenálló képességét a fenyegetések teljes spektrumával szemben.[36] 2021-ben a brüsszeli csúcstalálkozón kötelezettséget vállaltak arra, hogy megerősítik a tagállamok rugalmasságát és a polgári felkészültségi intézkedéseket.[37] A NATO 2022-ben egy új bizottságot hozott létre, az Ellenálló Képesség Bizottságot,[38] amely átvette a Polgári Vészhelyzeti Tervezési Bizottság[39] feladatait és szerepét is. Az Ellenálló Képesség Bizottság felelős az Észak-atlanti Szövetségen belül a stratégiai és szakpolitikai irányvonal megalkotásáért és a NATO ellenálló képességgel kapcsolatos tevékenységeinek koordinálásáért. A Szövetség legfontosabb politikai dokumentuma a stratégiai koncepció. A 2022. évben elfogadott stratégiai koncepció szerint a NATO alapvető feladatai – az elrettentés és a védelem, a válságmegelőzés és -kezelés, valamint az együttműködő biztonság – szempontjából kritikus fontosságú az ellenálló képesség. Annak elfogadásakor a tagállamok egyetértettek abban, hogy megerősítik a nemzeti és szövetségi szintű ellenálló képességet a katonai és nem katonai fenyegetésekkel, valamint a biztonságot érintő kihívásokkal szemben is.[40] A 2023-as vilniusi csúcstalálkozón a szövetséges vezetők megismételték a Szövetség elkötelezettségét a rugalmasság megerősítése mellett. Kiemeltek továbbá több olyan területet, amely további odafigyelést igényel, beleértve a társadalmi ellenálló képességet, az egészségügyi rendszereket, a kritikus infrastruktúrát és az ellátási láncokat is.[41]

A NATO 1992 és 2023 között 23 alkalommal rendezte meg a NATO Válságkezelési Gyakorlatát (CMX),[42] ahol a polgári vezetők mellett a katonai törzsek és a NATO Parancsnokságok vesznek részt. A 2023-ban megrendezett CMX 23 gyakorlaton a fentiekben felsoroltak mellett részt vett Finnország és Svédország, valamint az Európai Külügyi Szolgálat, az Európai Bizottság, valamint az Európai Tanács és az Európai Unió Tanácsa

32 NATO 2023b.
33 Lásd: www.katasztrofavedelem.hu/265/mi-a-polgari-vedelem#Mi%20a%20polg%C3%A1ri%20v%C3%A9delem?
34 NATO 2023b.
35 NATO 2007.
36 NATO 2016.
37 NATO 2021.
38 Resilience Committee (RC) – Ellenálló Képesség Bizottság.
39 Civil Emergency Planning Committee (CEPC) – Polgári Vészhelyzeti Tervezési Bizottság.
40 NATO 2022b.
41 NATO 2023c.
42 Crisis Management Exercise (CMX) – Válságkezelési Gyakorlat

Főtitkársága is. Ezen gyakorlatok célja a NATO stratégiai, politikai és katonai szintű konzultációs és döntéshozatali eljárásainak tesztelése.[43]

Magyarország

Magyarország mint az Európai Unió egyik tagja természetesen eleget tett a 2008-as európai uniós irányelvnek. Annak kiadása előtt, 2008-ban a kormány tárcaközi szakmai munkacsoport bevonásával megalkotta a nemzeti kritikus infrastruktúrák védelméről szóló Nemzeti Zöld Könyvet,[44] majd 2012 novemberében kihirdették, és több lépcsőben hatályba lépett a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, valamint a 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.[45] A 2013. évi L. törvény[46] szabja meg az állami és önkormányzati szervek mellett a kritikus rendszerek és létesítmények információbiztonsági keretrendszerét, amelyek hatósági felügyeletét a Nemzetbiztonsági Szakszolgálat látja el.[47] 2020-ban lépett hatályba a Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Kormány határozat, amelynek számos rendelkezése a létfontosságú rendszerek védelmére vonatkozó feladatokat fogalmazott meg.

A hazai szabályozásban a kritikus infrastruktúrák védelmében érintett ágazatokat és alágazatokat az 1. táblázat tartalmazza.

1. táblázat: A kritikus infrastruktúrák védelmében érintett ágazatok és alágazatok

Ágazat	Alágazat
Energia	villamosenergia-rendszer létesítményei (kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek)
	kőolajipar
	földgázipar
	távhő
Közlekedés	közúti közlekedés
	vasúti közlekedés
	légi közlekedés
	vízi közlekedés
	logisztikai központok
Agrárgazdaság	mezőgazdaság
	élelmiszeripar
	elosztó hálózatok

43 NATO 2023a.
44 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.
45 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.
46 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
47 Lásd: www.katasztrofavedelem.hu/109/kritikus-infrastrukturak-vedelmevel-osszefuggo-hatosagi-feladatok-jogszabalyok

Ágazat	Alágazat
Egészségügy	aktív fekvőbeteg-ellátás és a működtetéséhez szükséges szolgáltatások
	mentésirányítás
	egészségügyi tartalékok és vérkészletek
	magas biztonsági szintű biológiai laboratóriumok
	gyógyszer-nagykereskedelem
Társadalom-biztosítás	társadalombiztosítási ellátások igénybevételéhez kapcsolódó informatikai rendszerek és nyilvántartások
Pénzügy	pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei
	bank- és hitelintézeti biztonság
	készpénzellátás
Infokommunikációs technológiák	internet-hozzáférési szolgáltatás és internet-infrastruktúra
	elektronikus hírközlési szolgáltatások, elektronikus hírközlő hálózatok
	műsorszórás
	postai szolgáltatások
	kormányzati elektronikus információs rendszerek
Víz	ivóvíz-szolgáltatás
	felszíni és felszín alatti vizek minőségének ellenőrzése
	szennyvízelvezetés és -tisztítás
	vízbázisok védelme
	árvízi védművek, gátak
Honvédelem	honvédelmi rendszerek és létesítmények
Közbiztonság-védelem	rendvédelmi szervek infrastruktúrái

Forrás: www.katasztrofavedelem.hu/110/erintett-agazatok-alagazatok

Az Európai Unió NIS irányelvének integrációja is megtörtént a hazai szabályozásban, aminek következtében már megjelent a kibervédelem.[48] Hazánk a NIS 2 irányelvet is bevezette 2024. január 1-jén,[49] ezzel igyekszik csökkenteni a kiberbiztonsági fenyegetések kockázatát és biztosítani a szolgáltatások folyamatosságát.

Magyarországon a NATO védelmi struktúrája is megvalósul a kritikus rendszerelemek vonatkozásában. Egyrészt a honvédelmi létfontosságú rendszerelemek tekintetében.[50] Másrészt a nemzeti szabályozás lehetőséget ad arra, hogy honvédelmi érdekből, jogszabályban meghatározott feltételek alapján kijelölhető, nem honvédelmi ágazatba tartozó elem is nemzeti létfontosságú rendszerelemmé váljon. Az üzemeltetői biztonsági terv megalkotásához a honvédelmi hatóság speciális előírásokat tehet, ahol külön rész foglalkozik a honvédelmi sajátosságokkal, a honvédelmi szervekkel történő kapcsolattartással és az együttműködés rendjével.[51]

48 Mógor–Angyal 2022: 119.
49 23/2023. (XII. 19.) Szabályozott Tevékenységek Felügyeleti Hatóság rendelet az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásáról.
50 359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről.
51 Mógor–Angyal 2022: 119.

A nemzeti ellenálló képesség megszilárdításában előrelépést jelentett a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény,[52] amely önálló fejezetben határozza meg a nemzeti ellenálló képesség rendszerének követelményeit.

A területvédelmi tartalékosok és a kritikus rendszerelemek

Magyarországon a tartalékos rendszer keretfeladatait a Nemzeti Katonai Stratégiában fogalmazták meg.[53] A politikai vezetés e dokumentumban határozta meg a haderő részére a honvédelmi kiegészítő és hátországvédelmi képességeket, valamint a tartalékosokkal szemben támasztott elvárásokat. A Magyar Honvédség folyamatosan erősíti reguláris és tartalékos haderejét egy, a kor színvonalán álló fegyveres erő kialakítása érdekében, hogy az képes legyen a jelenkor biztonsági kihívásainak és kockázatainak megfelelni. Az önkéntes tartalékos rendszernek képessé kell válnia békében és a különleges jogrend bevezetése esetén is a hivatásos és szerződéses állomány támogatására, az új típusú kihívásokat is beleértve, valamint kiegészítő erőként azzal koherens rendszert alkotni.[54]

A területvédelmi erők rendeltetése az ország függetlenségének, területi épségének és határainak katonai védelme bármely lehetséges agresszor támadásával szemben, ami összhangban van a NATO-szabványokkal. A szövetség minden tagállamának rugalmasnak kell lennie, saját védelmi képességeinek kiépítésére vonatkozóan (Észak-atlanti Szerződés 3. cikkely), a nemzetközi szerződésekből eredő közös védelmi feladatok ellátása, természeti és ipari katasztrófavédelmi tevékenységek végzése, valamint a nemzetközi jog szabályainak megfelelően humanitárius feladatok ellátásának érdekében. A tartalékos rendszer kiegészíti a reguláris fegyveres erők képességeit, azonban helyettesíteni nem képes azt.

A területvédelmi erők fő feladatai összhangban vannak a Magyar Honvédség Magyarország Nemzeti Katonai Stratégiájának megfogalmazott küldetésével.[55] A területvédelmi tartalékos erők fő feladatai az alábbiak:

- a területvédelmi rendszer folyamatos működtetése és fejlesztése;
- részvétel őrzés-védelmi feladatokban, a létfontosságú rendszerelemek vagy más néven a kritikus infrastruktúra védelmében, valamint a polgári védelmi feladatok támogatásában;
- a tartalékos állomány alapkiképzése és további kiképzések végrehajtása;
- helyi protokolláris feladatok ellátása, valamint hadisírok, katonai és hősi emlékművek fenntartása és kegyeleti tevékenységekben való részvétel;
- Magyarország területének területvédelmi biztosítása, valamint a lakosság élet- és vagyonbiztonságának védelme;
- részvétel a tömeges bevándorlás elleni védekezésben;
- különböző válságkezelési tevékenységek összehangolása és megvalósítása, valamint részvétel a katasztrófavédelmi feladatokban a nemzeti biztonsági rendszer más elemeivel együttműködve a helyi közösségek védelme és támogatása érdekében;

52 2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról.
53 1393/2021. (VI. 24.) Korm. határozat.
54 1393/2021. (VI. 24.) Korm. határozat.
55 1393/2021. (VI. 24.) Korm. határozat.

- a Befogadó Nemzeti Támogatás katonai feladatainak biztosítása és koordinálása a szövetséges erők hatékony fogadásának és Magyarországon való állomásoztatásának lehetővé tétele érdekében;
- a magyar társadalomban a hazafias értékek megőrzése, erősítése, valamint a katonai nevelési programok nemzedékeken átívelő megvalósítása.[56]

A területi elven (járásonként) szervezett önkéntes védelmi képesség, amely az Önkéntes Területvédelmi Tartalékos (ÖTT)[57] rendszert jelenti, összesen 197 ÖTT-századot alkot Budapest kerületeiben és az ország járásaiban. Az ÖTT megyénként alkot egy területvédelmi zászlóaljat (TVZ), zászlóaljanként egy aktív kiképző századdal, valamint régiónként egy, összesen hét területvédelmi ezredet (TVE).

A Magyar Honvédség Területvédelmi Erők Parancsnoksága (MH TVEP) felelős a területvédelmi feladatokat ellátó szervezeti elemeinek hadműveleti és harcászati szintű irányításáért. Az alárendeltségébe tartozik az ÖTT szolgálati forma bevezetése óta megalakított hét TVE is.

A területvédelmi tartalékosok fentiekben felsorolt feladataiból kiemelkedik a kritikus rendszerelemek védelme. Az ÖTT-katonák elsősorban a saját járásukban látnak el feladatokat, emiatt kiemelkedő helyismerettel rendelkeznek. A katasztrófajellegű események, mint a természeti, ipari vagy civilizációs katasztrófák esetében részt vehetnek a megelőzésben (például: árvízvédelem) és a katasztrófák következményeinek felszámolásában (például: földrengések utáni keresés, kutatás, romeltakarítás) is, de ezzel a feladatcsoporttal a terjedelmi korlátok miatt nem foglalkozom.

A területvédelmi tartalékosok az ártó szándékú cselekmények, mint a háborús cselekmények, a fegyveres összeütközések, a hibrid támadások és a terrorcselekmények esetében kiképzettségük és felszerelésük miatt elsősorban élőerővel megvalósított őrzés-védelmi feladatokat láthatnak el. Elsődlegesen, de nem kizárólag az energia-, a közlekedés, az infokommunikációs technológiák és a honvédelmi ágazat területén.

Az egyik legnagyobb veszély, amely a katonák által őrzött objektumokra leselkedhet, az a fegyveres támadás (terrorcselekmény, tüzérségi tűzcsapás, drónokkal vagy beszivárgott élőerővel végrehajtott támadás, szabotázs stb.). Általánosságban kijelenthető, hogy napjainkban a leggyorsabb és legegyszerűbb formája az ilyen típusú támadások előkészítéséhez szükséges információk beszerzésének a nyílt források felhasználásával a közösségi média felületeiről történhet.

A nyílt információ forrásai

Az Információs Hivatal honlapján[58] megtalálhatóak a hírszerzés forrásai, amelyek lehetnek: humán műveleti tevékenység,[59] technikai hírszerzés,[60] valamint nyílt forrású hírszerzés.[61]

---

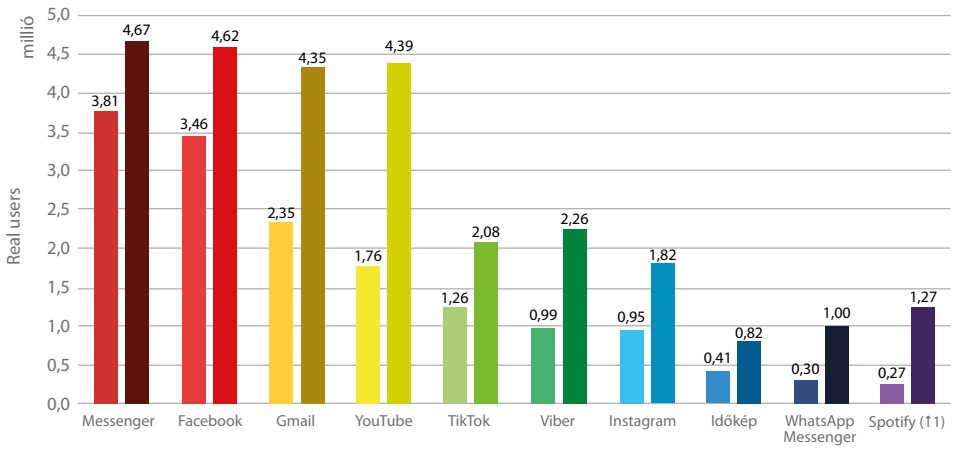
56 Magyar Honvédség Sipos Gyula 6. Területvédelmi Ezred.
57 25/2016. (XII. 22.) HM rendelet az egyes honvédelmi miniszteri rendeletek módosításáról.
58 Lásd: https://ih.gov.hu/
59 Human Intelligence – HUMINT.
60 Signals Intelligence – SIGINT.
61 Open Source Intelligence – OSINT.

A nyílt forrású hírszerzés fogalma: „bárki számára hozzáférhető, nyilvános és legális eszközökkel megszerezhető információk, melyeknek forrásai az elektronikus média, az írott sajtó, az internetes oldalak, az ingyenes és kereskedelmi adatbázisok lehetnek. Ezek szisztematikus gyűjtése és feldolgozása révén hírszerzési szempontból releváns információk keletkeznek."[62]

A nyílt információ a fent felsorolt forrásokból szabadon hozzáférhető, ebből következik, hogy nem válthatja ki az elsősorban minősített forrásokból megszerzett titkos és bizalmas információkat. Ennek ellenére olyan információkat tudhatunk meg a segítségével, amelyek elősegíthetik akár a minősített információk közti tájékozódást is. A nyílt információk felhasználásának hatalmas előnye, hogy az internet segítségével olyan adatokhoz juthatunk hozzá szabadon, akár valós időben, minimális anyagi ráfordítás mellett, amilyenekről néhány évtizeddel ezelőtt még álmodni sem lehetett. Természetesen mint mindennek, ennek is vannak hátrányai. A hátrányok közé tartozik például a rendelkezésre álló adatok gigantikus mennyisége – rendszerezésére a mesterséges intelligencia alkalmazása nyújthat segítséget. További hátránya, hogy számos, az internetre feltöltött anyag pontatlanságokat tartalmaz, vagy éppen dezinformációs céllal került fel a világhálóra, azonban ezek kiszűrésére is léteznek módszerek.[63]

Vizsgáljuk meg, hogy egy kritikus infrastruktúra elleni támadás megtervezéséhez milyen adatokhoz férhetünk hozzá nyílt forrásokat használva, vagyis az internetet és a közösségi média elemeit alkalmazva. Mindenekelőtt ki kell választanunk a célpontot, amelynek elsődleges funkciójáról, a hierarchiában elfoglalt helyéről annak hivatalos honlapjáról tájékozódhatunk. A kritikus infrastruktúra célpontként történő azonosítása során annak ellátott funkciója irreleváns. A támadás helyszínének kiválasztását követően több olyan, akár ingyenes szolgáltatást is igénybe vehetünk, amelyekkel a célterületről műholdképet, utcai nézetet (például: Google Maps, Maxar Technologies), valamint más, akár 3D-s térképet is letölthetünk, segítségükkel meghatározva a behatolási pontokat. A célpont felderítésében segítségünkre lehetnek a különböző videómegosztó portálok (YouTube, TikTok stb.), hiszen ezekre az emberek néhány like reményében rengeteg videót töltenek fel. A felvételek felbontásának minősége manapság akár a 12K-t[64] is elérheti, de egy viszonylag olcsó mobiltelefonnal is képesek 4K felbontású videók elkészítésére és feltöltésére. Amennyiben valaki célzott keresést használ, számos, addig ismeretlen adatot találhat a célpontról, amellyel megkönnyíti a gyenge pontok meghatározását. A nyílt információk egy másik nagy szeletét a hazánkban is népszerű különböző közösségi oldalak adják.

62 Információs Hivatal: A hírszerzés forrása. Lásd: https://ih.gov.hu/a-hirszerzes-forrasai.html
63 Bányász–Orbók 2013.
64 Lásd: www.youtube.com/watch?v=lFKCmnhPftM



1. ábra: A tíz legtöbb internetezőt elérő applikáció Magyarországon 2024. februárban (átlagos napi real users és havi real users)
Forrás: NMHH 2024.

Az 1. ábrából világosan kirajzolódik, hogy a közösségi médiát többen használják, mint az e-mail-szolgáltatást. Hazánkban 2024 februárjában a tíz legtöbb internetezőt elérő applikációból négy a közösségi médiához tartozott. Általánosságban véve kijelenthető, hogy a közösségi média felhasználóinak nagy többsége nem törődik a személyes adatainak védelmével, az applikációk biztonsági beállításaival vagy az általuk alkalmazott informatikai eszközök megfelelő biztonsági garanciáinak betartásával. Anyagi szempontból ugyan a közösségi média használata az esetek többségében ingyenesnek tekinthető, mégis óriási árat fizet vagy fizethet érte a felhasználó. Kiadja a személyes adatait, kapcsolati hálóját (például: LinkedIn), valamint az életének szinte minden mozzanatát. Az adatokat megszerző cégek ezeket továbbadják másoknak reklámcélra.[65] A nyílt forrású hírszerzés használatával nagyon sok érzékeny információhoz juthatunk hozzá az óvatlan felhasználók nem szándékos és sokszor nem is tudatos segítségével. A Facebook, hazánkban a jelenleg legnépszerűbb közösségi alkalmazás, például alapesetben a következő adatok hozzáféréséhez kér engedélyt a mobiltelefonon telepítve: naptár, tárhely (médiafájlok), fényképezőgép, helyadatok, hívásnaplók, mikrofon, névjegyek, telefon.[66] Az itt felsorolt adatok kiszolgáltatásáról az átlagos felhasználók többségének elképzelése sincs.[67]

A kritikus infrastruktúra védelmével megbízott katonák is emberek, akik a fenti adatok alapján nagy valószínűséggel használják a közösségi média felületeit. A katonák ilyen típusú feladatba történő bevonása előtt nagyon fontos a közösségi média használatából eredő veszélyekre figyelmeztetni és felkészíteni őket, valamint arra, hogy mire kell figyelniük. Elmagyarázni nekik az ebben az esetben az őket (is) védő rendszabályokat, ismertetni a közösségi média felületein alkalmazható biztonsági beállításokat, ahogyan ez a külszolgálatokban érintett, különösen a veszélyes területeken szolgáló katonák

65 Bányász–Orbók 2013.
66 Forrás: a szerző Facebook-applikációja.
67 Bányász–Orbók 2013.

esetében meg is történik. A kulcsszónak, véleményem szerint, a felkészítés során az információtudatosságnak kell lennie.

Most pedig tekintsük át, hogy mire kell még figyelni a katonáknak, milyen veszélyek leselkednek rájuk mint közösségimédia-felhasználókra az orosz–ukrán háború tapasztalatai alapján.

A nyílt információ amatőrök általi felhasználása hírszerzésre az orosz–ukrán háborúban

A nyílt információk megszerzésének a jelenleg is zajló orosz–ukrán háborúban is sok formáját alkalmazták és alkalmazzák. Megdöbbentő módon nemcsak a hivatalos szervek, hanem az „egyszerű" állampolgárok (az úgynevezett fotelkémek vagy Twitter-kémek) is. Ennek köszönhetően teljesen új szintre emelkedett a nyílt forrású hírszerzés.

Sokszor önkéntesen tevékenykedő állampolgárok próbálják meg kideríteni, mi igaz az orosz és ukrán oldal által is erősen befolyásolt narratívákból. A Twitter-kémek ellenőrzik a fotók, videók és beszámolók valóságtartalmát, a munkájukat pedig az ukrán és az orosz hadsereg is egyaránt felhasználja.

Hogyan lesz valaki Twitter-kém? – vetődik fel a kérdés. Az egyik választ a *Washington Post* hasábjain találhatjuk meg. Egy 29 éves férfi, Kyle Glen, aki klinikai kutatóként dolgozott Walesben, 2023-ban felfedezett egy videót a *Telegram*on. A képkockákon az volt látható, hogy feltehetően az orosz hadsereg egy ukrán civilek által használt menekülési útvonalat bombázott. Többen úgy vélték, ez ukrán dezinformáció. A férfi elemezni kezdte a felvételt, és felfedezett egy jellegzetes nevezetességet, egy olyan ortodox templomot, amelynek négy aranykupolája is volt. A Google Maps felhasználásával, valamint az Associated Press által készített fénykép segítségével meghatározta az épület pontos koordinátáit. A területtel foglalkozó Discord-, Reddit- és Twitter-bejegyzések átnézése során a robbanás szemtanúinak beszélgetéseire bukkant. Mindössze tizenkét perccel azután, hogy észrevette a felvételt, már teljesen biztos volt abban, hogy az általa felfedezett videó valódi, és közzétette az általa megalkotott elemzést a Twitter-fiókján. Létrejött új identitása: Twitter-kém lett.[68]

Természetesen nincs egyedül. Az egyik leghíresebb fotelkém az alig 20 éves Justin Peden, egy alabamai egyetemista, aki a Twitteren „The Intel Crab" néven vált híressé. Jelenleg több mint 334 500 követővel rendelkezik,[69] és több tízmillióan tekintették meg a bejegyzéseit. Az általa alkalmazott technika az, hogy ingyenes és nyíltan elérhető térképszolgáltatásokat, például a Google Earth-öt és a Yandex Maps-t használja fel, esetenként fizetős kereskedelmi műholdas adatokkal párosítja azokat, így lokalizálja az orosz légicsapásokat, tüzérségi csapásokat és egyéb érdekes pontokat. Ezt a folyamatot nevezik geolokációnak. Egy kép apró részletei alapján kideríthető, hogy pontosan hol készült. Elegendő azt térképekkel vagy kereskedelmi műholdas adatokkal összevetni, és azonnal,

[68] Verma 2022.
[69] Twitter: *IntelCrab*.

igen nagy pontossággal megerősíthető az, ami addig a pillanatig csupán megérzés vagy elmélet lett volna.[70]

A hobbikémek száma hatalmas, például a Project OWL, a nyílt forráskódú hírszerzők privát közössége az orosz–ukrán háború kirobbanását követően öt hét alatt 15 000 tagról közel 30 000-re nőtt a csoport moderátorai szerint.[71] Az idő múlásával pedig egyre ügyesebbekké is váltak. Széles körű hírszerzési adatokat képesek begyűjteni egyszerű eszközökkel. Néhányan repülőgépek és hajók követésére, mások műholdképek elemzésére, míg többen a háborús területen működő webkamerák képeinek elemzésére specializálódtak. Mások a NASA bozóttűz-adatbázisát[72] használják az ukrán „termikus anomáliák" nyomon követésére.[73]

A Twitter-kémek a geolokáció segítségével meghatározhatják az egyes ellenséges eszközök valós helyzetét is. Az így megszerzett információt felhasználva az általuk támogatott fegyveres erők könnyedén megsemmisíthetik azokat, ahogyan ez az úgynevezett „teknőstank" esetében is történt. Villámgyorsan kiderült, hogy hol rejtőzködik, ugyanis az orosz civilek fényképeket készítettek az épületben, amelyeket az internetre is feltöltöttek. Az ukrán hadsereg egy öngyilkos drónja pedig lecsapott a kínálkozó lehetőségre.[74]

A másik meglepő forrása az információknak egy meglehetősen sajátos tevékenység, nem más, mint a társkeresés. Minden embernek, így a katonáknak is megvannak a szükségleteik; mint Maslow kifejtette, az emberi szükségletek piramisának első szintjén a fiziológiai szükségletek között vannak a szexuális szükségletek.[75] Ezt természetesen a hírszerzésben dolgozók is kihasználják. A Tinderre, napjaink egyik legelterjedtebb társkereső alkalmazására, sok orosz katona is regisztrált, amit észlelve ukrán nők vették fel velük a kapcsolatot és szedtek ki szenzitív információkat belőlük,[76] amelyeket valószínűleg továbbítottak az ukrán hatóságoknak.

Az ukrán kormány állampolgárait is bevonta a nyílt forrású hírszerzésbe, a Diia nevű e-kormányzati applikációval. A program eredetileg az állampolgárok számára készült e-ügyintézési felületként a bürokrácia csökkentésére. Az ukrán kormány az orosz inváziót követően elindította az erre épülő, E-Enemy nevű funkciót. Az applikáción keresztül az állampolgárok az orosz csapatmozgásokról és háborús bűncselekményekről tájékoztathatják az ukrán hadsereget.[77] Az ide képeket vagy videókat feltöltő személyek azonosíthatóságuk esetén veszélybe kerülhettek, amennyiben a képek megjelentek a médiában, és orosz kézbe jutottak.

Nem feledkezhetünk meg a nyílt információkat elemzők másik nagy csoportjáról, a hivatásos újságírókról és a digitális oknyomozó riporterekről sem. A Bellingcat kutatók, nyomozók és polgári újságírók független oknyomozó kollektívája. Az itt dolgozó személyeket a nyílt forráskódú kutatás iránti szenvedély fogta össze.[78]

---

70 Mahadevan 2022.
71 Verma 2022.
72 NASA FIRMS.
73 Nagy 2022.
74 Portfolio 2024.
75 Maslow 1943: 370–396.
76 Parker 2022.
77 Technokrata 2022.
78 Bellingcat: Who We Are. Lásd: www.bellingcat.com/about/who-we-are/

A fentiekben láthattuk, hogy a sokszor önkéntesen tevékenykedő „fotelkémek” milyen hatékonyan tevékenykednek. Feltételezhetjük azt, hogy a profi, a különböző hírszerző szolgálatok által ki- és továbbképzett szakemberek ennél is hatékonyabbak. Valószínűleg néhány apró adatmorzsa felhasználásával is össze tudnak rakni rólunk és az általunk őrzött objektumról egy használható képet. Elképzelhető, hogy komolyabb dolgokra is tudnak következtetni.

Összegzés

Tanulmányomban áttekintettem a kritikus rendszerelemek legfőbb jellemzőit, kialakulásuk rövid történetét. A kritikus infrastruktúrák alapvetően három fő típusra oszthatóak: az első típus biztosítja a nélkülözhetetlen javak előállítását, szállítását és a társadalom számára alapvető fontosságú szolgáltatások folyamatos elérhetőségét. A második típusú kritikus infrastruktúrák teszik lehetővé az egymással való összeköttetést és az együttműködés képességét. A harmadik típusú kritikus infrastruktúrák járulnak hozzá az ország köz- és külső biztonságának megteremtéséhez. Foglalkoztam az ezekre leselkedő fenyegetések fajtáival, amelyek lehetnek katasztrófajellegű események és ártó szándékú cselekmények. Rámutattam arra, hogy a kritikus infrastruktúrák védelme és működésének fenntartása a nemzetbiztonság szempontjából minden kormányzat meghatározó és létfontosságú feladata.

Megvizsgáltam a kritikus infrastruktúrák védelmére a 21. században létrejött szabályozást az Amerikai Egyesült Államok, az Európai Unió, az Észak-atlanti Szerződés Szervezete és Magyarország szempontjából.

Rámutattam arra, hogy a kritikus rendszerelemek védelmét esetenként a Magyar Honvédség is elláthatja. Ez a tevékenység megjelenik az Önkéntes Területvédelmi Tartalékosok feladatrendszerében is, összhangban a Magyar Honvédség Magyarország Nemzeti Katonai Stratégiájában megfogalmazott küldetésével. Az őrzés-védelmi feladat napjainkban egyáltalán nem egyszerű a néhány évtizeddel ezelőtt még egyáltalán nem létező nyílt információk elemzésével megvalósított hírszerzés miatt. Az így beszerzett adatok segítségével egy jól őrzött kritikus infrastruktúra elleni támadás is viszonylag egyszerűen megtervezhető, akár amatőrök számára is az interneten fellelhető különböző applikációk és a közösségi média használatával. Tanulmányomban az orosz–ukrán háborúból származó információk alapján rámutattam arra, hogy „egyszerű” civilek milyen hatékonyan támogathatják a hadseregek harcát, valamint hogyan igazolhatják vagy cáfolhatják a propaganda állításait az internet felhasználásával.

Felhívtam a figyelmet arra, hogy a kritikus infrastruktúra védelmével megbízott katonák is emberek, akiknek többsége minden bizonnyal használja a közösségi média felületeit. A katonák feladatba történő bevonása előtt fontos a közösségi média használatából eredő veszélyekre figyelmeztetni, és felkészíteni őket arra, hogy mire kell figyelniük. Elmagyarázni nekik az ebben az esetben őket (is) védő rendszabályokat, ismertetni a közösségi média felületein alkalmazható biztonsági beállításokat, ahogyan ez a külszolgálatokban érintett, különösen a veszélyes területeken szolgáló katonák esetében meg is történik.

Tehát a katonáink felkészítése során törekedni kell az információtudatosságra, mert az internetalapú nyílt forrású hírszerzési módokat csak így lehet kivédeni.

Sajnos az eddigiekben nem fordítottunk erre túl sok figyelmet. Valószínűleg nehéz lesz a katonák digitális lábnyomát olyan szintre hozni, ahol már nem túl nagy, de mégis használhatják a közösségi médiát önmaguk és az általuk védett objektumok veszélyeztetése nélkül. Mindezt elérni kizárólag csak oktatással és az internethasználat tudatos központi és önkorlátozásával lehet. A tanulmány bevezetőjében megfogalmazott hipotézisem, amely szerint a kritikus rendszerelemek védelme érdekében az azok őrzés-védelmét ellátó katonáinkat fel kell készíteni az internet és a közösségi portálok biztonságos használatára, igaznak bizonyult.

Felhasznált irodalom

A Kormány 1393/2021. (VI. 24.) Korm. határozata Magyarország Nemzeti Katonai Stratégiájáról

A Tanács 2008/114/EK irányelve (2008. december 08.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32008L0114&from=HR

Az Európai Parlament és a Tanács (Eu) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016L1148

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről

Az Észak-atlanti Szerződés. Online: www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=hu

Babos Tibor (2007): *The Five Central Pillars of European Security*. Brussels: NATO Public Diplomacy Division. Online: www.files.ethz.ch/isn/56271/07_Babos.pdf

Babos Tibor (2016): The First Critical Infrastructure Protection Research Project in Hungary. In Nádai László – Padányi József (szerk.): *Critical Infrastructure Protection Research*. Switzerland: Springer International Publishing, 1–22. Online: https://doi.org/10.1007/978-3-319-28091-2

Bányász Péter – Orbók Ákos (2013): A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. *Hadtudomány,* 23(e-szám), 188–209. Online: http://hdl.handle.net/20.500.12944/1371

Bognár Balázs – Bonnyai Tünde – Vámosi Zoltán (2019): *Kritikus infrastruktúrák védelme I.* Budapest: Dialóg Campus.

Bonnyai Tünde (2019): Történeti áttekintés. In Bognár Balázs – Bonnyai Tünde (szerk.): *Kritikus infrastruktúrák védelme I.* Jegyzet. Budapest: Dialóg Campus, 29–46. Online: http://hdl.handle.net/20.500.12944/12450

Critical Foundations – Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection. Washington DC, 1997. október 13. Online: www.fas.org/sgp/library/pccip.pdf

European Programme for Critical Infrastructure Protection. Online: https://eur-lex.europa.eu/legal-content/EN-HU/TXT/?from=EN&uri=LEGISSUM%3Al33260

Haig Zsolt – Kovács László (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. Budapest: NKE. Online: www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf

Magyar Honvédség Sipos Gyula 6. Területvédelmi Ezred. Online: https://honvedelem.hu/alakulat/magyar-honvedseg-sipos-gyula-6-teruletvedelmi-ezred.html

Mahadevan, Alex (2022): This College 'Nerd' Investigates the Ukraine War from the Digital Front Lines. *Poynter,* 2022. május 24. Online: www.poynter.org/reporting-editing/2022/the-intel-crab-twitter-ukraine-russia-war-osint-justin-peden/

Maslow, Abraham H. (1943): A Theory of Human Motivation. *Psychological Review,* 50(4), 370–396. Online: https://doi.org/10.1037/h0054346

Mógor Judit – Angyal István (2022): A létfontosságú rendszerek védelmére vonatkozó szabályozás fejlesztése. *Scientia et Securitas,* 3(2), 118–125. Online: https://doi.org/10.1556/112.2022.00102

Mógor Judit – Földi László – Solymosi József (2008) Lépések a kritikus infrastruktúra védelmének magyarországi szabályozása felé. *Hadmérnök,* 3(4), 15–27. Online: http://hadmernok.hu/archivum/2008/4/2008_4_mogor.pdf

Nagy Nikoletta (2022): Fotelkémek ezreit nevelte ki az orosz–ukrán konfliktus. *24.hu,* 2022. június 8. Online: https://24.hu/tech/2022/06/08/osint-nyilt-forrasu-megfigyeles-kemek-orosz-ukran-haboru-kozossegi-media/

NASA FIRMS: https://firms.modaps.eosdis.nasa.gov/map/#d:24hrs;@0.0,0.0,3.0z

NATO (2016): *Warsaw Summit Communiqué*. Online: www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

NATO (2021): *Brussels Summit Communiqué*. Online: www.nato.int/cps/en/natolive/news_185000.htm?selectedLocale=en

NATO (2022a): *Crisis management*. Online: www.nato.int/cps/en/natohq/topics_49192.htm

NATO (2022b): *NATO 2022 Strategic Concept*. Online: www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO (2023a): *NATO Crisis Management Exercise 2023 (CMX23)*. Online: www.nato.int/cps/en/natohq/news_212527.htm

NATO (2023b): *Resilience, Civil Preparedness and Article 3*. Online: www.nato.int/cps/en/natohq/topics_132722.htm

NATO (2023c): *Vilnius Summit Communiqué*. Online: www.nato.int/cps/en/natohq/official_texts_217320.htm

NATO Parliamentary Assembly (2007): *The Protection of Critical Infrastructures*. Online: www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/270/270907/270907jopling_en.pdf

NMHH (2024): https://nmhh.hu/cikk/245667/Az_online_mediater_kozonsege_2024_februar

Parker, Nick (2022): RUDE ARMY Randy Russian Soldiers Bombard Ukrainian Girls With Flirty Tinder Requests. *The U.S. Sun,* 2022. február 23. Online: www.the-sun.com/news/4757640/russian-soldiers-tinder-ukraine/

Portfolio (2024): Túl nagy sztárrá vált az oroszok új páncélos szörnyszülöttje, meg is lett az eredménye. *Portfolio,* 2024. április 10. Online: www.portfolio.hu/global/20240410/tul-nagy-sztarra-valt-az-oroszok-uj-pancelos-szornyszulottje-meg-is-lett-az-eredmenye-679615

Technokrata (2022): Az ukránok e-kormányzati appot is bevetnek az orosz hadsereg ellen. *Technokrata,* 2022. április 21. Online: www.technokrata.hu/app/2022/04/21/diia-e-kormanyzati-app-ukrajna/

The USA PATRIOT Act: Preserving Life and Liberty. Washington DC, 2001. október 26. Online: www.justice.gov/archive/ll/what_is_the_patriot_act.pdf

The White House (2003): *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*. Washington DC. Online: www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

Twitter: *IntelCrab*. Online: https://twitter.com/IntelCrab

Verma, Pranshu (2022): The Rise of the Twitter Spies. *The Washington Post,* 2022. március 23. Online: www.washingtonpost.com/technology/2022/03/23/twitter-open-source-intelligence-ukraine/

Zöld Könyv A Létfontosságú Infrastruktúrák Védelmére Vonatkozó Európai Programról. Brüsszel, 17.11.2005, COM(2005) 576 végleges.

Jogi források

23/2023. (XII. 19.) Szabályozott Tevékenységek Felügyeleti Hatóság rendelet az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásáról

25/2016. (XII. 22.) HM rendelet az egyes honvédelmi miniszteri rendeletek módosításáról

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról

2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

NEMZETBIZTONSÁGI SZEMLE
12. évfolyam (2024) 2. szám 38–54. | DOI: 10.32561/nsz.2024.2.3

Márton Balázs[1]

Lehetőségek a nemzetközi terrorizmussal kapcsolatos integrált kormányzati tájékoztatás és a nemzetbiztonsági megközelítés erősítésére

Possibilities of Strengthening Integrated and National Security Approach in the Governmental Information Process Regarding International Terrorism

A nemzetközi terrorizmus súlyos kihívást jelent az Európai Unióban. Annak ellenére, hogy Magyarországon alacsony a nemzetközi terrorizmusból fakadó kockázat, a globális és a regionális biztonságpolitikai folyamatok azt vetítik előre, hogy fokozni kell a nemzetközi terrorizmus elleni nemzeti erőfeszítéseket. Ezeknek a részét képezik a nemzetbiztonsági megközelítést igénylő felderítési, koordinációs és kormányzati tájékoztatási feladatok. Az integrált kormányzati tájékoztatás eléréséhez az általános hatáskörű nemzetbiztonsági fúziós központ létrehozása érdemi előrelépés, azonban a nemzetközi terrorizmussal kapcsolatos információmegosztás, koordináció és kormányzati tájékoztatás rendjében fennmaradt néhány párhuzamosság és átfedés. A vonatkozó jogszabályok, valamint az érintett szervek feladat- és hatáskörének pontosítása mellett, a Terrorellenes Koordinációs Bizottság biztonsági architektúra szerveitől való függetlenítése megfelelő lehet ezek korrekciójára. Nemzetközi példa igazolja, hogy egy különös hatáskörű fúziós szerv felállításának van létjogosultsága. Megfontolandó volna a bizottság mellett egy ilyen szervként funkcionáló állandó titkárságot szervezni, amely egyfelől elősegítheti, hogy a bizottság független, teljes körű, objektív és integratív módon láthassa el a döntéstámogató feladatait, sőt akár arra is alkalmas lehet, hogy a nemzetközi terrorizmust mint egyre nagyobb biztonsági kihívást láthatóbbá tegye.

Kulcsszavak: *nemzetbiztonság, fúziós központ, rendvédelem, terrorizmus, titkosszolgálat, terrorelhárítás*

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

According to Europol's assessment, international terrorism is a serious challenge in the European Union. Despite the low risk of international terrorism in Hungary, global and regional security policy developments predict that national efforts against this threat must be strengthened. These include reconnaissance, coordination and governmental information tasks requiring a national security approach. In order to achieve integrated government information, the creation of the national security fusion center is a significant step forward, however, some parallels and overlaps remain in the order of information sharing, coordination and government information related to international terrorism. In addition to clarifying the relevant legislation and the tasks and powers of the relevant state agencies, the independence of the Anti-Terrorism Coordination Committee from the security architecture agencies may be appropriate for their correction. According to international example the establishment of a fusion center with special powers related to international terrorism may have added value. It should be considered to organize a permanent secretariat functioning as such a fusion center to the committee, which could, on the one hand, help the committee to perform its decision-supporting tasks in an independent, comprehensive, objective and integrative manner, and could even be suitable to make international terrorism more visible as an ever-increasing security challenge.

Keywords: *national security, fusion center, law enforcement, terrorism, intelligence, counter terrorism*

Bevezetés

A nemzetközi terrorizmus súlyos veszélyt jelentő biztonsági fenyegetés az Európai Unióban – derül ki az Europol legfrissebb helyzetértékelési jelentéséből. A dokumentum szerint 2022-ben összesen 28 terrorcselekmény történt a tagállamok területén, amelyekbe a meghiúsult és megakadályozott események is beleértendők.[2] A nemzetközi terrorizmusra Magyarország is kihívásként tekint, a Nemzeti Biztonsági Stratégia külön szól a szervezett, nemzetközi, fundamentalista vallási irányzatokkal és a migrációval összefüggő terrorizmusról.[3]

Magyarországon a terrorfenyegetettségi helyzet a jelen tanulmány lezárásának időpontjában alacsonyként értékelhető. Terrortámadásokat eddig szinte kivétel nélkül magányos elkövetők, sporadikus jelleggel követtek el, jóllehet tetteik a büntetőjog szerint terrorcselekménynek minősültek.[4] Ez a fajta úgynevezett belföldi terrorizmus a tanulmány érdeklődési körén kívül esik. Az aktuálisan alacsony fenyegetettségi szint által sugárzott békesség látszatában viszont hibás döntés lenne elkényelmesedni. Az előttünk álló időszak jóval nehezebbnek ígérkezik, legalábbis, ha a jelen biztonságpolitikai folyamataiból indulunk ki. Ezek alapján egyre komolyabb erőfeszítést fog igényelni, hogy a nemzetközi terrorizmus jelentette fenyegetést a mostanihoz hasonló, alacsony

[2] Europol 2023.
[3] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Korm. határozat 66.
[4] Az Egységes Nyomozó Hatósági és Ügyészségi Bűnügyi Statisztika (ENYÜBS) adatai szerint a regisztrált terrorcselekmény bűncselekmények száma 2018. VII. hótól összesen 54.

szinten tartsuk. Az orosz–ukrán háború, a térségbe irányuló fegyverszállítmányok, a proliferáció, a balkáni régió immanens instabilitása, a nyugat-balkáni migrációs útvonal telítettsége, a klímaváltozás és a népességnövekedés okozta újabb migrációs hullámok, a globális migráció növekedése, valamint a közel-keleti térségben zajló folyamatok mindegyike afelé mutat, hogy Magyarországnak a következő évtizedben minden erejével a nemzeti rezilienciája megőrzésére kell törekednie, amelynek mérvadó összetevője a nemzetközi terrorizmus elleni harc.

A nemzetközi terrorizmus elleni harc sokösszetevős feladat, megtalálható benne (1) a terrorcselekmények megelőzése, (2) a terrorista csoportok és a terrorszervezetek felderítése és felszámolása, (3) a terrorcselekmények következményeinek kezelése, (4) a védelmi képességek megerősítése, illetve (5) a veszélyhelyzetekre való felkészülés.[5] A teendők sorrendjében az első, viszonylag jól elkülöníthető szakasz a terrorfelderítés. A terrorfelderítéshez nemzetbiztonsági megközelítésre és eszközrendszerre, ezeken belül pedig széles körű információgyűjtésre, információegyesítésre (fúzió), értékelő-elemző feldolgozásra, koordinációra, előrejelzés-készítésre, trendelemzésre, stratégiai tervezésre és a politikai döntéshozó egységes tájékoztatására van szükség. Ezek megelőzik a potenciális terrorcselekmény elkövetését *(preoperativitás),* és a belbiztonság fenntartása mellett a szövetségesi kötelezettségek teljesítése érdekében is folytathatók. A terrorfelderítéshez rendelt erőforrásokat a fenyegetés attribútumaihoz célszerű igazítani. A felderítés után preventív és/vagy preemptív jellegű aktív intézkedés vagy felszámolás következhet, amely utóbbi során a nemzetbiztonsági metodika ideiglenesen háttérbe szorul, és a rendészeti szemlélet és az eseménykezelés dominál *(intraoperativitás).* A felszámolás elvezet a nemzetközi terrorizmus elleni harc *posztoperatív* szakaszához, amely magában foglalja a következmények kezelését. A megelőzés, a védelmi képességek erősítése és a felkészülés a biztonsági szféra komplementer szereplőinek és a lakosságnak a bevonásával zajló általános prevenciót szolgáló proaktív és folytonos teendők. A következőkben kizárólag a terrorfelderítés szakaszával és ezen belül az információfúzióval, információmegosztással, a közös elemzéssel-értékeléssel *(joint analysis),* koordinációval és a politikai döntéshozó egyesített (integrált) tájékoztatásával foglalkozom. A politikai döntéshozó tájékoztatására a kormányzati tájékoztatás kifejezést használom.

A hipotézisem szerint, noha az általános hatáskörű nemzetbiztonsági fúziós központ (Nemzeti Információs Központ, NIK) létrehozása az integrált kormányzati tájékoztatás elérése érdekében tett komoly előrelépésnek bizonyult, a nemzetközi terrorizmus vonatkozásában fennmaradtak párhuzamosságok és átfedések. A hatályos struktúrában konzerválódik a rendészeti megközelítés, és olyan aszimmetriák találhatók, amelyek nehezíthetik a releváns információk szintetizálását, széttöredezhetik a kormányzati tájékoztatást, ráadásul fontos képességeket szoríthatnak háttérbe. A megoldást a terrorfelderítési ökoszisztéma finomhangolása és a főbb szervek feladat- és hatáskörének áramvonalasítása jelenthetik, amelyek többleterőforráshoz vezethetnének. A kormányzati tájékoztatás szélesebb körű integrálhatósága érdekében megfontolás tárgyát képezheti egy – valamilyen fokú szervezeti önállósággal rendelkező – kifejezetten a nemzetközi terrorizmusra fókuszáló különös hatáskörű fúziós szerv életre hívása.

[5] 1163/2020. (IV. 21.) Korm. határozat 99.

A fentiek igazolásához bemutatom a nemzetközi terrorizmusra irányuló kormányzati tájékoztatás rendjének hazai alakulását, a jobb áttekinthetőség végett három korszakra bontva: 2001-től 2010-ig, 2010 és 2022 között, valamint 2022 után. A rövid történeti kitekintéssel az a célom, hogy dinamikájában láttassam az egyes szerveket és szerepüket. A hatályos szisztéma felvázolásakor rávilágítok azokra a problémás részekre, amelyek kiigazításához hasznosak lehetnek a felvetéseim, amelyeket a tanulmány végén részletezek. A terjedelmi korlátok pusztán átfogó vizsgálatot engednek, ezért részletes kodifikációs megoldásokat és szervezeti terveket a tanulmány nem tartalmaz.

A nemzetközi terrorizmusra irányuló kormányzati tájékoztatás 2001 és 2010 között

A nemzetközi terrorizmus fogalma mint globális fenyegetés a köztudatban 2001. szeptember 11-én az Amerikai Egyesült Államokban elkövetett terrortámadásokat követően honosodott meg. A tragikus esemény egy sor reformtörekvésnek adott lendületet, amelyek az amerikai nemzetbiztonsági közösségen *(Intelligence Community)* belüli horizontális koordináció és a politikai döntéshozó tájékoztatásának javítását tűzték zászlójukra. A nemzetközi terrorizmus hatásai a nemzetbiztonsági igazgatás hazai megszervezésében is érezhetők voltak. Magyarországon a ’90-es években megerősödő szervezett bűnözés elleni harc jegyében már 2000-ben törvény született a Szervezett Bűnözés Elleni Koordinációs Központ (SZBKK) létrehozásáról. Ez információegyesítő, koordináló és stratégiai elemző feladatokra jött létre, tevékenysége középpontjában – ahogyan nevéből is világos – a szervezett bűnözés, s nem a terrorfelderítés állt. A rendészeti igazgatás részét képező központ korlátozott mandátuma miatt rendvédelmi fúziós szerv volt és nem válhatott a nemzetbiztonsági ökoszisztéma részévé. A nemzetközi terrorizmusra irányuló felderítés ebben az időben a polgári elhárítás szervének (Nemzetbiztonsági Hivatal, NBH) hatáskörébe tartozott. A nemzetbiztonsági szolgálatokról szóló törvény (Nbtv.) szövege egészen 2010-ig úgy rendelkezett, hogy az NBH felderíti és elhárítja külföldi hatalmak, szervezetek vagy személyek terrorcselekmény elkövetésére irányuló törekvéseit. Ezt egészítette ki, hogy a polgári hírszerzésért felelős szerv (Információs Hivatal, IH) a nemzetbiztonságot veszélyeztető, külföldi terrorszervezetekről folytatott információgyűjtést. Az említett nemzetbiztonsági szolgálatok az Nbtv. nyújtotta lehetőségek mentén nemzetbiztonsági eszközrendszerrel úgynevezett szűrő-kutató felderítést végezhettek. A felderítés csak konkrét terrorcselekmény elkövetésének gyanúja esetén oszlott meg az NBH és a Rendőrség között, attól függően, hogy a jelzés melyik szervhez érkezett, illetve melyik szerzett róla tudomást.[6] A büntetőeljárási törvény alapján folytatott bűnüldözési célú felderítés eltérő megközelítést kíván a nemzetközi terrorizmus elleni harc jegyében alkalmazott nemzetbiztonságihoz képest, így ebben az irányban nem mélyítem a vizsgálódást. Az Nbtv. a katonai nemzetbiztonsági szolgálatokhoz is telepített a terrorizmussal kapcsolatos

[6] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 2010. III. 31. napján hatályos állapota, 5. § *c)*, 4. § *c)*, 5. § *i)*.

feladatokat. A nemzetközi terrorizmus elleni fellépés katonai szegmense önálló diszciplína része, ezért ez szintén kívül esik a tanulmány érdeklődési körén.

A horizontális együttműködés terén a kétezres évek elején tapasztalható hiátus kitöltésére a jogalkotó 2005-ben egy állandó testület létrehozásáról döntött, amely a terrorfelderítés műveleti koordinációját segítette. A Terrorellenes Koordinációs Bizottság (TKB) kifejezetten az ország nemzetközi terrorizmus elleni fellépésben vállalt kötelezettségeire és az érdekeinket közvetlenül veszélyeztető támadások ellen jött létre, hogy a segítségével a terrorveszéllyel és terrorfenyegetettséggel kapcsolatos információk együttes értékelése és hatékonyabb felhasználása valósulhasson meg. A bizottsággal az akkori kormányzat célja kettős volt. Az ország érdekeit esetlegesen fenyegető terrorcselekmény felderítésének segítése érdekében (1) a nemzetbiztonsági szolgálatok és a rendvédelmi szervek által műveleti, valamint partnerszolgálati együttműködés keretében szerzett, a terrorizmusra és terrorcselekményekre vonatkozó információk cseréje, összegzése, értékelése, valamint (2) válsághelyzetben a felderítő, műveleti intézkedések összehangolása és a szükségesnek ítélt hatósági intézkedések kezdeményezése. Az utóbbi tevékenység már az eseménykezelés körébe tartozik, intraoperatív természetű, amellyel most nem foglalkozom. A bizottságot az NBH főigazgató-helyettese elnökölte, és munkája során hasznosíthatta az SZBKK adatbázisát, valamint az SZBKK a kölcsönös információcsere kialakításához állandó kapcsolattartó személyt delegált a bizottság mellé.[7] A bizottság hét állandó tagja[8] között felülreprezentáltak voltak a nemzetbiztonsági szolgálatok. A nemzetközi terrorizmust érintő hatáskörök megoszlása alapján túlnyomórészt részükről érkezhettek olyan releváns információk, amelyeket a bizottságban „ütköztetni" lehetett. A bizottsághoz saját erőforrásokat nem rendeltek, a logisztikai bázist az NBH biztosította.[9] Önálló értékelő-elemző kapacitások híján feltehetőleg az NBH szintetizálta az összegyűjtött információkat. A kormányzati tájékoztatás a polgári nemzetbiztonsági szolgálatok irányításában közreműködő politikai államtitkár felé valósult meg, rajta keresztül tájékoztatták a miniszterelnököt, a bizottság tagjait irányító minisztereket, a Nemzetbiztonsági Kabinet[10] vezetőjét, valamint az érintett minisztereket. Ezenfelül a bizottság szükség szerint, de legalább félévente beszámolt a tevékenységéről és az érintett szervekkel történő együttműködésről a Nemzetbiztonsági Kabinetnek.[11]

A bizottság felállítása racionális lépés volt, hiszen a koordináció mellett megteremtődött a terrorfelderítésre irányuló információk megosztásának intézményközi *(interagency)* platformja. Értékelő-elemző kapacitások híján ez egy olyan nyitott („üres") platform volt, amelyen keresztül a tagok az információikat „ütköztethették". A fúziós központok tevékenységének első lépése, az információk összegyűjtése, koncentrálása tudott a bizottság

7 A terrorfelderítés műveleti koordinációjáról és a Terrorellenes Koordinációs Bizottság létrehozásáról szóló 2239/2005. (X. 28.) Korm. határozat 2, 4.

8 Nemzetbiztonsági Hivatal, Információs Hivatal, Nemzetbiztonsági Szakszolgálat, Katonai Biztonsági Hivatal, Katonai Felderítő Hivatal, Országos Rendőr-főkapitányság, Határőrség.

9 2239/2005. (X. 28.) Korm. határozat 3.

10 A kormány Nemzetbiztonsági Kabinetet létesített a nemzetbiztonsággal kapcsolatos feladatainak összehangolására, az állam- és közbiztonság védelmével összefüggő döntéseinek előkészítésére, valamint e tárgykörökben a kormányzati intézkedést igénylő aktuális kérdések megvitatására és megoldásuk elősegítésére, amelyen állandó meghívottként vett részt a Miniszterelnöki Hivatal nemzetbiztonsági ügyekben illetékes politikai államtitkára. A Kormány kabinetjeiről szóló 1107/2002. (VI. 18.) Korm. határozat.

11 2239/2005. (X. 28.) Korm. határozat 6–7.

előtt megvalósulni, méghozzá az összes fontos entitás bevonásával, hiszen a nemzetközi terrorizmusra irányuló felderítést végző nemzetbiztonsági szolgálatok mellett integrálta azokat a rendvédelmi (Országos Rendőr-főkapitányság) és fegyveres szerveket (Határőrség), amelyektől érdemleges adatok beérkezését várhatták. Pozitívum, hogy a működése során kifejezetten a nemzetközi terrorizmusra összpontosítottak, és igazodva a fenyegetés komplex és stratégiai természetéhez, ahhoz nemzetbiztonsági irányból közelítettek, amelyet egyebek mellett az NBH központi szerepe is kifejezett. A nyitottság hátránya viszont, hogy speciális szaktudás, szakértői bázis és információs adatbank a bizottság bázisán nem tudott létrejönni. A bizottság segíthette a vertikális információáramlást is azáltal, hogy a politikai döntéshozó felé „bemeneti oldali csatlakozó", a műveleti és a politikai szint közötti interkonnektor volt. Ami a kormányzati tájékoztatást illeti, az elgondolás szerint a bizottságon keresztül meg tudott valósulni a politikai döntéshozó egyetlen csatornán keresztüli tájékoztatása *(single flow reporting)*. Ezzel szemben a működésével a rendszerszintű párhuzamosságok nem voltak kiküszöbölhetőek, legfeljebb azoknak az ellentmondásos értesüléseknek a továbbítása volt kiküszöbölhető, amelyeket a tagok a bizottság előtt megosztottak egymással. A bizottság közel sem lehetett alkalmas egy fúziós központ hiányából fakadó űr betöltésére, jóllehet nem is ez volt a célja.

A nemzetközi terrorizmusra irányuló kormányzati tájékoztatás 2010 és 2022 között

A kétezres évek második évtizedében a nemzetbiztonsági és a rendvédelmi szervek körében végrehajtott átalakítások alapjaiban rajzolták újra a nemzetközi terrorizmus elleni harc – ideértve a kormányzati tájékoztatás – hazai rendjét. A rendőrségi törvény (Rtv.) módosításával felállítottak egy önálló, terrorizmust elhárító szervet (Terrorelhárítási Központ, TEK), amelynek feladatként a belföldön tevékenykedő terrorszervezetek felderítését, az e szervezetek által elkövetni tervezett bűncselekményeknek, valamint annak a megakadályozását határozták meg, hogy az ország területéről bármilyen szervezet vagy magánszemély terrorszervezet működését elősegítse.[12] A terrorizmust elhárító szerv nyomozóhatósági jogkört nem gyakorolhatott, az Rtv. alapján végezhető rendészeti célú titkos információgyűjtésre volt jogosult, bírói engedélyhez kötött titkos információgyűjtést kizárólag bűnüldözési célból folytathatott. Jóllehet a jogalkotó a terrorizmust elhárító szerv megalapításának indokaként hivatkozott a terrorizmus nemzetközi megnyilvánulásai által támasztott egyre nagyobb kihívásokra, kezdetben mégis több körülmény szólt amellett, hogy az új szerv felderítési hatásköre a belföldi terrorizmussal kapcsolatos feladatokra korlátozódik. Ilyen körülmény volt, hogy a terrorizmust elhárító szerv nem nemzetbiztonsági szolgálat, hanem a „terrorizmus elleni nemzeti felderítő szervként"[13] végzi a tevékenységét, bűnüldözési célú felderítést folytathat, s végül, hogy a polgári hírszerzés szervének nemzetközi terrorizmusra vonatkozó hatásköreit nem veszi át (ez,

[12] Az egyes rendészeti tárgyú és az azokkal összefüggő törvények módosításáról szóló 2010. évi CXLVII. törvény 7/E. §.

[13] T/1426. számú törvényjavaslat egyes rendészeti tárgyú és az azokkal összefüggő törvények módosításáról részletes indokolása 60.

mint látni fogjuk, később is érintetlen maradt). Az Nbtv. és az Rtv. módosítása és a terrorizmust elhárító szerv feladatai ellátásának részletes szabályairól szóló kormányrendelet[14] a TEK-et széles körű, a nemzetközi terrorizmus felderítésére vonatkozó hatáskörökkel ruházta fel. A polgári elhárításért felelős nemzetbiztonsági szolgálattól a terrorizmust elhárító szervhez allokálták a külföldi hatalmak, szervezetek vagy személyek terrorcselekmény elkövetésére irányuló törekvéseinek a felderítésére és elhárítására irányuló feladatköröket, ahogyan az ellátásukhoz szükséges szűrő-kutató titkos információgyűjtő feladatot, amelyet – e feladat nemzetbiztonsági aspektusa miatt – a terrorizmust elhárító szerv az Nbtv. szabályait betartva kellett hogy végezzen.[15] Ezek alapján elviekben az sem volt kizárható, hogy a terrorizmust elhárító szerven belül idővel egy különös hatáskörű fúziós szerv formálódjon, hiszen a terrorfenyegetettségi helyzet elemzése, értékelése jellemzően az ilyen típusú szerveknél összpontosul. Ráadásul a terrorizmust elhárító szerv hatásköre kiterjedt a terrorcselekmények megelőzését és elhárítását végző szervek – kivéve a Katonai Nemzetbiztonsági Szolgálat és az IH tevékenységének – koordinálására, a külföldi terrorizmust elhárító szervekkel, külföldi és nemzetközi rendvédelmi szervekkel való együttműködésre, továbbá a TKB működésével kapcsolatos előkészítő, végrehajtó és adminisztrációs feladatokra.[16] A rendvédelmi szerv egyre inkább nemzetbiztonsági arculatot vett fel, hibrid formát kezdett ölteni, amely zavaros helyzetet teremtett, amiről korábban több tanulmány is született.[17]

A fenti változásokkal közel egy időben merült fel, hogy az SZBKK bázisán, annak gyengeségeit kiküszöbölendő, egy általános hatáskörű nemzetbiztonsági fúziós központ létesüljön. A tervezett új nemzetbiztonsági szolgálatnak (Nemzeti Információs és Bűnügyi Elemző Központ, NIBEK) a terrorizmust elhárító szerv az együttműködő szerve lett volna, de a NIBEK a terrorszervezetekkel és a terrorcselekményekkel kapcsolatos adatokat soron kívül továbbította volna a TEK felé, és már itt szintetizálták volna azokat, valamint itt történt volna a kormányzati tájékoztatás is. A NIBEK a javaslat szövege alapján pusztán „figyelemmel kíséri" a terrorszervezetek és a terrorista csoportok tevékenységét. A fúziós központok nemzetbiztonsági struktúrákon belül általában elfoglalt helyéből és szerepéből következik, hogy a nemzetbiztonsági relevanciájú információk feléjük „áramolnak". A tervezett szabályozás azt a képet vetítette előre, hogy a NIBEK az általános hatáskörű, míg a TEK a különös hatáskörű fúziós szerv szerepét töltheti be, amely konstelláció elősegíthette volna a nemzetbiztonsági és a rendvédelmi igazgatás közötti együttműködést. Innen nézve, a nemzetközi terrorizmus elleni harc mintegy eszköze lett volna a biztonsági architektúra szervei közötti kohézió növelésének. Végül a nemzetközi terrorizmusra irányuló kormányzati tájékoztatás szempontjából az sem elhanyagolható körülmény, hogy a NIBEK-kel dolgozó modell elképzelése szerint a nemzetbiztonsági szolgálatok, így a polgári hírszerzés szerve (IH) és a terrorizmust elhárító szerv egyaránt a polgári nemzetbiztonsági szolgálatokért felelős miniszter (ekkor belügyminiszter) felügyelete alá tartoztak volna.[18]

[14] A terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól szóló 295/2010. (XII. 22.) Korm. rendelet.

[15] Az egyes rendvédelmi tárgyú törvények módosításáról, valamint az azzal összefüggő további törvénymódosításokról szóló T/5004. számú törvényjavaslat részletes indokolása 60.

[16] T/5004. számú törvényjavaslat részletes indokolása 3. §.

[17] Szentgáli 2015; Kis-Benedek 2013.

[18] T/5004. számú törvényjavaslat részletes indokolása 59, 11, 12.

A nemzetközi terrorizmus elleni küzdelem csúcsszervévé előlépő TEK – a háta mögött a NIBEK nemzetbiztonsági támogatásával – elinflálta volna a TKB hozzáadott értékét. Vélhetőleg ez is szerepet játszhatott a TKB karakterének módosulásában. Amíg a bizottság genezisében eredetileg a műveleti koordináció mellett egyértelműen benne volt a felderítés fokozása érdekében a nemzetbiztonsági szolgálatok és a rendvédelmi szervek közötti, információfúzióra emlékeztető („csere, összegzés, értékelés") preoperatív feladatkör, addig egy 2015-ös – mai napig hatályos – kormányhatározat kizárólag a rendvédelmi szervekre szűkítette a tevékenységét.[19]

A NIBEK felállítása végül elmaradt. Helyette 2016-ban az SZBKK feladatait a terrorizmus elleni teendőkkel kibővítve és bizonyos mértékig megváltoztatva egy általános hatáskörű nemzetbiztonsági fúziós központként működő nemzetbiztonsági szolgálat vette át (Terrorelhárítási Információs és Bűnügyi Elemző Központ, TIBEK). A TIBEK-hez telepítették a nemzetközi terrorizmussal kapcsolatos terrorfelderítés és a kormányzati tájékoztatás kulcselemeit. A kormányzati tájékoztatás a TKB, a TIBEK és a TEK hármasa által a belügyminiszter felé valósulhatott meg. A preoperatív feladatok a TEK (terrorfelderítés) és a TIBEK (műveleti szintű elemzés-értékelés, részleges információfúzió) között oszlottak meg, a TKB pedig fokozatosan az eseménykezelés szerve lett. Kétségtelen, hogy a nemzetközi terrorizmusra irányuló kormányzati tájékoztatás hazai evolúciójában ez az időszak volt a leginkább mentes a hatásköri átfedésektől. Ezzel együtt sem beszélhetünk homogén és teljes körű kormányzati tájékoztatásról, hiszen ebben a struktúrában partvonalra szorulhattak a külföldi eredetű információk, amelyek megléte esszenciális a nemzetközi terrorizmus esetén. Ez azért történhetett, mert egyfelől a TIBEK – ahogyan erre egy korábbi tanulmányomban rámutattam – főleg jogi korlátok miatt nem fejlődhetett valódi, általános hatáskörű nemzetbiztonsági fúziós csúcsszervvé.[20] Másfelől, a polgári hírszerzés szerve (IH) nem a polgári nemzetbiztonsági szolgálatokért felelős miniszter (a belügyminiszter), hanem a polgári hírszerzési tevékenység irányításáért felelős miniszter (a külügyminiszter) felügyelete alá tartozott. Ehhez hozzájött még az is, hogy a nyílt forrású hírszerzést (Open-Source Intelligence, OSINT), amely kulcsösszetevője a nemzetközi terrorizmusra irányuló felderítésnek, strukturálisan nem emelték ki.

A nemzetközi terrorizmusra irányuló kormányzati tájékoztatás 2022 után

A 2022-ben megalakult új kormányzat a nemzetközi biztonsági helyzet romlása miatt átszervezéseket hajtott végre a nemzetbiztonságot érintő politikai döntéshozatalban és a nemzetbiztonsági igazgatásban.

Különös hatáskörű politikai döntéshozó fórumként a Nemzetbiztonsági Kabinet Védelmi Tanáccsá alakult. Egyebek mellett a Védelmi Tanács felelősségi körébe tartoznak a terrorizmus elleni küzdelemmel kapcsolatos politikai döntések. Az új Kormányban

[19] A terrorizmus elleni küzdelem feladatainak egységes végrehajtási rendjéről szóló 1824/2015. (XI. 19.) Korm. határozat 19.

[20] Márton 2023.

az összes polgári nemzetbiztonsági szolgálat felügyeletét ugyanaz a miniszter (Miniszterelnöki Kabinetirodát vezető miniszter) látja el, aki maga is tagja a Védelmi Tanácsnak.[21]

Az Nbtv. módosításával a TIBEK jogutódjaként létrejött Magyarország történetében az első valódi, a nemzetközi szakirodalomban jegyzett definícióknak maradéktalanul megfelelő általános hatáskörű nemzetbiztonsági fúziós központ (NIK). A NIK nemzetközi terrorizmussal kapcsolatos feladatai részeként figyelemmel kíséri és elemzi Magyarország terrorfenyegetettségi helyzetét, a terrorhelyzetre vonatkozó információkat, a Magyarország terrorveszélyeztetettségi helyzetét érintő tendenciákat, a terrorveszélyeztetettségi helyzetet érintő új jelenségekről elemzéseket, tanulmányokat készít. A terrorfenyegetettségi kérdésekkel kapcsolatos stratégiai döntések meghozatalának elősegítése céljából mások mellett kormányzati tájékoztató és döntéstámogató tevékenységet folytat, amelynek érdekében az együttműködő szervek számára információs igényeket határozhat meg, sőt Magyarország terrorhelyzetére vonatkozó információk értékelése alapján javaslatot tehet a terrorfenyegetettség szintjének meghatározására.[22] A NIK a nemzetbiztonsági szolgálatok felé kötelezően teljesítendő hírigényt adhat. A nemzetbiztonsági szolgálatok egyúttal külső hírigényt nem teljesíthetnek. A NIK együttműködő szervei[23] között vannak rendvédelmi szervek, így a terrorizmust elhárító szerv is.[24] A NIK együttműködő szervei egyébként – a Védelmi Igazgatási Hivatalt leszámítva – átfedésben megegyeznek a TKB állandó tagjaival.[25]

A terrorizmust elhárító szerv feladatai ellátásának részletes szabályairól szóló kormányrendelet értelmében a TEK feladata továbbra is elemezni és értékelni Magyarország terrorfenyegetettségének helyzetét, a terrorcselekmények megelőzése és elhárítása tekintetében szervező és koordinációs teendőket lát el, valamint lényegében működteti és elnököli a TKB-t. Olyan fontos nemzetközi együttműködési hálózatok tagja, mint például az ATLAS[26] vagy különböző európai uniós munkacsoportok[27] stb.

A TKB a Védelmi Tanácsnak a terrorveszéllyel, illetve terrorfenyegetettséggel kapcsolatos kormányzati feladatai koordinálásának hatékony teljesítése érdekében működik. A TKB továbbra is betölti az interkonnektor szerepét a műveleti és a politikai szint között azzal, hogy a terrorfenyegetettségről szóló beszámolóját 2022 után a Védelmi Tanács

21 A Kormány ügyrendjéről szóló 1352/2022. (VII. 21.) Korm. határozat 27.

22 1995. évi CXXV. törvény 8/A. §.

23 Belügyminisztérium, Budapest Főváros Kormányhivatala, Országos Rendőr-főkapitányság, Országos Katasztrófavédelmi Főigazgatóság, Büntetés-végrehajtás Országos Parancsnoksága, Országos Idegenrendészeti Főigazgatóság, Nemzeti Védelmi Szolgálat, Terrorelhárítási Központ, Nemzeti Adó- és Vámhivatal, Alkotmányvédelmi Hivatal, Információs Hivatal, Nemzetbiztonsági Szakszolgálat, Katonai Nemzetbiztonsági Szolgálat.

24 Együttműködő szervek (NIK) (2024), lásd: https://nik.gov.hu/egyuttmukodo-szervek

25 Alkotmányvédelmi Hivatal, Nemzetbiztonsági Szakszolgálat, Információs Hivatal, Katonai Nemzetbiztonsági Szolgálat, Terrorelhárítási Központ, Országos Rendőr-főkapitányság, Nemzeti Védelmi Szolgálat, Országos Katasztrófavédelmi Főigazgatóság, Nemzeti Adó- és Vámhivatal, Nemzeti Információs Központ, Országos Idegenrendészeti Főigazgatóság, Védelmi Igazgatási Hivatal.

26 Az ATLAS hálózat az uniós tagállamok és társult országok rendészeti különleges beavatkozási egységeiből áll. Lásd: www.europol.europa.eu/partners-collaboration/atlas-network

27 A Belügyminisztériumnak az Európai Unió intézményei és ügynökségei tagállami kormányzati részvétellel működő döntéshozó és döntés-előkészítő szerveiben a kormányzati álláspont kialakításával és az ezen intézmények és ügynökségek munkájában való részvétellel kapcsolatos eljárásra vonatkozó szabályzata kiadásáról szóló 10/2015. (VI. 8.) BM utasítás.

részére végzi. A TKB megőrizte rendvédelmi fókuszát, és bizonyos tekintetben megmaradt az eseménykezelés túlsúlya.

A nemzetközi terrorizmusra irányuló kormányzati tájékoztatás neuralgikus pontjai

A fenti történeti kitekintéssel az volt a célom, hogy az olvasó perspektivikusan ismerhesse meg a nemzetközi terrorizmusra irányuló kormányzati tájékoztatás rendjét és a részt vevő szerveket. Az alábbiakban a hatályos rendszer elméleti értékelését végzem, s ezen keresztül kísérletet teszek néhány dilemma bemutatására.

Elsőként a kormányzati tájékoztatáshoz kapcsolódó értékelő-elemző fázisban fennmaradt párhuzamosságokat emelném ki. A különböző forrásból származó információk összessége az általános hatáskörű nemzetbiztonsági fúziós központ (NIK) irányába „áramlik", amely a feldolgozást követően a kormányzati tájékoztatást végzi. Noha a terrorizmust elhárító szerv hatáskörébe szintén beletartozik a terrorfenyegetettség helyzetének elemzése és értékelése, a jogszabályok alapján közel sem világos, hogy ez a tevékenysége a nemzetközi terrorizmusra kiterjed-e. Amennyiben igen, akkor viszont ehhez csak korlátozott erőforrások állnak a rendelkezésére, mivel a külföldi információk megszerzéséhez nem rendelkezik a szükséges jogszabályi felhatalmazással, nem nemzetbiztonsági szolgálat, és nemzetbiztonsági célú titkos információgyűjtést nem folytathat. A hiányzó erőforrásokat a nemzetbiztonsági szolgálatoktól átadott információk pótolhatnák, azonban a szolgálatok (esetünkben leginkább az IH és a NIK) a jogszabály szövege szerint nem kötelesek előzetesen megosztani a nemzetközi terrorizmussal kapcsolatos információikat a terrorizmust elhárító szervvel. Az Nbtv. úgy fogalmaz, hogy a NIK „átadhatja" a releváns információkat a terrorizmust elhárító szerv részére.[28] A terrorizmust elhárító szerv pedig hírigényt nem adhat a nemzetbiztonsági szolgálatok felé.

Másodikként a TKB szerepét és a kormányzati tájékoztatásban való részvételét tekintve találhatók ellentmondásos pontok. Ami a TKB szerepét illeti, a hatályos modell felépítése, így a TKB TEK-hez rendelése (logisztikai bázis, elnöklés) arra utalnak, hogy a TKB inkább az eseménykezelés szerve, amelynek feladata a terrorfokozatok meghatározásában és a válsághelyzeti koordinációban merül ki. A TKB-ról szóló kormányhatározat szövege azonban ettől eltérő értelmezésre vezet. A kormányhatározat szerint:

> „A TKB feladata a rendvédelmi szervek által műveleti, valamint partnerszolgálati együttműködés keretében szerzett, *a terrorizmusra* és terrorcselekményekre – ideértve az Alaptörvényben rögzített jogállami berendezkedést, annak alapintézményeit és alapértékeit támadó és veszélyeztető hazai és külföldi tevékenységet – *vonatkozó információk cseréjé*vel, *összegzésé*vel, *értékelésé*vel, illetve válsághelyzetben a felderítő, műveleti intézkedések összehangolásával és a szükségesnek ítélt hatósági intézkedések kezdeményezésével kapcsolatos koordinációs tevékenység ellátása." *(Kiemelés tőlem – M. B.)*

[28] 1995. évi CXXV. törvény 8/A. § *ib) – ic).*

A jogszabályból, figyelemmel az „illetve válsághelyzetben…" distinkciót jelentő nyelvi fordulat használatára, a korábbi kettős feladatrendszer olvasható, azaz hogy a TKB az intraoperatív feladatain kívül, a válsághelyzet bekövetkezésétől függetlenül, azt megelőzően, általában végzi információk cseréjét, összegzését és értékelését. Ráadásul ezek olyan információk, amelyek a terrorizmusra és külföldi tevékenységre egyaránt vonatkozhatnak, ami lényegében nem más, mint a nemzetközi terrorizmus. A TKB információegyesítő és -megosztó természetét erősíti, hogy később a kormányhatározat explicit módon tesz említést a „TKB terrorveszéllyel, illetve a terrorfenyegetettséggel kapcsolatos elemző-értékelő tevékenységéről". Ha a TKB kizárólag egy eseménykezelési szerv, akkor a jogszabály megfogalmazása félreértésekre adhat okot. Ebben az esetben a kormányhatározat és a TKB feladatrendszerének pontosabb körülírása volna célszerű. Ha azonban elfogadjuk azt, hogy a TKB működése túlmutat az eseménykezelésen, akkor ez elvezet a következő ellentmondáshoz, konkrétan a TKB illeszkedéséhez a kormányzati tájékoztatás rendjébe. A kormányhatározat alapján a „TKB Magyarország terrorfenyegetettségéről, a hozzá eljuttatott információkról és az annak alapján megtett intézkedésekről a belügyminiszter útján tájékoztatja a Védelmi Tanácsot." Ezenfelül a TKB kifejezetten a Védelmi Tanács támogatása érdekében működik („biztosítja a Védelmi Tanács feladatellátását").[29] Ez alapján a TKB egyértelműen kormányzati tájékoztatást végez, elvégre a belügyminiszer mint politikai döntéshozó informálása már önmagában kimeríti a kormányzati tájékoztatás definícióját. Ezzel viszont párhuzamosságot idéz elő, hiszen nem egyértelmű, hogy a nemzetközi terrorizmussal kapcsolatos információ beérkezését és feldolgozását követően a kormányzati tájékoztatás a NIK vagy a TKB útján történik-e. Ahogy már korábban említettem, az Nbtv. a NIK hatáskörébe utalja a terrorfenyegetettségi helyzet elemzését, értékelését és a tájékoztatást, amely utóbbi bevégzetté válása a TKB szerepét, legalábbis ezen a téren, kiüresíti. Ez nem jelenti azt, hogy a TKB így nem bizonyulna hasznosnak, például a biztonsági architektúra többi résztvevőjének visszatájékoztatására és a potenciális eseménykezelésre való felkészülésre. Ha ez így van, akkor viszont a kormányhatározat megfogalmazása indokolatlanul zárja ki a nemzetbiztonsági szolgálatokat, mivel a nemzetközi terrorizmussal kapcsolatban pont ezeknek a szerepe igen hangsúlyos. Ha a TKB megalapítása körüli szándékot figyelembe vesszük, és az eseménykezelés mellett a kormányzati tájékoztatás és koordináció szerveként tekintünk rá, akkor nem világos, hogy a jogalkotó miért nem az általános hatáskörű nemzetbiztonsági fúziós központot középpontba helyezve működteti azt, vagy vezet be legalább tematikus elnöklést a működésében.

Harmadikként a kormányzati tájékoztatáshoz kapcsolódó koordinációs fázis – ami még nem eseménykezelés – területén azonosíthatók problémás részek. A terrorizmust elhárító szerv a feladatairól szóló kormányrendelet alapján „szervezi és koordinálja a terrorcselekmények megelőzését és elhárítását végző szervek – kivéve a Katonai Nemzetbiztonsági Szolgálat és az Információs Hivatal – tevékenységét".[30] Egyes szerzők már 2012-ben rámutattak arra az ellentmondásra, hogy noha a polgári hírszerzés szervének koordinációját a jogalkotó nem engedi a TEK-nek, a TKB üléseinek elnöklése körében az IH

[29] 1824/2015. (XI. 19.) Korm. határozat 19, 18, 23, 13.
[30] 295/2010. (XII. 22.) Korm. rendelet 3. §.

tevékenységének koordinálására *de facto* mégis sor kell hogy kerüljön.[31] Ezt a képet tovább árnyalja a NIK megjelenése, figyelemmel arra, hogy az Nbtv. a NIK-et széles körű koordinációs feladatkörrel ruházza fel. Ez kiterjed a NIK együttműködő szerveinek hatáskörébe utalt valamennyi információra, mi több, az országos jelentőségű, több szervet érintő, a Kormány, a Kormány nemzetbiztonsági döntéseit előkészítő szervek, valamint annak munkáját segítő munkacsoport által meghatározott ügyekre.[32] Kétségtelen, hogy a TKB kormányzati döntés-előkészítést támogató testület, ahogyan az is, hogy a nemzetközi terrorizmus elleni harc országos jelentőségű és több szervet érintő ügy. A koordinációt tekintve, a TKB hatásköre is kérdéseket vet fel. A TKB – amely, ahogyan erre korábban már utaltam, erőteljesen rendvédelmi fókuszú, és funkciója az eseménykezelés felé tolódott – jogosult a tagjai intézkedését kezdeményezni az adott szervet irányító, felügyelő vagy vezető miniszternél. Ha a késedelem jelentős nemzetbiztonsági (!) sérelemmel járhat, a TKB közvetlenül kezdeményezheti a tagságát képező szervek – köztük a nemzetbiztonsági szolgálatok – intézkedését, a szervet irányító, felügyelő vagy vezető miniszter egyidejű értesítése mellett.[33] Ennélfogva a nemzetközi terrorizmus viszonylatában az a sajátos helyzet állhat elő, hogy egy rendvédelmi szerv (TEK) – amely rendvédelmi szervnél a releváns információk összessége a közjogi helyzetéből adódóan nem állhat rendelkezésre, s amely rendvédelmi szerv a polgári hírszerzés szervének tevékenységét nem koordinálhatja – által elnökölt testület mérlegeli a nemzetbiztonsági sérelem bekövetkezésének a lehetőségét, majd ha ezt megállapítja, akkor intézkedésre hívhatja fel többek között az IH-t és a NIK-et is.

A nemzetközi terrorizmusra irányuló integrált kormányzati tájékoztatás erősítésének lehetőségei

A nemzetközi terrorizmus jelentette fenyegetés felderítéséhez Magyarország biztonságpolitikai sajátosságaira figyelemmel – (1) más uniós tagállamokhoz képest relatíve alacsony az ország területén huzamos időtartamban tartózkodó harmadik országbeli állampolgárok száma, (2) az ország migrációs tranzitútvonalon fekszik, (3) a nyugat-balkáni és keleti irányból uniós külső határszakasszal rendelkezik, (4) hangsúlyos a partnerszolgálatokkal folytatott együttműködés melletti érdek stb. – kimagasló arányban szükséges a külföldi eredetű információk megszerzése, amely az Nbtv. alapján folytatott nemzetbiztonsági eszközök felhasználásával és nyílt forrású hírszerzéssel valósulhat meg. A nemzeti ellenálló képesség nem érhető el anélkül, hogy a nemzetközi terrorizmus elleni feladatok a fenyegetettség trendjeihez rugalmasan alkalmazkodnának. Némileg eltér a tárgytól, de talán itt van helye közbevetésemnek, ami szerint érdemes volna mérlegelni az alapvető célkijelölő dokumentumok hierarchiájában a Nemzeti Biztonsági Stratégia alatt elhelyezkedő Nemzeti Terrorellenes Stratégia kidolgozását, amelynek sarokpontját a nemzetközi terrorizmus elleni nemzeti védekezési képesség hosszú távú fenntartása képezhetné.

31 Hetesy 2011.
32 1995. évi CXXV. törvény 8/A.
33 1824/2015. (XI. 19.) Korm. határozat 22.

Az előző pontban részleteztem néhány olyan körülményt, amelyek magukban hordozzák a kockázatát a nemzetközi terrorizmusra irányuló kormányzati tájékoztatás eredményességének kedvezőtlen irányú befolyásolásának. Ezek után az a kérdés merül fel, hogy milyen korrekciós eszközök és módszerek állnak a rendelkezésünkre a fennmaradó hibák kiküszöbölésére. A legegyszerűbb megoldást a kodifikációs eszközök jelenthetik. A hivatkozott jogszabályok pontosítása, finomítása, nagyobb fokú egymáshoz illesztése, netán az érintett szervek feladat- és hatáskörének megváltoztatása a felvetett párhuzamok nagy részére megoldást jelentene. Mégis úgy vélem, hogy az érintett szervek jogköreinek megnyirbálása és áttelepítése drasztikus lépés, amely rövid távon lehet, hogy célravezető eredményekkel kecsegtet, de hosszú távon újabb nehézségeket vethet fel, például kizárhatja a korábban szerzett intézményi tudást és tapasztalatot, intézményközi versengést generálhat stb. Úgy vélem, hogy ezért érdemes jóval szofisztikáltabb rendezési módok után nézni, amire meglátásom szerint van lehetőség. Ehhez a külföldi jó gyakorlat áttekintése, a magyar viszonyokra történő adaptálása hasznosnak bizonyulhat. A következő néhány bekezdésben erre teszek kísérletet.

A jelen tanulmányban vázolt helyzet nagyon hasonlít ahhoz, amellyel a 2001. szeptember 11-i terrortámadást követően az Amerikai Egyesült Államok döntéshozói szembesültek. A szakmai viták eredőjeként határozták el a fúziós központok felállítását, köztük egy önálló, különös hatáskörű fúziós szervét, a nemzetközi terrorizmusra irányuló információk integrált elemzése, értékelése, a koordinált információmegosztás, az eseménykezelés és a politikai döntéshozót támogató stratégiai tervezés végrehajtása érdekében. A 2004-ben létrejött National Counterterrorism Center (NCTC) hatáskörei később aztán tovább bővültek, míg mára már tekintélyes adatbázist vezet különböző terroristákról, elemzéseket készít és stratégiai műveleti tervezést végez.[34] Az NCTC – önmeghatározása szerint – vezető szerepet tölt be azért, hogy a politikai döntéshozó megértse a terrorizmus jelentette fenyegetést, és arra megfelelően tudjon reagálni. Ennek érdekében intézményközi megbeszéléseket hív össze és vezet, amelyeken a terrorszervezetekről, azok képességeiről, terveiről, szándékairól és az ország érdekeire jelentett veszélyekről egyeztetnek a releváns állami szervek bevonásával. Továbbá olyan intézményközi csoportokat hív össze, vezet és támogat, amelyeken a terrorizmust elemző kapacitások hatékony és eredményes elosztását határozhatják meg és segíthetik elő, beleértve a megjelenő redundanciák kezelését. Integrált és az intézmények között koordinált elemzéseket állít össze a terrorizmus tárgyában, szükség esetén figyelmeztetéseket bocsát ki. A terrorizmussal kapcsolatos, világszerte történt események feldolgozására közös helyzetértékelési központot működtet. A tevékenysége eredményeként keletkező szintetizált információkat különböző terjesztési mechanizmusokon keresztül visszatájékoztatás céljából megosztja. A jogszabályokkal összhangban álló feladatok elvégzésére kérheti fel az érintett szerveket a stratégiai műveleti terveknek megfelelően.[35] Az előbbieken túl az NCTC még számos feladatot ellát, ha azok valamilyen formában a nemzetközi terrorizmus elleni harchoz kapcsolódnak. Az NCTC-t létrehozó elnöki rendelet ugyanis kimondja, hogy a különös hatáskörű fúziós szerv aktivitása nem irányul a tisztán belföldi terrorizmus elleni harcra.[36]

[34] The National Counterterrorism Center, lásd: www.dni.gov/index.php/nctc-who-we-are/history
[35] The National Counterterrorism Center, lásd www.dni.gov/index.php/nctc-what-we-do/overview
[36] Bush 2004.

Az NCTC és a TKB – legalábbis utóbbinak eredeti formája – között erős hasonlóság figyelhető meg, a különbség pusztán annyi, hogy az NCTC a feladatai ellátásához saját erőforrásokkal rendelkezik. Az általam vázolt problémák és a külföldi jó gyakorlat mentén elképzelhetőnek tartanám egy önálló, különös hatáskörű fúziós szerv életre hívását. Szinte magától értetődő volna, hogy egy ilyen központot a már létező, általános hatáskörű nemzetbiztonsági fúziós központ hatáskörének NCTC mintájára történő bővítésével,[37] a NIK szervezetén belül állítsanak fel. Ugyanakkor amellett is több érv szól, hogy a különös hatáskörű fúziós szerv a terrorizmust elhárító szerven belül volna ideális, folytatva, vagy inkább beteljesítve a TEK létrejöttét követő fejlődési útját. A magam részéről egy harmadik utas megoldást ismertetek, amely a nemzetbiztonsági szolgálatok és a rendvédelmi szervek közötti egyensúly fenntartására törekszik, hogy így legyen képes az érintett szervek mindegyikének hozzáadott értékét a lehető legnagyobb mértékben kiaknázni. Álláspontom szerint a TKB az elmúlt időszakban bizonyította hasznosságát, viszont nem mindig találta a számára megfelelő helyet a biztonsági ökoszisztémában. Éppen ezért logikus lépés volna a TKB nemzetbiztonsági szolgálatok és rendvédelmi szervek „közé" és „fölé" emelése, valamint ehhez egy saját, állandó titkárság hozzárendelése, amely egyben a különös hatáskörű fúziós szerv szerepét is betölthetné.

Az alábbiakban amellett érvelek, hogy egy ilyen szervezeti autonómiájú, különös hatáskörű fúziós szerv, amelyet Terrorellenes Koordinációs Titkárságnak (TKT) neveztem el, milyen többleterőforrással járulhatna hozzá a kormányzati tájékoztatáshoz. Először, a TKB és a munkáját koordináló TKT valamely, a szűkebb értelemben vett biztonsági architektúrához tartozó szerveken kívül álló entitás – például a polgári nemzetbiztonsági szolgálatokért felelős miniszter – alá tagozódásával megszűnne a TKB nemzetbiztonsági szolgálatok és rendvédelmi szervek közötti „hányatatott sorsa".

Másodszor, egy önálló TKT és a hozzárendelt személyzet a bizottság összes tagjától beérkező információ szintetizálásával átfogó intézményközi helyzetképet rajzolhatna fel a nemzetközi terrorizmus jelentette fenyegetésről, integrálva a nemzetbiztonsági szolgálatoktól és a rendvédelmi szervektől érkező információkat. Ennek előnye volna, hogy a TKT saját, tapasztalt elemzői – például a minisztérium szervezetén belül helyet kapó TKT-hoz vezényelt állomány részeként – a bizottság tagjainak szervezeti érdekeitől elkülönülten működhetnének, a feladataik ellátása során nem volnának kiszolgáltatva a biztonsági architektúra egyetlen szervének sem, s így a nemzetbiztonsági és a rendvédelmi ökoszisztémák felett, mintegy önálló szűrőként fellépve, független értékelést lennének képesek nyújtani, amelyet kevésbé torzíthat a szervek közötti esetleges versengés vagy a szervezeti érdekek diktálta belső nyomás. A TKT a közös műveleti tervezés érdekében összegezhetné és dokumentálhatná a TKB-n meghatározott feladatokat, teendőket, amelyeket a politikai döntéshozó és a tagok felé is „köröztetne". A feladatszabásokat nyomon követhetné, figyelemmel kísérné a bizottság javaslatainak végrehajtását és a tagok felé visszajelzést adhatna a feladatok teljesítésének aktuális állapotáról. A politikai döntéshozó felől érkező utasítások a TKT-n keresztül kerülhetnének a bizottság elé.

Harmadszor, a TKT képes volna arra, hogy láthatóbbá tegye a nemzetközi terrorizmus jelentette fenyegetést és az ellene folytatott nemzeti küzdelmet. Ez egyfelől magában

[37] Az NCTC az Office of the Director of National Intelligence (ODNI) részeként jött létre. Az ODNI az Amerikai Egyesült Államok általános hatáskörű nemzetbiztonsági fúziós központja.

foglalhatná a visszatájékoztatás strukturálását a bizottság tagjai és az egyéb érintett szervek felé, ennek keretei között például a TKB elé kerülő információk összesítéséről háttéranyagok, tájékoztatók készítését, a TKB emlékeztetőinek, a feladatszabásoknak az intézményközi megosztását, önálló, belső biztonságos intranet felület üzemeltetését és tartalommal feltöltését stb. (belső láthatóvá tétel). Másfelől jelenthetné a bizottság – nyilvánosságra hozható – munkájának kommunikációját a lakosság felé, például időszakos nemzetközi terrorizmus helyzetértékelési jelentések közzétételével, nyilvános internetes honlap üzemeltetésével és tartalommal való feltöltésével, amelyen általános tájékoztató anyagok is megoszthatók a terrorfokozatokról stb. (külső láthatóvá tétel). A külső láthatóvá tétel a felkészítés, megelőzés és az eseménykezelés lakossági tájékoztatásának felülete irányában is fejleszthető volna, de ennek részletezése a jelen tanulmány témáját meghaladná.

Negyedszer, a TKT figyelemmel kísérhetné és a bizottság részére rendszeresen becsatornázhatná azokat az információkat, amelyeket a nemzetközi terrorizmus jelentette fenyegetést elemző-értékelő, különös hatáskörű fúziós szervek (például a már említett NCTC, vagy az Europol mellett működő ECTC[38] stb.) a működési gyakorlatukat vagy a konkrét terrorfenyegetettség értékelését tekintve tesznek közzé.

Összegzés

Az elmúlt időszakban a geopolitikai folyamatok alakulása Európa-szerte növelte a nemzetközi terrorizmusból fakadó kockázatot. A globális fenyegetéssel egyetlen ország sem lehet képes önállóan szembenézni. A transznacionális együttműködés fokozása nem egyenlő a fellépés teljes uniformizálásával. Az államok immunrendszerét jelentő biztonsági ökoszisztémáknak rugalmasan kell alkalmazkodniuk a nemzetközi terrorizmus megnyilvánulásának adott térségre jellemző formáihoz. A magyar helyzet sajátosságai arra hívják fel a figyelmet, hogy a fenyegetés kivédéséhez nemzetbiztonsági szemléletmód alkalmazása, a hírszerzési metódusok előtérbe helyezése és stabil partnerszolgálati együttműködés kiépítése indokolt. A biztonsági közösség szerveitől érkező információk lehető legteljesebb körű és integrált kezelése a politikai döntéshozatal sikeres támogatásának alapvető előfeltétele. A nemzetbiztonsági igazgatáson belül, az általános hatáskörű nemzetbiztonsági fúziós központ megalakítása érdemi előrelépés, amely centralizálta a hírigényforgalmat és egycsatornássá tette a tájékoztatást. A nemzetközi terrorizmus elleni harc a nemzetbiztonsági szolgálatok mellett a rendvédelmi szervek és egyéb állami szervek koordinálását teszi szükségessé, amelynek elsődleges fóruma a TKB. A nemzetközi terrorizmussal kapcsolatos koordinációban, a kormányzati tájékoztatás rendjében az érintett nemzetbiztonsági szolgálatok és a rendvédelmi szervek között hatásköri átfedések és párhuzamosságok keletkezhetnek. Ennek az egyik oka az, hogy a TKB helyzete nem kellően kiegyensúlyozott. A vonatkozó jogszabályok indokolatlanul a rendvédelmi szervek körére korlátozzák a TKB működését, és ellentmondásos rendelkezéseket tartalmaznak a koordináció terén, az általános hatáskörű nemzetbiztonsági fúziós központ kormányzati

[38] Az Europol szervezetében működő European Counter Terrorism Centre, lásd: www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc

tájékoztatási tevékenységét megkettőzhetik, ezáltal az információ széttöredezésének veszélye állhat fenn. A kormányzati tájékoztatási rend áramvonalasításának lehetséges útjai (kodifikáció, normaszöveg pontosítása, hatáskör átcsoportosítása) közül az egyik, egy különös hatáskörű, kifejezetten a nemzetközi terrorizmus okozta fenyegetés elemzését, értékelését, a TKB adminisztratív működtetését, valamint belső (a TKB tagjai felé) és külső (a lakosság felé) tájékoztatást végrehajtó fúziós szerv TKB bázisán történő létrehozása. A TKB kívül helyezése a szűkebb értelemben vett biztonsági struktúrán, például a polgári nemzetbiztonsági szolgálatokért felelős miniszter alá szervezésével szintén megfontolandó lépés lehet. A javasolt módosítások mérlegelése erősítheti a TKB preoperatív hatásköreit, és azt a partikuláris érdekektől független, ezáltal objektívebb elemző-értékelő testületté formálhatják, amely így a nemzetközi terrorizmusban az intézményközi információösszesítés, információmegosztás, koordináció és közös műveleti tervezés elsődleges fórumává válhat, nagyobb hangsúlyt helyezve a kihívás nemzetbiztonsági megközelítésére. Ilyen módon képessé válhat, hogy a jelenleginél átfogóbb támogatást nyújtson a politikai döntéshozó részére, és hatékonyabban hajtsa végre az intraoperatív eseménykezelés körébe eső feladatait.

Felhasznált irodalom

A Belügyminisztériumnak az Európai Unió intézményei és ügynökségei tagállami kormányzati részvétellel működő döntéshozó és döntés-előkészítő szerveiben a kormányzati álláspont kialakításával és az ezen intézmények és ügynökségek munkájában való részvétellel kapcsolatos eljárásra vonatkozó szabályzata kiadásáról szóló 10/2015. (VI. 8.) BM utasítás

Europol (2023): *A terrorizmus Európai Unión belüli helyzetéről és tendenciáiról szóló jelentés (TE-SAT).* Luxembourg: Az Európai Unió Kiadóhivatala.

A Kormány kabinetjeiről szóló 1107/2002. (VI. 18.) Korm. határozat

A Kormány ügyrendjéről szóló 1352/2022. (VII. 21.) Korm. határozat

A terrorfelderítés műveleti koordinációjáról és a Terrorellenes Koordinációs Bizottság létrehozásáról szóló 2239/2005. (X. 28.) Korm. határozat

A terrorizmus elleni küzdelem feladatainak egységes végrehajtási rendjéről szóló 1824/2015. (XI. 19.) Korm. határozat

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

Az egyes rendészeti tárgyú és az azokkal összefüggő törvények módosításáról szóló 2010. évi CXLVII. törvény

Az egyes rendvédelmi tárgyú törvények módosításáról, valamint az azzal összefüggő további törvénymódosításokról szóló T/5004. számú törvényjavaslat részletes indokolása

Bush, George W. (2004): *Executive Order 13354 on National Counterterrorism Center (27 August 2004). Section 3/a.* The White House. Online: www.dni.gov/files/NCTC/documents/RelatedContent_documents/eo13354.pdf

Hetesy Zsolt (2011): *A titkos felderítés.* Doktori disszertáció. Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola.

Kis-Benedek József (2013): A nemzetbiztonsági szolgálatok együttműködése. *Hadtudomány,* 23(1–2), 100–114. Online: www.mhtt.eu/hadtudomany/2013/1_2/HT_2013_1-2_mhtt.pdf

Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Korm. határozat

Márton Balázs (2023): A NIBEK-től a Nemzeti Információs Központig. Nemzetbiztonsági fúziós központok Magyarországon. *Nemzetbiztonsági Szemle,* 11(1), 21–33. Online: https://doi.org/10.32561/nsz.2023.1.2

Szentgáli Gergely (2015): Csendben szolgálni. A magyar nemzetbiztonsági szektor helyzete és átalakítása 2010 és 2014 között – 2. rész. *Hadtudomány,* 25(3–4), 77–90. Online: https://doi.org/10.18530/BK.2015.4.90

T/1426. számú törvényjavaslat egyes rendészeti tárgyú és az azokkal összefüggő törvények módosításáról részletes indokolása

NEMZETBIZTONSÁGI SZEMLE
12. évfolyam (2024) 2. szám 55–80. | DOI: 10.32561/nsz.2024.2.4

Lendvai Tünde[1]

A Kínai Népköztársaság feltételezett kiberhírszerzési műveleteinek értékelése: eljárások és a nemzetközi hatások áttekintése

Assessment of Presumed Cyber-Intelligence Operations of the People's Republic of China: Overview of Procedures and International Impacts

A tanulmány kutatási célkitűzése, hogy áttekintést adjon a Kínai Népköztársaság kiberhírszerzési tevékenységének nemzetközi relációban megjelenő helyéről és szerepéről, eszközrendszeréről. A szekunder források feldolgozása kvalitatív módszerrel valósult meg, kiegészítve olyan esetpéldák elemzésével, amelyek jól szemléltetik az elmúlt 5–7 év során nyilvánosan attribútált, feltételezhetően kínai kibertéri hírszerző műveletek cél- és eszközrendszerét. Az Egyesült Államokat érő, 2015 után megindított műveleteket (a Marriott Szállodaláncot, az Equifax hitelminősítőt és az Anthem Biztosítót ért incidensek) gazdasági, technológiai és politikai előnyök megszerzése motiválta. A megszerzett adatok felhasználhatók adatigényes technológiák és speciális IoT-eszközök fejlesztési és piackutatási szakaszában. Az incidensek kapcsán az USA nyomozó szervei rávilágítottak egy átfogó kínai kiberhírszerzési kampány eshetőségére. A nemzetbiztonsági kockázatok közt megjelenik a piaci szereplőktől megszerzett adatbázisok kombinálhatósága a szövetségi alkalmazottak személyi ügyeit kezelő hivataltól 2015-ig megszerzett (OPM-adatlopás) érzékeny információkkal és személyes adatokkal.

Kulcsszavak: *Kínai Népköztársaság, KNK, kiberhírszerzés, kiberműveletek, kiberkémkedés*

The research aims to provide an overview of the People's Republic of China's presumed cyber intelligence activities in the international context. It utilizes qualitative analysis of secondary sources and publicly attributed case studies from the past 5-7 years. Operations launched in the US after 2015, such as the Marriott, Equifax,

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola Kiberbiztonsági Kutatóintézet, e-mail: lendvai.tunde@uni-nke.hu

and Anthem incidents, were driven by economic, technological, and political motives. The acquired data might be used for developing data-driven technologies (AI, ML) and IoT tools. US investigative agencies suspect a broader Chinese cyber intelligence campaign, posing national security risks by combining acquired databases with sensitive information and personal data obtained from the Office of Personnel Management of federal employees (OPM data theft) until 2015.

Keywords: *People's Republic of China, PRC, cyber intelligence, cyber operations, cyber espionage*

Bevezetés

Hadtudományi szempontból vizsgálva, a nemzetközi érdekérvényesítés eszközeként kell értelmezni az állami és állam alatti kiberműveleti képességeket, ideértve a fejlett perzisztens fenyegetések[2] (APT vagy fejlett perzisztens fenyegetés) tevékenységét.[3] Ebből kiindulva, a Kínai Népköztársaságot (KNK vagy Kína) vizsgáló biztonság- és védelempolitikai, valamint az orientalisztikai kutatási területek már 2003-tól (az első felderített APT-kampánytól kezdve) vizsgálták az állami és állam alatti kiberegységekhez köthető kiberhírszerzési műveletek stratégiai célrendszerét, a pekingi vezetés globális hatalmi ambíciói kontextusában.[4] Kína kibertéri aktivitása 2012–2015 között ismét jelentős sajtópublicitást kapott (különösen a Snowden-ügy tapasztalatai kapcsán), az időszakban feltárt hírszerzési célú APT-kampányok miatt (lásd az USA köztisztviselőinek személyügyi hivatalát és az Anthem Biztosítót ért incidensek), majd 2017-ben a kínai Nemzetbiztonsági Törvény módosításának okán.[5] Ezen előzmények mellett, 2019-től tovább nőtt a Kínához kapcsolódó (kiber) fenyegetés-percepció a Huawei vállalat szoftverének és egyéb termékeinek integritását és bizalmasságát kétségbe vonó incidensek és a rájuk reflektáló kiberdiplomáciai események

[2] Az *Advanced persistent threat* (APT) jelen kontextusban állami háttértámogatással működő kiberbűnözői csoport. Az APT olyan kibertámadási modell, amelyben a támadó csoport vagy kiberbűnözők rendkívül komplex eljárásokat és fejlett támadó eszközöket alkalmaznak, továbbá hosszú időn keresztül képesek észrevétlenek maradni a célzott hálózatokban, hogy érzékeny információkat szerezzenek meg. Az APT-csoportoknak az ilyen műveletek kivitelezéséhez előzetesen – akár humánalapú technikákat alkalmazva, mint a *social engineering* vagy HUMINT – komoly figyelmet kell fordítaniuk az áldozatok folyamatos megfigyelésére a megfelelő támadási pont meghatározásához (pl. célzott adathalász-támadás kivitelezése), és rendkívül sok erőforrásra a hosszú távú hálózati jelenlét fenntartása érdekében. Ez utóbbi jelentheti a költségek időarányos megtérülését, nehezen hozzáférhető *zero-day* sérülékenységek vagy beszállítói láncok felhasználását és a rendkívül mély szakértelem rendelkezésre állását kormányzati, katonai vagy ipari titkok megszerzése érdekében. Ezen jellemzők és a célorientált feladat-megvalósítás okán feltételezhető, hogy az APT-csoportok tevékenységét állami támogatással hajtják végre. A támadók által alkalmazott TTP-k és célpontkiválasztás utal arra, hogy feltehetőleg mely nemzethez, országhoz köthető a támadás.

[3] Berzsenyi 2023: 19, 99–104, 111–113, 123–125.

[4] Lindsay–Cheung 2015: 58–60.

[5] A 2017-es kínai Nemzetbiztonsági Törvény *(National Intelligence Law)* célja a kínai állam biztonságának védelme és az országban működő szervezetek és egyének felett gyakorolt ellenőrzésének erősítése. A törvény számos kötelezettséget ír elő a szervezeteknek, többek között a kötelező állami adatszolgáltatást és az együttműködést a kínai állambiztonsági hatóságokkal, ami a technológiai multivállalatok üzleti titkainak bizalmasságát és piaci érdekeit is felülírhatja.

miatt.[6] Noha a kibervédelmi szakirodalom jelentős része a technológiai orientáltságú megközelítést alkalmazó CTI-jelentéseken (*cyber threat intelligence* – kiberfenyegetések elleni hírszerzés) alapszik, a kínai hátterű kiberbiztonsági incidenseket stratégiai szinten elemző, kvalitatív értékelést végző kutatócsoportok már 2015-ben és 2020-ban is felhívták a figyelmet publikációikban a kínai technológia- és tudástranszfer-hálózatok kockázataira, valamint a kínai technológiai óriáscégek adatgyűjtő tevékenységére.[7]

A kiberhírszerzés terminológiai és kiberbiztonsági háttere

Napjainkra a kínai hátterű IKT-technológiák és -szolgáltatások infrastrukturális, valamint fogyasztói beágyazottságából eredő fenyegetettségpercepció nem csupán tovább erősödött az euroatlanti szövetségi rendszer katonai és nemzetbiztonsági gondolkodásban, hanem bizonyos mértékben a biztonságiasítás jegyeit is magában hordozza, különösen az 5G-hálózat kiépítéséhez társuló biztonsági aggályok miatt (például hírszerzés- vagy szolgáltatáskiesésben rejlő zsarolási potenciál).[8] Ennek eredményeképp Kína és az euroatlanti szövetségi rendszer közt fennálló kiberdiplomáciai kapcsolatokat bizalmi krízishelyzet dominálja. Ez a jelenség különösen az Amerikai Egyesült Államok és az Egyesült Királyság kiberdiplomáciai kapcsolatait terheli meg, egyrészt a kölcsönösen alkalmazott szankciós politika miatt, amelyek IKT-termékeket és -vállalkozásokat vagy technológia- és tudástranszfer-együttműködéseket sújtanak.[9] Másrészt az utóbbi három évben az amerikai és brit kormányzat egyaránt aktívan alkalmazta a nyilvános attribúciót Kínával szemben, különösen az APT31 tevékenységére visszavezetett események miatt, amelyet közvetlenül a kínai Állambiztonsági Minisztérium állam alatti kiberegységei közé sorolnak.[10] Ennek kiemelendő példája az USA Igazságügyi Minisztériuma által 2024 márciusában nyilvánosságra hozott vádiratkivonat, amelyben a KNK hét állampolgárát vádolják számítógépes behatolásra és elektronikus csalásra irányuló összeesküvéssel, mert részt vehettek az APT31 egyes műveleteiben. A vádak szerint a célpontok között szerepeltek az USA mindkét nagy politikai pártjának kampányain dolgozó munkatársai, a 2018-as félidős választást és a 2020-as elnökválasztást megelőző időszakban. Továbbá érintettek voltak minisztériumi köztisztviselők, szenátorok és házastársaik, valamint amerikai vállalatok és kínai disszidensek is.[11] Az USA Pénzügyminisztériuma és brit tisztségviselők részéről ugyanezen események nyilvános attribúciójának egy másik megtorló formája volt egy kínai hátterű vállalat és két vállalkozó elleni bilaterális szankciók közös bejelentése 2024. március 24-én. London a Kínával kritikus törvényhozók elektronikus levelezési fiókjának feltörési kísérletével vádolja az APT31-ként azonosított csoportot, illetve egy másik

6 Kaska–Beckvard–Minárik 2019.
7 Lindsay–Cheung–Reveron 2015, Hannas–Tatlow 2020.
8 Friis–Lysne 2021.
9 Greig 2024.
10 Értsd: a nyilvános attribúció mint kiberdiplomáciai eszköz olyan eseteket takar, amelyek során az érintett („megtámadott") állam a sajtóban vagy diplomáciai fórumokat felhasználva teszi felelőssé az incidensért vagy kiberműveletért a feltételezett „támadó" államot. A nyilvános attribúció célja a hasonló tevékenység elrettentése, a „leleplezett" hírszerző tevékenység miatti megszégyenítés diplomáciai eszközként való alkalmazása által.
11 US Department of Justice 2024.

kínai hátterű kibertéri fenyegetést tesz felelőssé a brit választási bizottság (választásokat felügyelő szervezet) 2021–2022-es kompromittálásáért.[12] A kínai diplomaták Nagy-Britanniában és az Egyesült Államokban egyaránt alaptalannak minősítették a fenti vádakat.[13]

A brit és amerikai kormányokkal ellentétben, a kínai külpolitika általánosságban tartózkodik a nyilvános attribúció alkalmazásától. Kiberdiplomáciai ellenpólusként, Kínához hasonlóan – a nagyobb euroatlanti kiberhatalmak által ugyancsak gyakorta nevesített – Oroszország is ellenzi a nyilvános attribúció gyakorlatát, és Észak-Korea is a legritkább esetben kommentálja a vádakat. Kína szakpolitikai perspektíváját az alábbi okokra vezette vissza az SIIS *(Shanghai Institutes for International Studies)* és a CEIP *(Carnegie Endowment for International Peace)* amerikai–kínai kutatócsoportja:

1. Egyrészt az eljárás miatt fennáll a hírszerző források és módszerek kompromittálódása, amely révén a kibertámadók korábbi hibáikat javítva még nehezebben lesznek detektálhatók. Objektív bizonyítékok – önkéntes – bemutatásának hiányában pedig megkérdőjelezhető az attribúció hitelessége.
2. Külpolitikai szempontból a nyilvános attribúció diplomáciai feszültséget generál, így csökkentheti a felek rugalmasságát más bilaterális ügyek rendezésében. Alapvetően alkalmatlan politikai eszköz az elrettentésre, ám kedvezőtlenül hat a kereskedelemre és csökkenti a bizalmat az érintett piacok és gazdasági szereplők által használt infrastruktúra és előállított termékek integritásában. Ezen túlmenően fennáll az elítélt ország megtorlásának lehetősége is.
3. Belpolitikai tekintetben a gyakorlat szükségtelen mértékű fenyegetettségérzetet generálhat a társadalomban, amely egyfelől a támadók zavarkeltési és megfélemlítési célját segítheti elő, továbbá teret ad a populizmusnak és a biztonságiasításnak, ami kedvezőtlen biztonságpolitikai környezetet teremthet. Ezzel összefüggésben a társadalom olyan belpolitikai nyomást helyezhet a kormányzatra, amely erősebb megtorló intézkedéseket sürgetve eszkalálja a helyzetet. Emiatt Kína a nyilvánosságot mellőző háttérdiplomáciára helyezi a hangsúlyt az offenzív kibertéri aktivitás kezelésében.[14]

A fentiekben leírt kiberdiplomáciai helyzet hozadékaként, egyre mélyülő külpolitikai érdekellentét figyelhető meg a NATO-szövetségesek körében, aminek fő eredője a tagállamok eltérő mélységű digitális technológiai kooperációja a Kínai Népköztársasággal.[15] Különösen igaz ez Magyarország esetében is, ami a kutatási téma aktualitását adja. A hazai gazdasági és politikai elit – nem reprezentatív kutatásban részt vevő – prominens szereplői többségében üdvözlendőnek tartják a kínai tőkebefektetést és más gazdasági-technológiai együttműködési lehetőségeket.[16]A tanulmány kutatási célkitűzése, hogy áttekintést adjon a Kínai Népköztársaság kiberhírszerzési tevékenységének nemzetközi relációban megjelenő helyéről és szerepéről és stratégiai eszközrendszeréről.

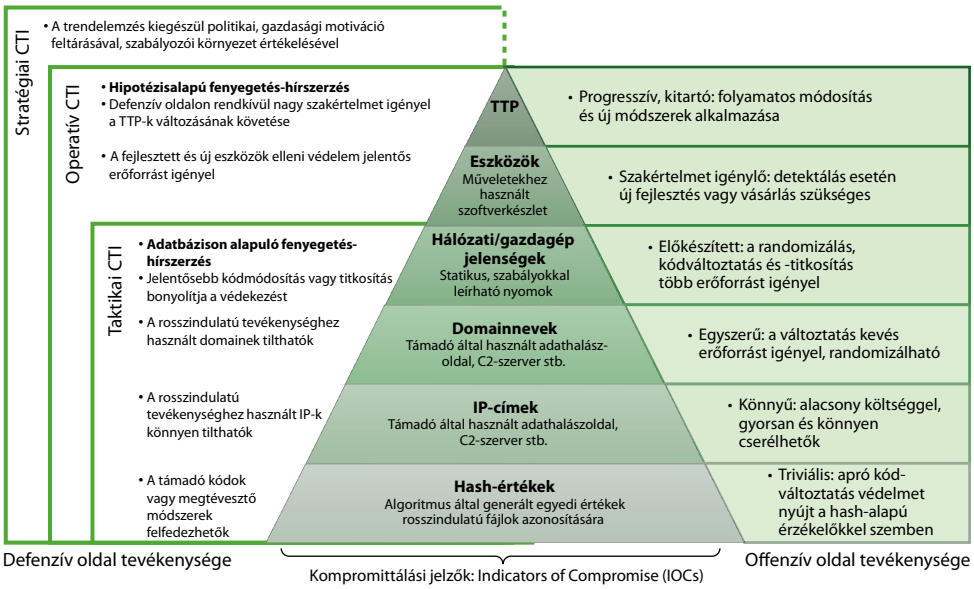
A nemzetbiztonsági tudományág egyik alapvetése, hogy minden nemzet kardinális érdeke a saját védelmét szolgáló hírszerzési információk megszerzése, valamint

12 Macaskill–Pearson 2024.
13 Pearson–Satter–Bing 2024.
14 Yang 2022.
15 Lima da Frota Araujo – Szunomár 2022.
16 Matura et al. 2022.

az ellenérdekelt hírszerzési tevékenység ellensúlyozása. A kibertér által lehetővé tett hírszerzési tevékenységet, a kiberhírszerzést (vagy CYBINT) a szakirodalom hírszerzési szakágként sorolja be, de összadatforrású tevékenységként jellemzi.[17] Ennek oka, hogy egy sikeres kiberműveletet (értsd: információszerző műveletet a kibertérben) ugyancsak megelőzhet más hírszerzési ágakba sorolt tevékenység, például HUMINT (emberi erőforrásokkal folytatott hírszerzés, a kiberbiztonsági szaknyelvben: social engineering, vagyis pszichológiai befolyásolás) vagy OSINT (nyílt forrású hírszerzés).[18] A kiberhírszerzési tevékenység feladatköre azonban kiterjed a kibertéri fenyegetettségek felderítésére is. A szakirodalom a felhasználás szintje szerint háromféle CTI-típust különít el:

1. *Strategic threat intelligence* (stratégiai szintű fenyegetettség-hírszerzés vagy -előrejelzés): A „stratégiai hírszerzés" átfogó jellegű, magas szintű áttekintést nyújt a fenyegetési környezetről *(threat landscape)* egy ország vagy gazdasági ágazat számára. Az incidensek historikus adatait és trendjeit kiegészítő kontextuális adatok, amelyek például a szabályozási környezetet, politikai vagy gazdasági motivációs hátteret jellemzik, egyaránt fontosak a stratégiai hírszerzés szempontjából. Az ilyen metodika mentén elemzett fenyegetésekre vonatkozó technikai attribútumok rávilágítanak a védelmi és detekciós képességek hiányosságai mellett a lehetséges jövőbeli stratégiai célpontokra, támadó eljárásokra.
2. *Operational threat intelligence* (operatív vagy műveleti szintű fenyegetettség-hírszerzés vagy -előrejelzés): Az operatív hírszerzés azokra a konkrét támadástípusokra vagy ágazatspecifikus fenyegetésekre összpontosít, amelyek potenciálisan veszélyt jelentenek az adott szervezetre. Kockázatorientáltan (például bekövetkezés valószínűsége, lehetséges támadási vektorok) kiemeli, hogy az incidenskezelő csapatnak hogyan javasolt priorizálnia egy adott incidenstípust vagy támadási kísérletet, és mely lépések lennének a leghatékonyabbak annak megakadályozásához vagy az informatikai rendszeren belüli terjedés korlátozásához. Az operatív fenyegetés-hírszerzés átfogóbb betekintést nyújt az offenzív aktorok képességeibe és támadásaik időzítésébe, így alkalmazva a stratégiai szintű hírszerzést egy valós élethelyzetre.
3. *Tactical threat intelligence* (taktikai szintű fenyegetettség-hírszerzés vagy -előrejelzés): A taktikai hírszerzés olyan technikai információk megszerzésére összpontosít egy incidens során, hogy támogassa a kiberbiztonsági szakembereket a védelmi intézkedések hatékonyabb koordinálásában, incidens reagálási tervek *(incident response plan)* felépítésében és a védelem rendszerének megtervezésében és konfigurálásában. Ennek értelmében a taktikai szintű fenyegetettség-előrejelzés az egyes incidensek lefolyásának (*cyber kill chain,* kiberbiztonsági modell) – akár valós időben történő – elemzése által szolgáltat információt az egyes támadó aktorok (például APT-k) által alkalmazott taktikai lépésekről, technikákról és eljárásokról (*tactics, techniques and procedures,* TTP) vagy például a támadók tevékenységének észleléséhez szükséges technikai indikátorokról, a kompromittálási jelzőkről (*indicators of compromise,* IOCs).[19]

[17] Szeleczki 2022.
[18] Dobák–Tóth 2021.
[19] Flashpoint Team 2022.



1. ábra: A kiberfenyegetettség-hírszerzés felhasználási szintjei mentén tagolt információforrások sematikus ábrája
Forrás: a szerző szerkesztése Bianco *2013 és* Berzsenyi *2023: 193 alapján*

Az 1. ábra mutatja be a David Bianco kiberbiztonsági és CTI-szakértő által megalkotott „fájdalompiramis" (*Pyramid of Pain,* PoP) nevű fenyegetésmodellt, amelyen az látható, hogy az egyes szinteken megjelenő technikák megváltoztatása mekkora nehézséget okoz a támadónak. Az offenzív tevékenység indikátor-központú skálázása a piramis teteje felé haladva vizualizálja, hogy milyen lehetőségek nyílnak ezen támadó technikák beazonosítására (adatbázison alapuló *[intel based hunting]* és hipotézis alapján *[hypothesis hunting]*), és milyen hatékonysággal csökkenthetők a támadások, amennyiben a védelmi rendszerekbe (például: SIEM, SOAR) becsatornázott riasztásokat és monitorozásból származó adatokat a specifikus IOCs-indikátorok szerint definiáljuk. A modell szemlélteti, hogy a támadó IP-címének blokkolása önmagában nem elegendő egy támadó aktor elrettentésére, azonban a támadó egyedi taktikáinak, technikáinak és eljárásainak (TTPs) célzása az IOCs-eken keresztül lényegesen akadályozhatja a kiberművelet sikeres végrehajtását, miközben az üzemeltetett védelmi megoldások naplófájljaiból a továbbiakban predikcióra (az ábrán *hypothesis hunting*) is felhasználható információ nyerhető ki. (Bianco modelljének elnevezése tehát a támadó aktor erőforrás-veszteségére utal, amely technikák és eszközök egy sikertelen támadási kísérlet esetén a védelmi rendszerek továbbfejlesztését szolgálják.)[20]

A kiberbiztonsági események és incidensek kezelését támogató CTI-rendszerek (értsd: CTI-platform-szolgáltatás) hatékony működésének alapfeltétele a becsatornázható információk minőségétől és pontosságától függ, legyenek azok akár ember, akár gép által olvashatók (adattáralapú). Emiatt a Kínához köthető APT-tevékenység elleni védekezéshez

[20] Bianco 2013.

elengedhetetlen a magán- és közszféra kooperációja az incidensek jelentésében, valamint a kiberbiztonsági szakmai közösség együttműködése a riportok egységes szempontrendszerek mentén történő publikálásában. A közös szabványok és módszertanok (például: MITRE ATT&CK-féle metodológia alkalmazása) lehetővé teszik az elemzések összehasonlítását, a védelmi megoldások hatékonyságának növelését, különösen a fals pozitív riasztások kiszűrése és a támadók felismerése tekintetében. Az új technológiák fejlődése (például AI, ML, IoT) lehetővé teszi a CTI-rendszerek hatékonyabbá tételét, ugyanakkor új kihívásokat is jelenthet a támadási felületek bővülése és az adatok mennyiségének növekedése miatt, különösen az ipari irányítási rendszerek esetén.[21]

Módszertan

A kutatás stratégiája deduktív megközelítést és kvalitatív értékelést alkalmaz, kiegészítve olyan esetpéldák feldolgozásával, amelyek jól szemléltetik az elmúlt 5–7 év során feltárt kínai kibertéri hírszerző műveletek cél- és eszközrendszerét. A kutatásnak módszertani szempontból két limitációja van. Az első, hogy a feltételezhetően állami támogatással megvalósult kiberműveleteket, így különösen az APT-k tevékenységét, az erőforrás-ráfordítás, anyagi haszonszerzés és a megszerzett információ hasznosíthatóságának arányából adódóan lehet kvalitatív módszerrel beazonosítani az esetekről készült technikai jelentések mellett, ezért a források megbízhatósága vitatható. A második, hogy az esetpéldák elemzése és a kínai kibertéri hírszerző tevékenységről nyilvánosan elérhető szakirodalom feldolgozása szekunder adatgyűjtési módszerrel valósult meg.

Az esetpéldák időtartam szerinti lehatárolását az offenzív kibereszközkészlet és -technikák folyamatos fejlődése és elavulása indokolta. Emellett a feltárt esetek napjainkra értek a nyilvános attribúciót követő, hivatalos nyomozati és bírósági szakaszba, így arányaiban több magasabb hitelességű forrás áll rendelkezésre. Az incidensek kiválasztásban további szempont volt azok kiberdiplomáciai jelentősége, ami abból a politikai célból eredeztethető, hogy az incidenst elszenvedő állam (a vizsgált esetekben az USA) nyilvánosan attributál kínai hátterű APT-*tevékenységet (public cyber attribution)* amellett, hogy a digitális nyomokat elemző *(digital forensics)* állami szervezetek vagy kiberbiztonsági vállalatok kínai hátterű tevékenységre utaló jeleket is feltártak publikált jelentésükben. Emiatt a tanulmány a kiberbiztonsági szakterület terminológiáját[22] és szempontrendszerét alkalmazza a kiberhírszerzési esetek feladatmegvalósítás-szempontú vizsgálata során.

A hadtudomány a kibertér által lehetővé tett hírszerzési tevékenységek célrendszerét a társadalmi érdekek nemzetbiztonsági artikulációja mentén vizsgálja, valamint az aktuális biztonság- és védelempolitikai helyzet, illetve külpolitikai relevanciája szerint értékeli. Kína esetében mindezen indikátorok a Kínai Kommunista Párt (KKP) ázsiai geopolitikai célkitűzéseinek változásában, a nagyhatalmi ambíciók előtérbe kerülésében és a kettős felhasználású csúcstechnológiák fejlesztési versenyének kiéleződésében mutatkoznak meg,

[21] Gyebnár 2023.

[22] A szerző szinonimaként használja az incidens kifejezést az ún. kiberbiztonsági eseményekre (értsd: sikeres kompromittáció).

ezáltal új prioritásokat behozva az ország külföldi célpontokra irányuló kibertéri információszerző tevékenységébe. A tanulmányban mindezeket áttekintő jelleggel mutatom be.

A KNK feltételezett kiberhírszerzési tevékenységének áttekintése 2003–2015 között

Az első Kínához köthető APT-csoportot a Mandiant kiberbiztonsági vállalat kutatói azonosították 2003-ban. A kutatók által feltárt Titan Rain kódnévvel ellátott műveletek során az APT1-es csoport számos amerikai kormányzati és katonai intézménybe hatolt be, illetve ezek ellátási láncába tartozó védelmi és technológiai iparágba tartozó szervezetek rendszereit kompromittálták, több terabyte-nyi érzékeny adatot zsákmányolva. A Titan Rain kampány feltárása diplomáciai feszültséget okozott az Obama- és Hszi-kormányzatok között, ám egyúttal jelentős hatást gyakorolt az amerikai szervezeti rezilienciát erősítő intézkedések bevezetésére és a nemzetközi kiberbiztonsági együttműködések növelésére. Az Egyesült Államok csatlakozott a Nemzetközi Kibervédelmi Ügynökséghez (*International Cyber Security Protection Alliance,* ICSPA),[23] és megosztotta a Titan Rain kampányról szerzett technikai információkat más országokkal. A kínai ipari kémkedés és hírszerzés akkori volumenét és az ellene fellépő nemzetközi kooperáció kiterjedtségét jól szemlélteti, hogy 2006–2007 között az Egyesült Királyság, Németország és Új-Zéland kormányai közösen hozták nyilvánosságra számos Kínához köthető kiberművelet technikai részleteit.[24] A Kínához köthető kiberhírszerzési tevékenység újabb mérföldkövének tekinthető a 2010-es Aurora kódnevű támadás, amely a Google forráskódjának megszerzése érdekében több különböző egyesült államokbeli vállalat rendszereibe is bejutott. Emellett említésre méltó a McAfee kiberbiztonsági szolgáltató 2011-ben publikált elemzése, amelyben a kutatók által Shady RAT kampánynak elnevezett behatolásokról 5 évre visszamenően tártak fel Kínához köthető APT-tevékenységet. Az incidensjelentésben az USA kormányzati szervei, magáncégek, valamint olyan nemzetközi szervezetek kompromittálódását hozták nyilvánosságra, mint az ENSZ és a Nemzetközi Olimpiai Bizottság.[25]

Inkster, továbbá Lindsay és Cheung is kiemelik kutatásaikban, hogy a haditechnikai eszközök mérnöki visszafejtése révén szerzett információ sokkal könnyebben adaptálható a védelmi ipari gyártásban és kutatásban, mint a digitálisan megszerezhető információk, amelyek például kutatási részadatként vagy gyártási „jó gyakorlatként" hasznosíthatók a releváns szakértelem hiányában. Emellett a haderő- és támogató infrastruktúra modernizációjában a kettős felhasználású technológiák vagy egyéb modern technikák terén a kutatási és technológiatranszfer-hálózatok legális és illegális felhasználása arányaiban sokkal számottevőbb a kiberműveletekhez képest (például Kína japán gyorsvasútterveken alapuló vasúthálózat-fejlesztése.

[23] A brit kezdeményezésre létrejött ICSPA a kiberbűnözés elleni nemzetközi fellépést segíti, valamint az ipari és kormányzati információmegosztásokon alapuló együttműködés keretét biztosítja.
[24] Lindsay–Cheung 2015: 58.
[25] Lindsay–Cheung 2015: 59–60.

1. táblázat: Kínai fegyverrendszerek külföldi technológiai függősége (Chinese Weapons System Dependence on Foreign Technology)

Platform (Platform)	**Sector** (Haderő-nem)	**Country of origin** (A technológia származási országa)	**Foreign content** (Az alkalmazott külhoni technológia aránya és kritikussága)	**Illicitly obtained material** (Jogellenesen megszerzett technológia és komponensek)
J-11B	Légierő	Oroszország	5 – Magas	Igen: Su-27SK mérnöki visszafejtése (reverse engineering)
J-16	Légierő	Oroszország	5 – Magas	Igen: Su-30MK2 mérnöki visszafejtése (reverse engineering)
J-15	Légierő	Oroszország	5 – Magas	Igen: Su-33 mérnöki visszafejtése (reverse engineering)
Donghai-10 LACM	Űrerők	Oroszország, Ukrajna, USA, Németország, Franciaország	5 – Magas	Igen: rakétatechnológia mérnöki visszafejtése (reverse engineering)
LuyangII romboló, 052C típus	Hadi-tengerészet	Oroszország, Ukrajna, USA	2 – Alacsony-közepes	Igen: német motortechnológia
Changzheng hordozórakéta	Űrerők	USA, Oroszország	1 – Alacsony	Igen: USA motortechnológia

Forrás: Lindsay–Cheung 2015 alapján kivonat és magyar fordítás

A kutatók ezen érvelését támasztja alá az 1. táblázat (Lindsay és Cheung adatgyűjtésének kivonata), amely a haditechnikai és védelmi ipari célpontokra irányuló kiberhírszerzési műveletek (beleértve az APT-tevékenységet is) haderőfejlesztésben való szerepét helyezi kontextusba azáltal, hogy öt fokozatú „magas–alacsony" skálán értékeli a kínai haderő egyes fegyverrendszereinek feltételezhető kitettségét a „külhoni" technológiáknak. A kutatók által vizsgált adatsor kivonata a 2015-ig hadrendbe állított eszközpark azon fegyverrendszereit jeleníti meg, amelyek technológiája vagy egyes komponensei tekintetében illegális információszerzés merült fel (és az incidens ténye nyílt forrásként elérhető).[26] A haditechnika megszerzésére irányuló tevékenység egyik leghírhedtebb esetpéldáját egy 2009 áprilisában kiadott jelentés tárta fel, amelyben a kínai hátterű APT-csoport 2007–2008 között hozzáfért az F-35-ös vadászgép titkosítatlan tervezési adataihoz, a Lockheed Martin, a Northrop-Grumman és a BAE technológiai konzultációinak és értekezleteinek megfigyelésével. Érdekesség, hogy ezen adatlopás miatt a kínai hatóságok vállalták a felelősséget. A katonai célpontokat érintő kiberhírszerzési műveletek másik kiemelkedő esetpéldája az „RSA-incidens", ami ugyancsak a beszállítói láncot kompromittálta. A Nemzetbiztonsági Ügynökség (NSA) kiber szakágazatát irányító Keith Alexander tábornok 2013-ban tett jelentést az úgynevezett RSA biztonsági rendszer[27]

[26] Lindsay–Cheung 2015: 59–60 és Inkster 2015.

[27] Ezt a rendszert használják azok a cégek, amelyek a Pentagon minősített dokumentumaival dolgoznak.

SecureID tokenjeinek 2012-es kompromittálódásáról. Az esetet az amerikai hatóságok és kormányzat egy 2011-ig visszanyúló behatolás visszafejtésével kínai aktorokhoz attribuálta. Keith tábornok megerősítette, hogy a beszállítói láncot érő adatlopási incidens (supply chain attack) tette lehetővé 2011 májusában (két hónappal az RSA kompromittálódását követően) a Lockheed Martin rendszereinek feltörését.[28]

A Kínához köthető állam alatti hackercsoportok tevékenységének felderítésében 2013 jelentett újabb fordulópontot. Ekkor a Mandiant kiberbiztonsági szolgáltató publikálta egy Sanghajba telepített PLA-egység (UNIT 61398) lokációját, amelyet az amerikai hatóságok 2006-ig visszamenően több angol nyelvterületen elkövetett adatlopásért és hálózati behatolásért tettek felelőssé. Habár az épületet rövidesen kiürítették, az esetet követően magas szintű egyeztetések és kiberdiplomáciai kapcsolatfelvétel indult az USA és Kína között, aminek keretében elnöki találkozó (Obama és Hszi elnökök) volt, illetve felállítottak egy kiberbiztonsági munkacsoportot a USA–Kína Stratégiai és Gazdasági Dialógus *(U.S.–China Strategic and Economic Dialogue)* gondozásában.[29] A Washington–Peking bizalomépítési kezdeményezéseket vizsgáló Inkster elemzésében a Snowden-botrány kirobbanására vezeti vissza ezen kiberbiztonsági kezdeményezés megrekedését. A kutatás alapján az eset beigazolta a kínai fél fenyegetéspercepcióját, és egyúttal betekintést engedett a Five Eyes együttműködés mélységébe és kiterjedtségébe, megerősítve a kínai felet abban, hogy az USA technológiai fölényével visszaélve épít ki hegemóniát a kibertérben, miközben diplomáciai szempontból kettős mércét alkalmaz és helyez nyomást a pekingi vezetésre.[30]

A fentiekben is bemutatott incidensekből visszafejthető adatok alapján az amerikai és más nemzetek kormányzati szervei (például CSIRT, GovCert-ek) és kiberbiztonsági magáncégek[31] számos különböző cél- és eszközrendszerrel rendelkező kínai hátterű hackercsoport tevékenységét különítették el, amelyek közül napjainkra megközelítőleg 120–130 önálló tevékenységet (kampányt vagy incidenst) tartanak nyilván APT-fenyegetésként.[32] A legjelentősebb APT-csoportok közül számos esetben megfigyelhető volt a hírszerzési célú tevékenység,[33] amelyekre az alábbi lista mutat be tipizálható jellemzőket:

1. Az APT1 csoport (más néven *Comment Crew*) tevékenysége elsősorban katonai és politikai célpontokat érintett, többek között az USA, Japán és India kormányzati szerveit is célba vették. Az APT1 tevékenységét a Mandiant hozta

28 Greenberg 2021.
29 USA White House 2015.
30 Inkster 2015: 42–47.
31 Például FireEye, Kaspersky, Mandiant, McAfee, MITRE, CrowdStrike.
32 Electronic Transactions Development Agency 2022a és Malpedia adatbázisa, lásd: https://malpedia.caad.fkie.fraunhofer.de/actor/apt1
33 Említésre méltó, hogy az APT10 csoport (más néven Codoso) célpontjai a védelemi, a telekommunikációs és a légi közlekedési szektorba tartoznak. Az APT17 csoport (más néven DeputyDog) tevékenysége főként az Egyesült Államok és Dél-Korea kormányzati szerveit, valamint az amerikai hadsereget célozta meg. Az APT19 csoport (más néven Deep Panda) tevékenysége elsősorban a védelmi iparba és az energiaszektorba sorolható vállalatokat érintette, továbbá a gyógyszeripar szereplőit. Az APT27 csoport (más néven Emissary Panda) az ázsiai régióra összpontosított, fő célja katonai és politikai információk megszerzése volt a kormányszervek, a régió államainak nemzetbiztonsági szervei, valamint a védelmi ipari és telekommunikációs szolgáltatók kompromittálásával. Electronic Transactions Development Agency 2022a és 2022b.

összefüggésbe a Népi Felszabadító Hadsereg vezérkari hivatala (*General Staff Department*, GSD) 3. osztályának 61398-as[34] egységével.[35]

2. Az APT30 csoport (más néven *Elise*) tevékenysége legalább 2005 óta érinti az ASEAN-tagállamokat, aktivitását Tajvan, Malajzia, a Fülöp-szigetek, Vietnám és Kína területén is detektálták, utóbbi esetben kiberbűnözői csoportként. A Mandiant által gyűjtött CTI-információk alapján feltételezhető, hogy az APT30 tagjai felváltva dolgozhatnak egy kollaboratív környezetben, és koherens fejlesztői terv mentén módosítják és adaptálják az általuk használt malware-ek (SHIPSHAPE, SPACESHIP, FLASHFLOOD) forráskódját. A csoport fő célpontjai közt kormányzati szerveket, nemzetbiztonsági szerveket, védelmi ipari vállalatokat, tudományos kutatóintézeteket és energiaipari vállalatokat tartanak számon.[36] Érdekesség, hogy az APT30 tevékenységét átfedésbe helyezik a Naikon néven számontartott, fejlett perzisztens fenyegetéssel, amely aktort a rendelkezésre álló nyílt információk alapján ugyancsak kínai hátterű entitásként tartják számon, és a hadsereg 78020-as számú egységéhez kötik. Berzsenyi értekezésében így jellemzi a Naikon mandátumát: „vélhetően kiterjed a regionális számítógépes hálózati műveletekre, rádiójelfelderítésre és politikai elemzésre a Délkelet-Ázsiával határos nemzetek kapcsán, azon belül is azokra, amelyek az energiahordozókban gazdag Dél-kínai-tenger területi vitáiban érintettek."[37]
3. Az APT31 csoport hírszerző tevékenységéhez olyan applikációkban található sebezhetőségeket használt ki, mint például a Java és az Adobe Flash. A Mandiant adatbázisa alapján az APT31 kormányzati és nemzetközi pénzügyi intézményeket, űrkutatási és védelmi szervezeteket, valamint csúcstechnológiai, építőipari és mérnöki vállalatokat, távközlési, továbbá médiaipari és biztosítási szolgáltatókat is kompromittált. A célpontok ezen széles skálája alapján feltehető, hogy a hírszerzési tevékenység célja, hogy rövid és középtávon hasznosítható információt szerezzenek politikai, gazdasági és katonai előnyök megszerzéséhez.[38]
4. Az APT40 csoport jellemzően az Övezet és Út kezdeményezés *(Belt and Road Initiative)* szempontjából stratégiailag fontos országokat veszi célba. A csoport kampányai elsősorban olyan globális szervezetekre fókuszálnak, amelyek a védelmi ipari vagy mérnöki vertikumban tevékenykednek. Emellett a Mandiant adatai alapján legalább 2013-tól kezdve egyre jelentősebb mértékben érintettek vegyipari, kutató- és oktatási intézmények, kormányzati és technológiai szervezetek is, valamint hajózási és légi közlekedési célpontok. Állam alatti kiberegységként értelmezve az APT40 tevékenységét a stratégiai cél az lehet, hogy a megszerzett

---

34 A kínai haderőben számok jelölik az egységeket (military unit cover designator, MUCD). Lásd Berzsenyi 2023: 94.

35 Electronic Transactions Development Agency 2021.

36 Mandiant 2021. Advanced Persistent Threat (APT) groups & threat actors. APT31. (Bővebben lásd: www.mandiant.com/resources/insights/apt-groups) és Malpedia adatbázisa: Fkie, F. [n.d.]. APT30 [Threat Actor], bővebben lásd: https://malpedia.caad.fkie.fraunhofer.de/actor/apt30), Electronic Transactions Development Agency 2022a és 2022b.

37 Berzsenyi 2023: 94 és Malpedia adatbázisa: Fkie, F. [n.d.]. Naikon (Threat Actor), bővebben lásd: https://malpedia.caad.fkie.fraunhofer.de/actor/naikon

38 Malpedia adatbázisa: Fkie, F. [n.d.]. APT31 (Threat Actor), bővebben lásd: https://malpedia.caad.fkie.fraunhofer.de/actor/apt31

információ által Kína előnyösebb pozíciót szerezzen meg a globális tengeri kereskedelemben, és megkönnyítse a katonai és polgári célra is alkalmazható kikötők létesítését. Emellett a csoport műveletei a kínai haditengerészeti erők eszközparkjának modernizálására is irányulhatnak, vagy a polgári célú hajózást fejlesztő projektek technológiájának megszerzésére (járművek és felszerelés).[39]

5. Az APT41 kettős műveleti célrendszerben működő, kémkedésre és finanszírozásra összpontosító csoportként olyan iparágakat vesz célba, mint a szerencsejáték, az egészségügy, a csúcstechnológia, a felsőoktatás, a távközlés és az utazási szolgáltatások.[40] Az APT41 gyorsan alkalmazkodik a célpontok IT-környezetében bekövetkező változásokhoz és észlelésekhez, és gyakran az incidensre reagáló személyek tevékenységét követően néhány órán belül újrakompilálja (gépi nyelvre történő módosítás) a rosszindulatú programokat. Több alkalommal észlelték, hogy az APT41 a közelmúltban nyilvánosságra hozott sebezhetőségeket is felhasználta, gyakran napokon belül létrehozta a specifikus sérülékenységet kihasználó támadó programokat *(weaponizing)* és alkalmazta a kártevőket *(exploiting)*.[41]

A fejezetben ismertetett incidensek historikus adatai alapján megállapítható, hogy a kínai kiberműveletek fő célpontjai 2015-ig a védelmi ipar, a mérnöki és csúcstechnológiai kutatásokat végző piaci és állami szféra vertikumába tartoztak. Emögött feltehetően olyan stratégiai célok húzódhattak meg, mint a haderő transzformációja és az eszközpark modernizációja, különösen a haditengerészeti, stratégiai támogató erők (kiberképességek idesorolandók), űrerők és légierő képességfejlesztése miatt. A vizsgált időszakban, a külpolitikai célok megvalósítását támogató kiberhírszerzési kampányok olyan nemzetközi szervezeteket érintettek (például: ASEAN és részes államok), amelyek a pekingi vezetés akkori geopolitikai célkitűzéseinek érdekszférájába estek bele. Ilyen cél volt például Kína regionális nagyhatalmi pozíciójának globális hatalmi státuszba emelése, a dél-kínai-tengeri kereskedelem (és útvonalak) feletti kontroll bővítése által és erőkivetítési képesség növelésével. Továbbá az ország napjainkra elért kiberhatalmi státuszát megalapozó csúcstechnológiai ipar gyártó- és tervezőkapacitásának kiépítését támogató információk megszerzése (akár legális és illegális eszközökkel), illetve az IKT-technológiákat érintő tudásmenedzsment-hálózatok létrehozása.

A KNK kiberhírszerzési képességei a nemzetközi színtéren: feladatrendszer és támogató infrastruktúra elemzése

A kiberhírszerzési feladatokat végrehajtó szervezeti háttér feltérképezésében kiemelten fontos a kínai katonai és polgári szolgálatok tevékenységi körének behatárolása, a magánszférában meglévő képességek integrálhatóságának, az együttműködési területeknek

[39] Plan et al. 2024.
[40] MITRE Corporation [n.d.] Groups. és Mandiant [n.d.]. APT41 Chinese Cyber Threat Group 04. 29. Bővebben lásd: www.mandiant.com/resources/blog/apt41-dual-espionage-and-cyber-crime-operation
[41] Pennino–Bromiley 2022.

célirányos vizsgálata. Kína esetében mindezeket az ország külpolitikai célkitűzéseinek és a nemzetközi közösségben képviselt álláspontjának tükrében szükséges értelmezni.

A KNK kiberbiztonsági környezete: a hatalmi játszma a digitális világban

A legtöbb kiberbiztonsági trendkutatás hangsúlyozza, hogy globális viszonylatban a feltételezhetően Kína támogatását élvező aktorok egyre növekvő számú és szofisztikáltságú kiberműveletben érintettek, amelyek közt adatlopási kampányok, és újabban, noha nem számottevő arányban, a kritikus infrastruktúrák elleni támadások is fellelhetők. Ennek jelentősége, hogy a Kínához köthető APT-csoportok képességfejlődése lehetővé teszi, hogy a tevékenységük során kinyert információ mennyiségét és minőségét tekintve egyre komplexebb nemzetbiztonsági célokat szolgáljon ki. Továbbá az ipari kémkedés és technológiatranszfer-hálózatok jogszerűtlen kihasználása mellett – a fejlesztésre fordítandó költségek és humántőke-befektetés kihagyásával – piaci versenyelőnyhöz juttathatják a kínai vállalatokat, vagy hozzáférést biztosíthatnak katonai és kettős felhasználású technológiákhoz. Mindezek mellett, a kínai külügy képviselői évek óta sikeresen közvetítik a KKP azon álláspontját, miszerint az ország sokkal inkább tekinthető a kibertérből érkező fenyegetések áldozatának, semmint kiváltó szereplőjének. Az alábbiakban részletezett körülmények kontextusba helyezik Kína kiberbiztonsági környezetét és infrastruktúráját, feltárva annak okát, hogy mi teszi Kínát kelet-ázsiai viszonylatban az első számú, leggyakrabban támadott célponttá, és miként reprezentálható a világviszonylatban is kimagasló, kiberbűnözői tevékenységre visszavezethető anyagi károkat elszenvedő országként.[42]

A Kínai Népköztársaság kiterjedt digitális piaca és elektronikus államigazgatási ökoszisztémája széles támadási felületet eredményez, ezenfelül kritikus hálózati rendszere számos külföldi (főként az ország számára kihívást jelentő amerikai és vele szövetséges országok gyártóihoz köthető) kibervédelmi és egyéb technológiai megoldástól függ. További kihívásokat generál, hogy Kína kiberbiztonsági szabályozói környezete továbbra is elmaradottnak tekinthető az Európai Unió és az Egyesült Államok szabályozási rendszereihez képest. A pekingi vezetés ezen kockázatok kezelését prioritásként jelölte meg a 2019-es védelmi fehér könyvben, és folyamatosan támogatja a hazai digitális ipart és a védelmi megoldások fejlesztését.[43] Azonban a 2019–2021 között kiadott jogi normák ellenére is, az ország digitális infrastruktúrájának védelmét célzó jogi szabályozói környezet és adatvédelmi normarendszer még nem átfogó jellegű,[44] így teret ad a Kínai Kommunista Párt és a hazai technológiai óriásvállalatok közti konfliktusnak, ami az utóbbiak adatvesztési botrányai, valamint az adatgyűjtés és -felhasználás mértéke miatt szélesedett ki az elmúlt két-három évben.[45]

A kínai K+F+I-szektor módszeres állami támogatása az 5G, mesterséges intelligencia és kvantumszámítási technológia tekintetében ugyancsak piaci, nemzetbiztonsági és katonai megrendelők igényeit is kielégíti. Mindemellett Peking még nem tudott domináns státuszt elérni az ázsiai régióban (a pekingi külügy olvasatában biztonságot nyújtó

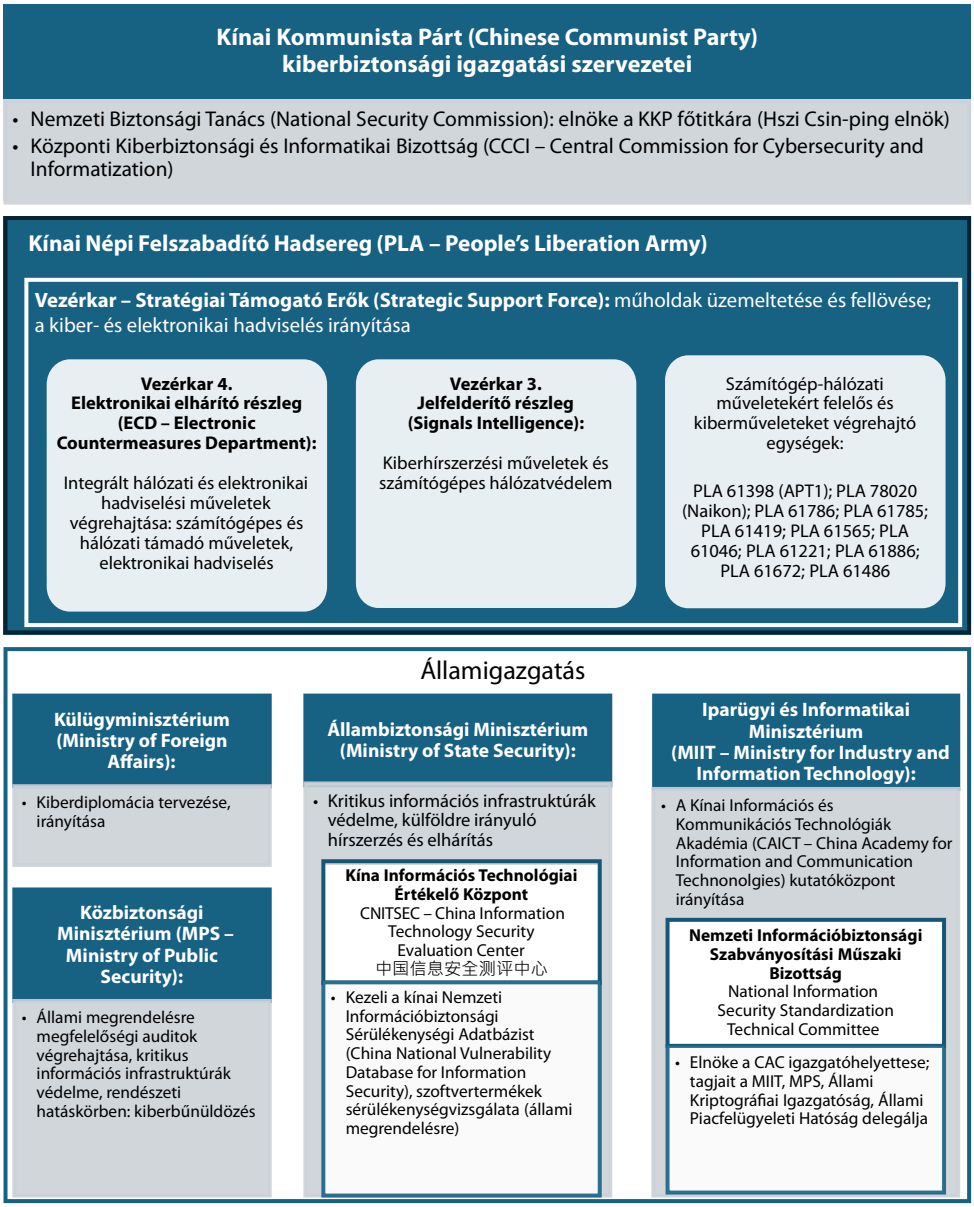
42 Lusthaus–Bruce–Phair 2020.
43 Segal 2020.
44 Kaszián 2021.
45 Mészáros 2021.

képességi szintet) az USA és szövetségesei kibertéri műveleti képességei és kiberbiztonsági technológiai iparával szemben. Egy ázsiai regionális konfliktus korai szakaszában az információs fölény megszerzése érdekében Peking képes lenne arra, hogy zavaró vagy pusztító célú kiberműveleteket indítson, különösen ellenfele parancsirányítási rendszerei, műholdas és kommunikációs hálózata ellen, amennyiben a katonai és a polgári hírszerzés vagy APT-csoportok tevékenysége révén megfelelően fel tud készülni.[46] A kínai katonai gondolkodásban egy olyan kibertéri művelet, amely hosszan tartó, jelentős zavarokat képes okozni a banki és telekommunikációs rendszerekben, stratégiai elrettentő hatással bírhat, mivel ezen szektoroktól való függőségük miatt képes lehet gátolni az USA vagy ázsiai regionális partnereinek beavatkozását egy fegyveres konfliktusba. A politikai és katonai vezetés azonban valószínűleg túl nagy kockázatnak tartja, hogy Kína legalább ugyanennyire sebezhető és kitett a fentiekhez hasonló megtorló vagy ellentámadásoknak, így konfliktus esetén katonai célpontok ellen indított műveletek vagy kiberfegyver alkalmazására kevesebb esélyt látnak a szakértők a kínai hálózati felderítés hatékonyságától függetlenül. Ezen ellentámadások miatti dilemma fenntartását célozza kibervédelmi fejlesztéseiben a kelet-ázsiai régió számos olyan állama – köztük Tajvan, Japán, Dél-Korea és Vietnám –, amelyek biztonságpolitikájában megjelenik a kínai kibertéri fenyegetettségpercepció. Az offenzív képességek növekedésével párhuzamosan várhatóan a következő években is jellemző lesz a kínai digitális piac terjeszkedése és a kritikus hálózatok sebezhetősége, amit a KKP fejlesztési támogatásokkal, valamint intézményesítési és szabályozási tevékenységgel igyekszik javítani. Az erősségek és gyengeségek ezen kombinációja azt eredményezi, hogy Kína elsősorban kiberkémkedési és dezinformációs kampányok általi fenyegetést jelent az ázsiai csendes-óceáni térségre.[47]

A kiberhírszerzési tevékenységet és információfeldolgozást támogató intézményi háttér

A Kínai Népköztársaság számos szervezete játszik fontos szerepet az ország digitális irányítási ökoszisztémájában. A 2. ábra szemlélteti azon államigazgatási szervezeteket, köztük a Népi Felszabadító Hadsereget (PLA), amelyek hatásköre kiterjed a digitális kormányzás valamely szegmensére (minisztériumok és háttérszerveik), vagy állami és pártfunkciójukon keresztül a kiberteret érintő igazgatási és szakpolitikai felelősségük van, ezáltal koordinálhatják a kiberhírszerzési feladatokat vagy az információk felhasználását. Kiemelendő, hogy valamennyi szervezet döntéshozatali struktúrájának a legfelsőbb szintjén a közvetlen elnöki hatalom és felügyelet jelenik meg. Sok más államhoz hasonlóan Kína esetében sem lehet egyértelműen szétválasztani a kiberhírszerzési és az elhárítási funkciókat, amelyek integráltan működnek az Állambiztonsági Minisztérium *(Ministry of Public Security)* szervezetében. Emiatt a felelősségiterület- és feladatkör-alapú szétválasztás mentén sorolták fel a külföldre irányuló hírszerzést végző szervezeteket. Az Állambiztonsági Minisztériumban két iroda végzi a külföldre irányuló hírszerzést: az első iroda felelősségébe tartozik a külföldre utazó diákok, akadémikusok és üzletemberek által megszerezhető technológiai

[46] Smith 2022.
[47] Segal 2020.



2. ábra: A Kínai Népköztársaság digitális és kibertéri igazgatásának legfontosabb intézményi szereplői
Forrás: a szerző szerkesztése Lee *2022 alapján*

és tudástranszfer, míg a második iroda a külföldi tartózkodási engedéllyel rendelkező állampolgárok által megvalósítható hírszerzést koordinálja. A kiberműveleti képességek a kínai haderőn belül a stratégiai támogató erők alá tartoznak. A katonai hírszerzési ágazat a PLA vezérkarán *(General Staff)* belül működik: a második részleg (2/PLA) koordinálja a védelmi attasék tevékenységét a nyilvános adatok megszerzése tekintetében, míg a harmadik úgynevezett Jelfelderítő részleg (3/PLA) felelős a SIGINT-tevékenységért, továbbá a számítógépes hálózatvédelemért és a kiberkémkedési tevékenység koordinálásáért. A negyedik úgynevezett Elektronikai elhárító részleg (4/PLA) hatáskörébe tartoznak a számítógépes és hálózati támadó műveletek. (A vezérkar negyedik részlegének offenzív kiberműveleti tevékenységét a kínai műveletszervezés integráltan kezeli az elektronikai hadviseléssel és Integrált Hálózati és Elektronikai Hadviselés [*Integrated Network Electronic Warfare,* INEW] tevékenységnek nevezi).[48]

Az információfeldolgozó és értékelő szervezetek közül két, közvetlenül a KKP-hoz köthető államigazgatási intézmény és egy közigazgatási testület emelhető ki. Az elmúlt évek politikai hatalomkoncentrációjának eredményeképpen a legszélesebb feladat- és hatáskört a Kibertér-igazgatási Hivatal (*Cyberspace Administration of China,* CAC) vonta magához, így Kína legfontosabb kiberbiztonsági hatósága, amely felelős az internetes tartalmak felügyeletéért és DNS-alapú szabályozásáért, a Kritikus Információs Infrastruktúrák (CII) felügyeletéért, valamint a kínai személyes adatok védelméről szóló törvény (*Personal Information Protection Law,* PIPL) gyakorlati implementációjáért, így szabályozói és felügyeleti hatásköre a piaci szereplőkre is kiterjed. A CAC helyettes igazgatójának irányítása alatt áll Kína szabványügyi és kriptográfiai kontrollszervezete, a Nemzeti Információbiztonsági Szabványosítási Műszaki Bizottság (*National Information Security Standardization Technical Committee,* más néven TC260). A CAC tevékenységét a Központi Kiberbiztonsági és Informatikai Bizottság (*Central Commission for Cybersecurity and Informatization,* CCCI) koordinálja, amelyet a kínai kormány 2014-ben hozott létre. A CCCI feladata a kiberbiztonsági stratégia kidolgozása, a kibertér-irányítás és a kínai kiberbiztonsági politika koordinálása, valamint a különböző kiberbiztonsági problémák kezelése. A CCCI vezetője az ország miniszterelnöke, és tagjai között szerepelnek a kínai legfőbb kormányzati szervek vezetői, a vezérkari főnök és más magas rangú tisztségviselők. A szervezet egyéb hatáskörei közé tartozik a kiberbiztonsági törvények és előírások kidolgozása, valamint a kínai kibertér fejlesztésével és védelmével kapcsolatos nemzetközi együttműködés koordinálása.[49]

A KNK feltételezett kiberhírszerzési műveleteinek áttekintése 2015-től napjainkig

Az elmúlt években több jelentős, kritikusinfrastruktúra-elemeket célzó esetet is feltártak, amelyeket az USA igazságszolgáltatási szervei vagy a megbízott kiberbiztonsági magáncégek a Kínai Népköztársasághoz köthető APT-csoportokhoz kapcsoltak. Fontos

[48] Campbell 2021 és Berzsenyi 2023: 92–96.
[49] Lee 2022.

azonban megjegyezni, hogy az ilyen szofisztikáltságú támadások során használt rosszindulatú programok (malware-ek) vagy ezek kódrészleteinek kinyerése esetén is nehéz bizonyítani, hogy melyik konkrét ország vagy APT-csoport felelőssége feltételezhető. A kiberbűnözők és állami aktorok egyaránt törekszenek nyomaik elrejtésére (például saját kódjának törlésére programozott malware-rel) és meghamisítására, például más kiberbűnözői csoportoktól vagy etikus hackerektől, vállalatoktól megszerzett támadó eszközök használatával. A bemutatott esetpéldák hasonló célpont- és eszközrendszere átfogó jellegű, kínai kiberhírszerzési APT-kampányra utalnak.[50]

A kampány egyik eleme a 2015-ben feltárt Anthem-adatlopási incidens, amelyet az amerikai egészségügyi iparágban bekövetkezett egyik legjelentősebb volumenű támadásként jegyeznek. A Deep Panda nevű APT-csoport 2014 decemberében mintegy 78,8 millió személy érzékeny adatait[51] szerezte meg az Anthem Inc. háttéradatbázisaiból, az Egyesült Államok egyik legnagyobb egészségbiztosító vállalatától. A belépési pont egy célzott adathalász-támadás volt, míg az incidens támadási vektora a Derusbi malware nevű kártékony szoftveren alapult, amelynek segítségével a támadók laterálisan (oldalirányban) mozogtak az Anthem hálózatán belül, és végül több mint 50 munkavállalói fiókhoz és 90 különböző rendszerhez jutottak hozzá. Az Anthem-adatlopás becslések szerint 260 millió dolláros kárt okozott a vállalatnak, amely összeg magában foglalta a rekordmértékű HIPAA-büntetést (16 millió USD)[52] és több száz millió dolláros jogi költségeket (például a 15 millió dolláros csoportos peres megállapodás), továbbá az ügyfelek tájékoztatására elkülönített kommunikációs költségeket, valamint a remediációs és helyreállítási intézkedések anyagi erőforrásait és a kiberbiztonsági szakértői díjazást.[53] Kérdéses, hogy a támadás politikai vagy gazdasági okokból történt-e, mindazonáltal további nemzetbiztonsági kockázatokat jelent, hogy a zsákmányolt adatok továbbértékesíthetők és felhasználhatók, például az érintettek célzott megfigyelésére, hamisított dokumentumok készítéséhez vagy más támadások kivitelezésére (például célzott adathalász-támadásra való felkészülés, megszemélyesítés).

Egyértelműbb kiberhírszerzési célpont volt az amerikai kormányzati szervek emberierőforrás-menedzsmentjével foglalkozó Személyzeti Menedzsment Hivatalát (Office of Personnel Management, OPM) ért támadás. Az adatlopás 2015. júniusi felfedezéséig mintegy 22 millió felhasználó személyes adatait szerezték meg olyan háttéradatbázisokból, amelyeken ujjlenyomatokat és olyan kitöltött űrlapokat tároltak, amelyek a kormányzati biztonsági engedélyekhez szükséges háttérvizsgálatok során gyűjtött személyes információkat tartalmaztak. Az incidensről kiadott hivatalos kongresszusi jelentésben a támadás idővonalát és a támadók tevékenységét csak részben sikerült visszafejteni, többek közt a behatolási pont sem volt egyértelműen beazonosítható, ám kiderült, hogy akár több különböző támadó aktor is jelen lehetett eltérő időpontban. Először 2013 novemberében törték fel az OPM egyes rendszereit, ekkor üzemeltetési kézikönyveket és a rendszer-architektúra

50 Krebs 2015.

51 Például nevek, születési adatok, társadalombiztosítási számok, egészségügyi ellátási azonosítószámok, kapcsolattartási adatok (pl. e-mail- és lakcím) és jövedelmi adatok. A támadók azonban nem fértek hozzá egészségügyi leletek adataihoz vagy fizetési és bankkártyaadatokhoz.

52 Az USA Egészségbiztosítási Portabilitási és Felelősségi Törvénye *(Health Insurance Portability and Accountability Act).*

53 Young 2021.

feltérképezéséhez felhasználható információkat szereztek meg. Egy hónappal később kísérelték meg az USIS és a KeyPoint feltörését, amelyek a kormányzati háttérellenőrzést és átvilágítást végző alvállalkozókként aktív hozzáféréssel rendelkeztek az OPM személyes adatokat tartalmazó szervereihez. A kongresszusi jelentés kiemeli, hogy az OPM IT-biztonsági személyzete azért nem tett lépéseket a támadók kizárására – amikor 2014 márciusában észlelték jelenlétüket egy olyan hálózatban, amely nem tartalmazott érzékeny adatokat –, mert így ellenhírszerzést végezve feltérképezhették egy potenciális APT-aktor tevékenységét. Az OPM szakemberei végül 2014 májusában kényszerítettek ki egy rendszerátállítást, amely végleg kizárta volna a támadókat, akik elkezdtek keyloggereket telepíteni a személyzeti adatbázisok adminisztrátorainak munkaállomásaira. Az OPM adatvesztését végül a beszállítói láncuk sérülékenysége okozta. Ugyanis még a rendszerátállítást megelőzően, feltehetőleg egy másik támadó aktor, észrevétlenül hitelesítő adatokat szerzett meg a KeyPoint vállalattól.

Ezeket felhasználva a korábbiaktól eltérő belépési pontot létesítettek az OPM rendszerében, és valósnak tűnő hozzáférési jogosultságot szereztek, amelyet a rendszerfrissítés érintetlenül hagyott. Így a támadók képessé váltak egy olyan malware telepítésére, amely a rendszerfrissítés ellenére hátsó kaput nyitott *(backdoor)*. 2014 nyarán ezen az útvonalon keresztül exfiltrálták a kormányzati háttérellenőrzések eredményeit tartalmazó adatbázisokat. A kongresszusi jelentésben nem tárták fel, hogy az első és második kiberművelet elkövetője ugyanaz az aktor lehetett-e, ám feltételezhető, hogy kooperáltak a rendszer-architektúrára vonatkozó és az üzemeltetési kézikönyvekből kinyerhető információk felhasználásával. 2014 októberére a támadók privilegizált AD-jogosultság-eszkaláció révén *(Active Directory privilege escalation)* telepítették a távoli irányítást *(remote control)* biztosító Sakula malware-t, illetve egy PlugX malware-változatot, amely távoli hozzáférést *(remote access)* biztosított, és lehetővé tette az OPM rendszereiben való navigálást, adatok tömörítését és kiszivárogtatását. Átjutva az OPM környezetén feltörték az amerikai belügyminisztérium egyik szerverét, így az év végére újabb adatokat loptak el a kormányzat személyzeti nyilvántartásaiból, majd 2015 márciusában exfiltrálták az ujjlenyomatokat tartalmazó adatbázisokat. Az OPM biztonsági szakemberei 2015 áprilisában, a titkosított SSL-forgalom ellenőrzésének alkalmával tárták fel jelenlétüket a rendszereikben a gyanús adatforgalom alapján. Az incidens nyilvános attribúciója 2018-ban volt, amikor az NSA képviselője a KNK-t nevezte meg a támadás felelőseként. Konkrét vádemelés ekkor még nem történt, mert az OPM-ügyben beazonosított eszközök, az Equifax-adatlopással és Marriott-incidenssel összehasonlítva, rávilágítottak egy átfogó kínai kiberhírszerzési kampány eshetőségére.[54]

Az Equifax Inc. hitelminősítő céget 2017-ben érte adatlopási támadás, amely mintegy 143 millió ügyfél olyan személyes adatait érintette (a felhasználók teljes neve, lakcíme, születési dátuma, vezetői engedélye, bankkártyaszáma, társadalombiztosítási száma), amelyek felhasználhatók megszemélyesítéshez, illetéktelen tranzakciók végrehajtására, vagy további megfigyelésre és profilozáshoz. Az Amerikai Igazságügyi Minisztérium hivatalosan 2020 februárjában emelt vádat négy kínai katonai tiszt ellen az Equifax-adatlopás miatt. A vádirat ismertetésekor azonban az esetet nyíltan összekapcsolták a Marriott

[54] Fruhlinger 2020a.

elleni és az OPM-támadással egy nagyobb művelet részelemeiként.[55] Fruhlinger kiberbiztonsági szakértő elemzésében a vádemelést meglehetősen szokatlan lépésként értékelte, mivel az Egyesült Államok ritkán indít büntetőeljárást külföldi hírszerzők ellen, hogy elkerülje az amerikai ügynökökkel szembeni megtorlást. Ebben a narratívában a feltárt APT-kampány kiberdiplomáciai hatása rávilágít arra, hogy az amerikai kormány mennyire súlyos nemzetbiztonsági incidensként értékelte a támadásokat.[56]

A Marriott-adatlopás kapcsán a *New York Times* és a *Washington Post* hírportálok 2018 decemberében egy névtelenséget kérő kormányzati kontaktra hivatkozva számoltak be a KNK tevékenységének gyanújáról, ám a kormányzati szervek ekkor még nem tettek közzé részletekbe menő hivatalos technikai jelentést.[57] A Marriott Szállodalánc szakemberei 2018 szeptemberében egy szokatlan adatelérési kérést *(unusual database query)* észlelő felügyeleti eszköz riasztása miatt indítottak kivizsgálást, a korábban a Starwood vállalathoz tartozó hotelek (például a Westin, Sheraton, St. Regis és W hotelek) foglalásait kezelő belső rendszerben. A digitális nyomelemzés másfél hónappal később visszafejtette, hogy valamikor 2014-ben törhették fel a Starwood IT-infrastruktúráját, amikor az még különálló vállalatként működött.[58] A négy év során megközelítőleg 500 millió vendég foglalási adatait titkosították és exfiltrálták egy olyan adminisztrátori fiók segítségével, amely felett átvették az irányítást egy távoli hozzáférést biztosító trójai vírus (*Remote Access Trojan,* RAT) és egy etikus hackerek által is használt nyílt forráskódú eszköz, a Mimikatz[59] segítségével, amelyek a támadás vektoraiként értékelhetők.[60] Az elkövetkező években további technikai részletet is publikáltak, 2022-ben a CrowdStrike szakértője, Ryan Cornateanu, egy e-mail-hamisítási technikára *(email spoofing)* vezette vissza a belépési pontot, amely adathalász-támadást tehetett lehetővé.

A csoportos kártérítési igények mellett a szállodaláncra 23,8 millió dolláros bírságot szabtak ki a GDPR[61] megsértése miatt, továbbá kötelezettséget vállalt az érintettek útlevélcsere-költségeinek átvállalására.[62] Fruhlinger kiberbiztonsági szakértő elemzésében rávilágít arra, hogy az incidens, hasonlóképpen az OPM-adatlopáshoz, azon tények alapján utalt állami kiberhírszerzési műveletre, hogy nem találtak arra utaló jeleket, hogy a megszerzett személyes adatokat tartalmazó csomagokat[63] eladásra kínálták volna a dark weben, vagy felhasználták volna anyagi haszonszerzés céljából megszemélyesítésre, ahogy egy kiberbűnözői csoport tette volna. Emellett a Marriott Szállodalánc az amerikai kormányzat és hadsereg egyik legnagyobb szállásadó partnere, így a zsákmányolt útlevél

55 BBC (2020).

56 Fruhlinger 2020a.

57 Nakashima–Timberg 2018 és Sanger et al. 2018.

58 A Marriott 2016-ban vásárolta fel a Starwoodot, de majdnem két évvel később a korábbi Starwood Szállodák (például a Westin, Sheraton, St. Regis és W hotelek) még nem kerültek át a Marriott saját foglalási rendszerére, és továbbra is a Starwoodtól örökölt IT-infrastruktúrát használták, lásd Fruhlinger 2020b.

59 A Mimikatz Microsoft-alapú végpontokon képes kivonni a rendszermemóriából a felhasználónév-jelszó párokat. Soare 2022.

60 Fruhlinger 2020b.

61 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről.

62 Hollander 2023.

63 Az adatcsomagok olyan információkat tartalmaztak, mint: név, születési dátum, nem, levelezési és e-mail-cím, telefonszám, útlevélszám, Starwood Preferred Guest (SPG) számlaadatok, érkezési és távozási adatok, foglalási dátum és kommunikációs preferenciák. Hollander 2023.

és személyazonosító igazolványok számai vagy bankkártyaadatok az OPM-adatlopás során szerzett információkkal kombinálhatók. Az így létrehozott big data adatbázis elemzésével lehetővé válhat a kormányzati alkalmazottak (köztük hírszerzők) és hivatásos személyek mozgásának nyomon követése.[64] Említésre méltó, hogy a szállodaláncot 2020-ban és 2022-ben is érték további, önálló incidensek, amelyeket azonban még nem attribuáltak.[65]

A SolarWinds vállalat Orion rendszerének egy másik sérülékenységét kihasználó támadás mögött kínai állami érdekről jelentek meg sajtóközlemények 2022-ben. Felügyeleti rendszerként a SolarWinds Orion terméke privilegizált hozzáféréssel rendelkezik az informatikai rendszerekhez, hogy napló- és rendszerteljesítmény-adatokat használhasson fel, így értékes célponttá vált. A Reuters hírügynökség az FBI folyamatban lévő nyomozására hivatkozva publikálta, hogy a feltételezhetően kínai aktorok a Sunburst nevű malware-t felhasználó támadással (amelyet orosz aktorokra attribuáltak 2020-ban) egy időben használták ki a SolarWinds rendszer sérülékenységét. Ezen második támadás alkalmával használt rosszindulatú programot a SolarWinds vállalat Supernova néven azonosította. A Reuters jelentése szerint a feltételezett kínai aktorok az Egyesült Államok Mezőgazdasági Minisztériumának egyik bérszámfejtő ügynökségét, a Nemzeti Pénzügyi Központot vették célba, amely megközelítőleg 600 ezer munkavállaló adatát kezeli, és több mint 160 ügynökségnek nyújt szolgáltatást. Arról azonban nincs információ, hogy történt-e kompromittálódás. Az újabb SolarWinds-eset is kiemelkedő jelentőségű, mert rávilágít arra, hogy az offenzív szereplők ismételten képesek voltak az Orion szoftvert támadó eszközzé formálni. A sajtóban megjelent vádakat a kínai külügyminisztérium is kommentálta, miszerint Kína határozottan ellenzi, és eltökélten küzd a kibertámadások és adatlopások minden típusa ellen, áll a Reuters által is idézett közleményben. A külügyminisztérium emellett hangsúlyozta azon igényét, hogy az amerikai kormányzat minden vádat konkrét bizonyítékokkal támasszon alá, utalva a technikai attribúció komplexitásából fakadó bizonytalansági tényezőkre.[66]

Noha az Anthem-adatlopási incidens, az Equifax – OPM – Mariott-kampány, valamint a SolarWinds-Orion szoftver kompromittálása különböző vertikumban elhelyezkedő intézmények elleni műveletek, párhuzamosságként azonosítható, hogy a megszerzett adatok lehetővé tehetik az Egyesült Államok kormányzati tevékenységének komplex megfigyelését, elemzését és befolyásolását, a szervezeti infrastruktúraelemek feltérképezése és a személyi állományról elérhető háttérinformációk révén. A fejezetben ismertetett kiberhírszerzési eseteket és a bevezetőben tárgyalt választási és általános politikai információszerzésre irányuló kiberműveleteket egyaránt az a stratégiai cél motiválhatta, hogy olyan háttér-információkhoz juttassák a kínai döntéshozókat, amelyek révén képesek finomhangolni az ország nemzetközi befolyásának növekedésére tett nonkonfrontatív erőfeszítéseket és konfrontatív – például választások eredményére ható – érdekérvényesítő képességét. Az ilyen célú kiberhírszerzési tevékenység napjainkra egyre mérvadóbbá vált a Kína nagyhatalommá válását közvetlenül megelőzően fennálló nemzetközi rendszert

64 Fruhlinger 2020b.
65 McGarry 2022.
66 Bing et al. 2021.

leginkább domináló országokban, amelyek jellemzően a globális „Nyugat" országai (az USA és az EU legnagyobb katonai-gazdasági befolyással rendelkező tagállamai).

Az USA mellett az európai régió célponttá válását helyezi kontextusba P. Szabó elemzése a kínai „kétvágányos" külpolitikai cél-, érték-, érdek- és eszközrendszerről, és magyarázatot ad arra, hogy a napjainkban tapasztalható befolyásolási törekvések – amelyek akár a kibertér által is megvalósulhatnak – milyen stratégiai hátrányok leküzdésére irányulnak. Az érintett államok társadalmának jelentős része – ideértve a domináns politikai erőket is – kritikus Kínával szemben. Ez egyrészt abból ered, hogy értékrendbeli ellentét áll fenn a pekingi vezetéssel a szocialista pártállami rendszer miatt, másrészt potenciális katonai fenyegetésnek értékelik Kínát. Harmadrészt, ezen államok lakosságának zöme úgy vélekedik, hogy rövid és középtávú gazdasági érdekei ellentétesek Kína IKT-technológiai és kereskedelmi befolyását növelő törekvéseivel.[67]

Összességében elmondható, hogy a kínai külpolitika – ideértve a nyilvános attribúcióhoz fűződő álláspontját – igyekszik eloszlatni az általa jelentett (katonai) fenyegetéssel kapcsolatos percepciót, mert az jelentősen korlátozza kiberhatalmi státuszának felépítését és nemzetközi érdekérvényesítő képességének növekedését (aminek stratégiai célja egy Kína által jelentősen befolyásolt vagy Kína által dominált világrend kiépítése). Annak ellenére, hogy napjainkra a kínai állami és állam alatti kiberegységek (APT) tevékenysége egyre konfrontatívabbá válik, és ezáltal egyre jelentősebb külkereskedelmi és kiberdiplomáciai szankciós intézkedést váltanak ki a „nyugati" nagyhatalmak részéről, Kína mindeddig tartózkodott az olyan mértékű, kritikusinfrastruktúra-elemeket érő károkozástól, amely az orosz vagy az észak-koreai állami aktivitást jellemzi.

Összegzés és konklúzió

Azon APT-csoportokról, amelyek feltehetően kiberbűnözői és kínai hátterű, állam alatti kiberegységként is tevékenységet folytatnak, globális viszonylatban megállapítható, hogy az általuk elkövetett – 2015 óta egyre gyakoribb – sikeres incidensek és behatolási kísérletek fő stratégiai célja a védelmi ipari és csúcstechnológiákra vonatkozó információk, továbbá a kínai geopolitikai célokat támogató hírszerzési adatok megszerzése. Napjainkban a kínai tevékenységre nyilvánosan attribútált kiberhírszerzési esetek jelentős arányban politikai befolyásszerzés céljából végrehajtott kiberműveletek (míg például Észak-Korea esetében az anyagi haszonszerzés a fő motiváció, és a célpontok többsége a pénzügyi vertikumban található szervezet). A kínai állam alatti (APT-) és állami (PLA-) kiberegységek offenzív kiberműveletei várhatóan tovább erősödnek az USA elnöki, európai uniós parlamenti és további tagállami választások közeledtével.

A védelmi technológiák fejlődése és az információmegosztás (például CTI-platformok és kormányközi kezdeményezések) ellenére, továbbra is nehézséget okoz csak technikai adatokra és a korábban feltárt – feltehetően kínai hátterű – kiberhírszerzési esetekre alapozva objektíven bizonyítani egy-egy támadás mögött meghúzódó állami érdekeltséget. Esetenként a támadás során feltárt geolokációs adatok (vagy IP-címek), programozási nyelv és a korábban publikált támadó eszközök (egyéb könnyebben reprodukálható offenzív

[67] P. Szabó 2020.

technikák és támadó kódrészletek) újbóli felhasználása miatt, a kielemzett digitális nyomok még évekig nem tudnak kielégítő bizonyítékot szolgáltatni a vádemeléshez és a kiberdiplomáciai szempontból kockázatos nyilvános attribúcióhoz. A bemutatott esetekből is látszik, hogy az egyes APT-csoportokra jellemző TTP-k beazonosítása (amelyek szintén fejlődnek az évek során), így a támogató állam beazonosítása is, referenciaként felhasználható vagy összehasonlítható incidensek bekövetkezése esetén lehetséges.

Összességében megállapítható, hogy a kiberhírszerzési tevékenység fő célja a gazdasági, technológiai és politikai előnyök megszerzése. A 2015 után megindított APT-műveletek célpontkiválasztása főként személyes adatok megszerzésére (Marriott-, Equifax- és Anthem-incidensek) irányult, amelyek tovább értékesíthetők vagy felhasználhatók adatigényes egészségügyi vagy pénzügyi intelligenciák (AI vagy ML) vagy speciális IoT-eszközök (IoMT – *internet of medical things,* az orvosi tárgyak internete) fejlesztési és piackutatási szakaszában. A kínai APT-csoportok rendkívül fejlett támadó eszközökkel és olyan szakértelemmel rendelkeznek, amit jól szemléltetnek az USA-ból származó esetpéldák, rámutatva arra, hogy a kínai hátterű APT-k képesek behatolni más országok hadiipari vállalatainak és védelmi minisztériumainak hálózataiba (RSA-incidens), vagy kompromittálni a személyi állomány adatbázisát (OPM-incidens), továbbá információkat gyűjteni a legújabb technológiákról és hadiipari fejlesztésekről (SolarWinds-incidens újabb sérülékenységének kihasználása). A kínai kiberhírszerzési tevékenység összetett, integrált rendszert alkot az Állambiztonsági Minisztérium és a hadsereg között.

A PLA képességeinek átalakítása és a haderőfejlesztési programok offenzív kiberképességek kialakítására tett erőfeszítései (például a Stratégiai Támogató Erők és a Vezérkar állományán belül) regionális szinten kiemelkedő katonai erővé emelték Kínát, ám növelték a digitális rendszerektől való függőségét is. Nemzetbiztonsági és katonai relevanciával is bír az utóbbi évek egyre erősödő trendje, hogy a kínai tehetségek fokozatos átáramlása tapasztalható a nemzetközi gyakorlatok és „hackerkonferenciák" résztvevői közül a hazai versenyek és platformok (például 2017-től a Tianfu Cup) irányába, mert ez a képességek tudatos elrejtésére való törekvést is jelentheti. Emiatt az offenzív képességekkel rendelkező kínai szakemberek tudásszintjének felmérése és nemzetközi összehasonlítása nehezebbé válik, továbbá az általuk használt szofisztikált támadó vagy sérülékenységeket feltáró programok eredményességéről is nehezebb tapasztalatokat és objektív visszajelzést kapni. Körülményesebbé és nehezebbé válik a védelmi rendszerek felkészítése és továbbfejlesztése.[68]

Felhasznált irodalom

BBC (2020): Equifax: US Charges Four Chinese Military Officers Over Huge Hack. *BBC,* 2020. február 11. Online: www.bbc.com/news/world-us-canada-51449778

Berzsenyi Dániel (2023): *Különleges kiberműveletek: A kiber különleges műveleti képesség és kialakításának vizsgálata*. PhD-disszertáció. Budapest: Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola. Online: https://doi.org/10.17625/NKE.2023.012

[68] Cimpanu 2021.

Bianco, David (2013): *Pyramid of Pain: A Model for Prioritizing Which Indicators of Compromise To Address First.* Online: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Bing, Christopher et al. (2021): Exclusive: Suspected Chinese Hackers Used SolarWinds Bug to Spy on U.S. Payroll Agency – Sources. *Reuters,* 2021. február 2. Online: www.reuters.com/article/us-cyber-solarwinds-china-exclusive-idUSKBN2A22K8

Campbell, Caitlin (2021): *China's Military: The People's Liberation Army (PLA).* Congressional Research Service, 2021. június 4. Online: https://crsreports.congress.gov/product/pdf/R/R46808

Cimpanu, Catalin (2021): Windows 10, iOS 15, Ubuntu, Chrome Fall at China's Tianfu Hacking Contest. *The Record,* 2021. október 17. Online: https://therecord.media/windows-10-ios-15-ubuntu-chrome-fall-at-chinas-tianfu-hacking-contest/

Dobák Imre – Tóth Tamás (2021): Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering). *Belügyi Szemle,* 69(2), 195–212. Online: https://doi.org/10.38146/BSZ.2021.2.2

Electronic Transactions Development Agency (2021): Threat Group Cards: A Threat Actor Encyclopedia – APT Group: Comment Crew, APT 1. Online: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=b99367ed-e483-40a3-98d0-8d3a2102a4ab

Electronic Transactions Development Agency (2022a): Threat Group Cards: A Threat Actor Encyclopedia – All Groups from China. Online: https://apt.etda.or.th/cgi-bin/listgroups.cgi?c=China

Electronic Transactions Development Agency (2022b): Threat Group Cards: A Threat Actor Encyclopedia – APT Group: APT 19, Deep Panda, C0d0so0. Digital Service Security Center, ETDA. Online: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=58c7e347-341c-4446-bf03-81fc1f7d9254

Flashpoint Team (2022): *Guide to Cyber Threat Intelligence: Elements of an Effective Threat Intel and Cyber Risk Remediation Program.* Online: https://flashpoint.io/blog/guide-to-cyber-threat-intelligence/

Friis, Karsten – Lysne, Olav (2021): Huawei, 5G and Security: Technological Limitations and Political Responses. *Development and Change,* 52(5), 1174–1195. Online: https://doi.org/10.1111/dech.12680

Fruhlinger, Josh (2020a): The OPM Hack Explained: Bad Security Practices Meet China's Captain America. *CSO,* 2020. február 12. Online: www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Fruhlinger, Josh (2020b): Marriott Data Breach FAQ: How Did It Happen and What Was the Impact? *CSO,* 2020. február 12. Online: www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

Greenberg, Andy (2021): The Full Story of the Stunning RSA Hack Can Finally Be Told. *Wired,* 2021. május 20. Online: www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/

Greig, Jonathan (2024): Us Sanctions Alleged Chinese State Hackers for Attacks on Critical Infrastructure. *The Record,* 2024. március 25. Online: https://therecord.media/us-sanctions-chinese-hackers-infrastructure-attacks

Gyebnár Gergő (2023): *The Future of Industrial Threat Intelligence.* Black Cell Magyarország Kft. Online: https://web.archive.org/web/20230419093133/https://blackcell.io/blog/2023/04/19/the-future-of-industrial-threat-intelligence/

Hannas, William C. – Tatlow, Didi Kristen szerk. (2020): *China's Quest for Foreign Technology. Beyond Espionage.* London: Routledge. Online: https://doi.org/10.4324/9781003035084

Hollander, Jordan (2023): Marriott Data Breach FAQ: What Really Happened? *HotelTechReport,* 2023. február 16. Online: https://hoteltechreport.com/news/marriott-data-breach

Inkster, Nigel (2015): The Chinese Intelligence Agencies – Evolution and Empowerment in Cyberspace. In Lindsay, Jon R. – Cheung, Tai Ming – Reveron, Derek S. (szerk.): *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain.* Oxford University Press, 29–50. Online: https://doi.org/10.1093/acprof:oso/9780190201265.003.0002

Kaska, Kadri – Beckvard, Henrik – Minárik, Tomáš (2019): *Huawei, 5G and China as a Security Threat.* NATO Cooperative Cyber Defence Center for Excellence (CCDCOE), 1–26. Online: https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/

Kaszián Ábel Gergő (2021): A GDPR kínai „unokatestvére" – avagy a kínai adatvédelmi törvény megszületése és várható hatásai. *Jogi Fórum,* 2021. szeptember 20. Online: www.jogiforum.hu/publikacio/2021/09/20/a-gdpr-kinai-unokatestvere-avagy-a-kinai-adatvedelmi-torveny-megszuletese-es-varhato-hatasai/

Krebs, Brian (2015): Catching Up on the OPM Breach. *Krebs on Security,* 2015. június 15. Online: https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/

Lee, John (2022): Cyberspace Governance in China: Evolution, Features and Future Trends. *Asie Visions*, (129). Ifri. 2022. július 29. Online: www.ifri.org/en/publications/notes-de-lifri/asie-visions/cyberspace-governance-china-evolution-features-and-future

Lima da Frota Araujo, Carlos Raul – Szunomár Ágnes (2022): Kelet-Közép-Európa a digitális selyemúton? Lehetséges politikai gazdaságtani magyarázatok. *Közgazdasági Szemle*, 69(3), 367–388. Online: https://doi.org/10.18414/KSZ.2022.3.367

Lindsay, Jon R. – Cheung, Tai Ming (2015): From Exploitation to Innovation: Acquisition, Absorption, and Application. In Lindsay, Jon R. – Cheung, Tai Ming – Reveron, Derek S. (szerk.): *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain.* Oxford University Press, 51–86. Online: https://doi.org/10.1093/acprof:oso/9780190201265.003.0003

Lindsay, Jon R. – Cheung, Tai Ming – Reveron, Derek S. szerk. (2015): *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain.* Oxford University Press. Online: https://doi.org/10.1093/acprof:oso/9780190201265.001.0001

Lusthaus, Jonathan – Bruce, Miranda – Phair, Nigel (2020): *Mapping the Geography of Cybercrime: A Review of Indices of Digital Offending by Country.* 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). 2020. szeptember 7–11. Online: https://doi.org/10.1109/EuroSPW51379.2020.00066

Macaskill, Andrew – Pearson, James (2024): Britain Says China Hacked Electoral Watchdog, Targeted Lawmaker Emails. *Reuters,* 2024. március 25. Online: www.reuters.com/world/uk/uk-deputy-pm-set-address-lawmakers-chinese-cyber-security-threat-2024-03-24/

Matura Tamás et al. (2022): *Risky Business? Assessing Political Economic and Technological Risk Perceptions of Relations between the People's Republic of China and Hungary.* Budapest: Central and Eastern European Center for Asian Studies.

McGarry, Pat (2022): Lessons Learned from the Marriott Hack of 2022. *Threater,* 2022. június 9. Online: www.threatblockr.com/blog/lessons-learned-from-the-marriott-hack-of-2022

Mészáros R. Tamás (2021): Annyi adatot gyűjtöttek, hogy a Kínai Kommunista Párt is megijedt tőle. *G7,* 2021. július 25. Online: https://g7.hu/vilag/20210725/annyi-adatot-gyujottek-hogy-a-kinai-kommunista-part-is-megijedt-tole/

Nakashima, Ellen – Timberg, Craig (2018a): U.S. Investigators Point to China in Marriott Hack Affecting 500 million guests. *Washington Post,* 2018. december 12. Online: www.washingtonpost.com/technology/2018/12/12/us-investigators-point-china-marriott-hack-affecting-million-travelers/

Pearson, James – Satter, Raphael – Bing, Christopher (2024): US, UK Accuse China of Cyberespionage That Hit Millions of People. *Reuters,* 2024. március 25. Online: www.reuters.com/technology/cybersecurity/us-sanctions-chinese-cyberespionage-firm-saying-it-hacked-us-energy-industry-2024-03-25/

Pennino, Alex – Bromiley, Matt (2022): GAME OVER: Detecting and Stopping an APT41 Operation. *Mandiant,* 2019. augusztus 19. Online: www.mandiant.com/resources/blog/game-over-detecting-and-stopping-an-apt41-operation

Plan, Fred et al. (2024): *APT40: Examining a China-Nexus Espionage Actor. Mandiant.* Online: www.mandiant.com/resources/blog/apt40-examining-a-china-nexus-espionage-actor

P. Szabó S. (2020): A Kínai Népköztársaság „kétvágányos" külpolitikája. In P. Szabó Sándor – Horváthné Varga Polyák Csilla (szerk.): *Lehetőségek és kihívások a magyar–kínai kapcsolatok területén. I. kötet. Politikai kapcsolatok.* Budapest: Ludovika, 9–28.

Sanger, David E. et al. (2018): Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing. *New York Times,* 2018. december 11. Online: www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html

Segal, Adam (2020): China's Pursuit of Cyberpower. In Segal, Adam et al.: The Future of Cybersecurity across the Asia-Pacific. *Asia Policy,* (15)2, 60–66. Online: https://doi.org/10.1353/asp.2020.0034

Smith, Zhanna Malekos (2022): Emerging Cyber Threats: No State Is an Island in Cyberspace. *CSIS,* 2022. március 23. Online: www.csis.org/analysis/emerging-cyber-threats-no-state-island-cyberspace

Soare, Bianca (2022): What is Mimikatz? What Can It Do and How to Protect. *Heimdal,* 2022. december 7. Online: https://heimdalsecurity.com/blog/mimikatz/

Szeleczki Szilveszter (2022): A kiberhírszerzés értelmezése és helye a nemzetbiztonságban. *Nemzetbiztonsági Szemle,* 10(4), 17–29. Online: https://doi.org/10.32561/nsz.2022.4.2

USA White House, Office of the Press Secretary (2015): *FACT SHEET: President Xi Jinping's State Visit to the United States. Cybersecurity.* Online: https://obamawhitehouse.

archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

US Department of Justice (2024): *Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians*. 2024. március 25. Online: www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived

Yang, Fan (2022): The Problem with Ill-Substantiated Public Cyber Attribution: A Legal Perspective. In Levite, Ariel E. et al. (szerk.): *Managing U.S.-China Tensions Over Public Cyber Attribution*. Washington, D.C: Carnegie Endowment for International Peace, 6–14. Online: https://carnegieendowment.org/files/Perkovich_et_al_Cyber_Attribution_web.pdf

Young, Kelli (2021): Cyber Case Study: Anthem Data Breach. *Coverlink*, 2021. szeptember 27. Online: https://coverlink.com/case-study/anthem-data-breach/

NEMZETBIZTONSÁGI SZEMLE
12. évfolyam (2024) 2. szám 81–97. | DOI: 10.32561/nsz.2024.2.5

Horváth Ferenc[1]

Új képzési módszerek alkalmazásának tapasztalatai a Nemzetbiztonsági Szakszolgálatnál

Experience in the Application of New Training Methods at the SSNS

A technikai lehetőségek fejlődése, az új generációk munkaerőpiacra lépése, illetve az elmúlt évek pandémiás kihívásai együttesen olyan közeget teremtettek, amelyek nélkülözhetetlenné tették, hogy a hagyományos oktatási megoldások mellett új szemléletű képzési módszerekkel próbáljuk meg biztosítani a pályára lépők számára a betanulást, illetve a már polgári nemzetbiztonsági pályán lévők számára a továbbképzési lehetőségeket. A hagyományos paradigma szerint a pályakör betöltéséhez szükséges ismereteket elméleti oktatással, előadásokkal, jegyzetekkel, vizsgákkal kell biztosítani, miközben szigorúan ellenőrizni kell a részvételt, a felkészülést és a számonkérés tisztaságát. Egy lépést jelent előre, de érdemi változást önmagában nem hoz, amikor ugyanezeket a megoldásokat elektronikus felületekre helyezik át. Az igazi áttörést az jelenti, amikor magukat a tanulókat, az ő igényeiket és sajátosságaikat sikerül fókuszba helyezni. Amikor a tanulásra szorítás helyett a tanulás lehetőségének felhasználóbarát megteremtése válik elsődlegessé. Az ismeretátadás helyett a kompetenciafejlesztés, a közlés helyett az interakció, a beszéd helyett a multimodális megtapasztalás, a kötelezés helyett a gamifikáció, az emlékezettesztelés helyett a gyakorlati alkalmazás, az oktatói hatalom helyett a partneri bevonás. A tanulmány az új képzési módszerekkel kapcsolatos gyakorlati tapasztalatainkat foglalja össze.

Kulcsszavak: *képzés, kompetenciafejlesztés, e-learning, tréning*

The development of technical possibilities, the entrance of new generations into the labor market, and the challenges presented by recent pandemics have created an environment that necessitates the provision of training opportunities for newcomers to the profession. It also highlights the need for advanced training opportunities for those already pursuing careers in civilian national security, incorporating new training methods alongside traditional educational solutions. According to the traditional

[1] PhD, Nemzetbiztonsági Szakszolgálat, e-mail: fhorvath25@gmail.com

paradigm, the knowledge required to complete the career circle should be provided through theoretical education, which includes lectures, notes, exams, with strict control over attendance, preparation, and the clarity of examinations. However, merely transferring these solutions to electronic interfaces represents a step forward but does not, in itself, effect any real change. A genuine breakthrough occurs when the focus shifts to the students – considering their needs and characteristics – prioritizing the user-friendly creation of learning opportunities over rigid learning constraints. This approach emphasizes competence development over simple knowledge transfer, interaction over mere communication, multimodal experiences over plain speech, gamification over obligation, practical application over memorization, and partner involvement over authoritarian teaching. This study summarizes our practical experiences with these innovative training methods.

Keywords: *training, competence development, e-learning, training*

Bevezetés

A rendvédelmi szféra számára minden tekintetben nagy kihívást jelent, hogy lépést tudjon tartani. A technológiai újítások, innovációk rendszerbe állítását költségvetési korlátok és szigorú beszerzési szabályok közepette kell megvalósítani. Az ebben részt vevő kvalifikált szakembereket kompetitív munkaerőpiaci környezetben kell tudni bevonzani és megtartani, alapvetően kötött bértáblával. A szervezeti kultúra ugyan már elszakadt a rendszerváltás előtti hierarchikus és autoriter szovjet rendvédelmi modelltől, de még messze van a versenyszféra felhatalmazáson és partnerségen alapuló működésmódjától. Az új generációk munkahelyi beilleszkedése más preferenciák mentén zajlik, mint a korábbi generációké,[2] így a pályára állítás képzései terén is haladni kell a korral.

A tanulmány az elmúlt bő évtized során bevezetett új megoldásokat taglalja a Nemzetbiztonsági Szakszolgálat képzési rendszerében. Ezek mindegyike az interaktivitás és gyakorlatiasság irányában bővíti a képzési palettánkat, igazodva az újabb generációk ismeretelsajátítási szokásaihoz. A hagyományos előadás és írásos jegyzet, majd szóbeli vagy írásbeli vizsga alapján történő, tisztán elméleti oktatás mellett 15 éve intézményszerűen megjelentek a tréningek, illetve a szituációs gyakorlatok és ezek esettanulmányként való közös elemzése. Elterjedtté váltak az e-learning-megoldások, több ízben írtunk mi magunk is forgatókönyvet és gyártattunk le interaktív, gamifikált anyagokat, amelyeket az egész állomány rugalmas időbeosztásban tudott teljesíteni. A pandémia idején terjedt el a webkamerás oktatás, online közvetítés, illetve a videókkal bővített elektronikus tananyag megosztása Moodle felületen. Ezt fejlesztik tovább a nyelvoktatásban az online képzési felületek (például Classroom, Teams) és a jelenléti oktatást színesítő kompetitív teszt- és kvízalkalmazások (például Redmenta, Wordwall, Kahoot, Quizlet), videómegosztók tartalmai (például YouTube). Az angol nyelvoktatás fókusza a hagyományos, kurzuskönyvön alapuló tudásfelépítő tanfolyamok helyett az intenzív, kommunikációcentrikus formák irányába mozdult el, ahol már inkább a meglévő passzív tudás aktivizálásán, hadra

[2] Lyons–Kuron 2014.

fogásának gyakorlásán, a magabiztosság fejlesztésén van a hangsúly, azaz a beszélt/írott nyelven, az elmélet és a nyelvhelyesség helyett.

A tanulmányban ezeket az új képzési megoldásokat, illetve az ezek bevezetésével kapcsolatos tapasztalatokat foglaljuk össze.

Új képzési megoldások a rendvédelemben

Az elmúlt években számos tanulmány látott napvilágot azzal kapcsolatban, hogy a rendvédelmi oktatásban hogyan kaphatnak helyet új képzési módszerek. Olyannyira fontos ez a téma, hogy 2020-ban a Belügyi Tudományos Tanács *Online és offline tanítási-tanulási módszerek a belügyi ágazatban* címmel pályázatot hirdetett annak érdekében, hogy a témakörrel kapcsolatos tapasztalatokat hatékonyan megoszthassák egymással a szakemberek. E pályázat díjazottjai az elektronikus oktatási megoldások hatékony hasznosíthatóságáról számoltak be, illetve kiemelték, hogy a pályára lépő új generációk tanulási szokásaihoz jobban illeszkednek az elektronikus megoldásokkal támogatott oktatási formák, legyen szó nyelvoktatásról,[3] e-learning-tananyagokról,[4] vagy információs és kommunikációs technológiák (IKT) által támogatott oktatásról.[5] Ehhez persze szükség van a digitális kompetenciák fejlesztésére mind a diákok, mind a tanárok részéről – és ez inkább az utóbbi oldalról jelent kihívásokat, hiszen az új generációk „digitális bennszülöttek".[6]

A pályára lépők közszolgálati pályaorientációs képzésének módszertani lehetőségei kapcsán foglalja össze Belényesi a szakirodalom alapján az új generációk tanulási szokásait, igényeit;[7] ezek a hagyományos, frontális megoldásoktól való elszakadás irányába mutatnak.[8] Molnár az NKE RTK-n a Covid–19-pandémia idején kötelezően bevezetett digitális oktatási megoldásokra adott tanári visszajelzéseket mutatja be olvasmányos módon, vállaltan szubjektív formában, átfogó képet adva e módszerek nehézségeiről és lehetőségeiről. A naplóbejegyzés formában megírt beszámolókból kiviláglik, hogy a digitális oktatás során is szükség van a tanár útmutató, értékközvetítő szerepére, és a legfőbb hozzáadott értéket a hallgatóság véleményalkotó gondolkodásának, interakcióra való nyitottságának bátorításán keresztül lehet megteremteni. A digitális megoldások tehát szerencsés esetben nem helyettesíthetik, hanem kiegészítik a jelenléti képzéseket, ahol a tanár személyes emberi kapcsolaton keresztül is lehetőséget kap a motiválásra, értékközvetítésre, támogatásra, ahol kereteket tud biztosítani a tanuláshoz.

Az interaktív, cselekvésen alapuló képzési módszerek alkalmazhatóságát vizsgálja Stréhli[9] a közigazgatásban és a rendvédelemben a vezetőképzés során, és beszámolója alapján az akciótanulás hatékonyan alkalmazható e területen. A coaching szemléletű softkompetencia-fejlesztés ugyancsak képes hozzájárulni e szférában a vezetők hatékonyságának fejlesztéséhez.[10] A tréningek létjogosultságát támasztja alá a rendészeti

3 Barnucz–Uricska 2021.
4 Havasi 2021.
5 Kertai et al. 2021.
6 Adamik et al. 2021.
7 Belényesi et al. 2018.
8 Molnár 2021.
9 Stréhli 2022.
10 Paksi-Petró – Stréhli 2021.

képzések palettáján[11] Fekete–Bajnok–Hegedűs tanulmánya is, hiszen a köz szolgálata óhatatlanul megköveteli a szociális készségek fejlesztését, aminek a leghatékonyabb eszköze a gyakorlati megtapasztalás és a tanulságok közös feldolgozása, beépítése, ami a tréning lényege. A tréningmódszertan nemcsak a társas készségek támogatása, hanem a pályaszocializáció elősegítése terén is hasznos eszköz lehet a nemzetbiztonsági pályakörre való felkészítés során.[12] Ezt a betanulás alatt kiegészítik a munkakörelemzések során azonosított kritikus munkaköri kihívásokat dramatizáló helyzetgyakorlatok saját élményű lejátszásán alapuló képzési formák is, ahol a résztvevők valós műveleti tét nélkül próbálhatják ki és gyakorolhatják a civil szakmai sémáiktól eltérő, professzionális szakmai reakciókat igénylő megoldásokat, akár videó-visszajelzés mellett is. A helyzetgyakorlatok kialakításának és az élményanyag feldolgozásának részleteit ismerteti az integritásképzés példáján keresztül Horváth tanulmánya.[13]

A szakirodalom áttekintése alapján látható, hogy az újszerű képzési megoldások egyik vonulata a digitalizált tartalmak bevonásán alapszik, míg a másik a szociális készségek gyakorlatias, cselekvésen keresztül megvalósuló, kooperatív tanulási módszereinek alkalmazására összpontosít. Mindkét esetben a hagyományos, tisztán elméleti és frontális oktatási módszerektől való elszakadás motívuma van jelen, ami felveti, hogy az igazán korszerű és hatékony képzésekre sokkal jelentősebb erőforrást szükséges fordítani, mint azt megszoktuk. Legyen szó ugyanis akár jelenléti, akár digitális képzési megoldásokról, az oktatás megtervezése során figyelemmel kell lenni arra, hogy az oktatás kellő mélységben hasson, azaz lehetőség szerint minden olyan idegrendszeri szintet vonjunk be a tanulási folyamatba, ami a fejleszteni kívánt ismeret, készség, képesség megnyilvánulásában szerepet játszik.[14]

A Nemzetbiztonsági Szakszolgálat képzési és továbbképzési rendszerének kialakítása során ezeket a szempontokat tartottuk szem előtt.

A továbbiakban összefoglaljuk a saját tapasztalatainkat az új képzési módszerek alkalmazásával kapcsolatban.

A tréningmódszertan sajátosságai

A nemzetbiztonsági pályakör sajátságos kihívásokkal szembesíti a pályára lépő munkatársakat, amelyekre az iskolarendszer és a korábbi munkahelyek nem képesek maradéktalanul felkészíteni őket. Van ugyan lehetőség a Nemzeti Közszolgálati Egyetem polgári nemzetbiztonsági alap- és mesterszakán célirányos felkészítésben részesülni, ám ez a lehetőség csak a már rendvédelmi pályán elindult jelentkezők számára nyitott. Szükség van tehát olyan képzésekre, amelyek segítenek összehangolni a pályakör és a pályára lépők elvárásait, viszonyulási módjait, értékeit.

A pszichológiai műveltség fejlesztése 20–25 évvel ezelőtt még nálunk is elméleti előadásokkal, jegyzettel és vizsgával vette kezdetét, ám 12 évvel ezelőtt elszakadtunk ettől a szemlélettől, és az elméleti ismeretanyagot ismeretterjesztő irodalomként már csak

11 Fekete–Bajnok–Hegedűs 2023.
12 Horváth 2015.
13 Horváth 2018.
14 Horváth 2022.

opcionálisan olvasgatják munkatársaink; a képzés veleje a gyakorlatifeladat-megoldáson, közös megbeszélésen keresztül valósul meg, tréning formájában. Az elmúlt években erőfeszítéseket tettünk az egyéni és társas kompetenciák fejlesztése érdekében, mára már változatos tréningkínálatot biztosítunk munkatársaink számára. Ön- és emberismeret, együttműködés, csapatépítés, konfliktuskezelés, érvelés- és tárgyalástechnika, kommunikáció, ügyfélszolgálati kommunikáció, a titok kommunikációs védelme, kreativitás, rendszergondolkodás, stresszkezelés, prezentáció, tanulásmódszertan, mentorképzés, integritás, nemzetbiztonsági etika és egyedi igényekre szabott további tréningek állnak rendelkezésre.

A tréning interaktív, bevonáson és gyakorlati magtapasztaláson, majd megbeszélésen és tudatos feldolgozáson alapuló képzési módszer. Előnye, hogy sokkal mélyebben bevonja a tanulási folyamatba a személyiséget, mint az elméleti ismeretátadás. Hátránya, hogy viszonylag kis létszámú csoportokban hatékony, így az egy oktatott munkatársra jutó fajlagos tanterem- és oktatóigény magas. 10–14 főnél nagyobb csoportban túl hosszú ideig tart, amíg mindenki meg tud szólalni, így vontatottá válik a munka. A csoport összetétele is meghatározó; a tagok nemi, életkori, státusz szerinti összetétele igen fontos dinamikai tényező, ezért lehetőség szerint a szervezésnél ezekre is oda kell figyelni. Tíz fő körüli létszámmal még a rövid távú memória kapacitása korlátjainak közelében mozgunk, meg tudjuk jegyezni, ki mit mondott, csinált. Minden emberre külön-külön oda kell figyelni, nem úgy, mint egy előadás során. Ez a befektetés azonban megtérül, hiszen a tréningek a képzési eredményeken túl szervezetfejlesztési potenciált is hordoznak magukban, segítenek a problémák felszínre hozásában, diagnosztizálásában és a megoldások alapjainak kidolgozásában is.

Mára elértük, hogy az állomány megismerte és megszerette a tréningeket, így a személyes bevonódás eléréséhez szükséges nap eleji „felmelegedés" kevesebb időt vesz igénybe. A tréning során olyan tudatállapotot kell kialakítani, amely alkalmas az új ismeretek, készségek befogadására. E nyitottság része, hogy el kell engedni a munkahelyi gondokat, amelyek foglalkoztatják a résztvevőket. A folyamat elején – szükség esetén – a jégtörő gyakorlatok kapcsán teret kell engedni a „ventillációnak", azaz ki kell tudni szellőztetni a fejüket. Igénylik, hogy valaki meghallgassa mindazokat a témához kapcsolódó szervezeti problémákat, amelyeket máshol nem mondhatnak el. Ezt a fázist nem szabad túlzásba vinni, mert könnyen elszabadulhatnak az indulatok, de a tréner hitelességét, a bizalmat megalapozza, ha képes empatikusan meghallgatni ezeket, tud valami megnyugtatót mondani, például a felvetett problémákat időről időre anonim módon összegezve javaslat formájában felterjeszti a szervezet döntéshozói felé. Ez a felszínre kerülő érzelmi feszültség adja meg az alapját annak a csoportdinamikának, amelyre a tanulási folyamat során építeni lehet. A lényeg, hogy minden résztvevő érzelmekkel és gondolatokkal vonódik be a közös munkába, senki sem marad kívülálló, mindenki véleménye számít, mindenkit demokratikusan meghallgatnak. Nem kell mindenben egyetérteni, sőt, helye van az ellenvéleménynek is. Ki kell alakítani a párbeszéd kultúráját a vitával szemben. A tréner moderálja, mederben tartja a kommunikációt, megszólítja a csendeseket, szabályozza a hangosak megnyilvánulásait, azaz összefoglalja, témára vonatkoztatja és lezárja az elburjánzó gondolatsorokat, anekdotákat. Ha leül a dinamika, izgalmas gyakorlatokkal, vitaindító témákkal felpörget, ha túl nagy a hév, összegez, racionális síkra hoz, értelmez,

lenyugtat. Ideális esetben a bevezető szakasz végére mindenki „átesik a tűzkeresztségen", megszólal, megnyilvánul, szerepel.

Ezt követik az olyan feladatok, amelyek játékos formában hoznak tanulságot, előhozzák a szabad gyermeki ént, amely nyitott szívvel képes befogadni az új tanulságokat a képzés során. A gyakorlatok stimulusokként, impulzusokként lehetőséget teremtenek helyzetek átélésére és tudatos szintre hozására, megbeszélésére. Olyan helyzetek ezek, amelyek során a hétköznapi élet valamely paraméterét mesterségesen megváltoztatjuk, ezáltal tudatosodik annak a tényezőnek a szerepe. Például, ha úgy kell megoldani egy feladatot, hogy közben nem lehet beszélni, akkor világossá válik a verbalitás fontossága, ám egyben nő az érzékenység az alternatív kommunikációs lehetőségek irányába is. A játék során elkerülhetetlen a frusztráció, a kudarc, ám ezeket az élményeket is be lehet, be kell forgatni a dinamikába és a tanulságok levonásába. Ugyancsak fontos, hogy minden esetben a munkahelyi kontextusra is vissza kell kötni a tanultakat. Mihez hasonlít ez a szervezeti viszonyokra vetítve, hogyan lehet elkerülni a való életben ezeket a buktatókat, mit lehet tenni a hatékonyság érdekében? Minden tréningblokk egy-egy fontos üzenet köré kell hogy épüljön. A gyakorlatok és a tréneri szerep moderációs aspektusának célja, hogy ezeket az üzeneteket átadja, megértesse, és gyakorlatban használhatóvá tegye. A tréning csak akkor éri el a célját, ha az üzenetek célba érnek, ha tudatos szintre emelkednek, ha záráskor tanulságként meg lehet őket fogalmazni, mielőtt mindenki visszamegy a feladatkörébe dolgozni. Nem minden üzenet vezet azonban azonnali viselkedésváltozáshoz. Van, hogy tudati szinten megszületik a megértés, de érzelmi szinten több idő kell annak beépítéséhez. Ilyenkor úgy működik a tréning, mint a kiskertben a magok ültetése. Az üzenet bekerül a talajba, kap egy kis megerősítést (vizet és fényt), de kicsírázni, szárba szökni csak később fog, a hétköznapok során. Sok esetben évekkel később jönnek vissza munkatársak és mondják, hogy hajdan történt vagy elhangzott valami egy tréningen, és annak hosszabb távon lettek mélyreható eredményei.

A tematikában megtervezett feladatokra sok esetben nem marad idő a nap során, de ez nem baj. Alapszabály, hogy nem mi vagyunk a feladatokért, hanem azok vannak értünk. A lényeg a beszélgetés, amelyet elindítanak. Ha már kevés feladat is bőséges élményanyagot és véleményt képes a felszínre hozni, a foglalkozás elérte a célját. A résztvevők nem a trénertől tanulnak, hanem a tréner által egymástól. A tréner a kereteket adja, a folyamatokat szabályozza. Az egyes feladatok olyanok, mint az üres poharak: önmagukban nem érnek sokat, tele kell őket tölteni tudással – és ez a résztvevők dolga. A tréner nem elmondja a témához kapcsolódó elméleti ismereteket, hanem olyan kérdéseket tesz fel, ami által – a feladatok átélt élményanyagához kötve – ráébreszti a résztvevőket, hogy mi a fontos tudnivaló, hogyan működik a jelenség. A tréner elméleti felkészültsége ennek ellenére kardinális jelentőségű. Hiányában maradhat puszta játszadozás a tréning, hiszen ha nem tereli a megbeszélést a megfelelő tanulságok irányába, akkor végül nem áll össze az ismeretek köre értelmes egésszé. Ugyancsak meddő, ha a tréner mindent elmond, és nem enged teret – például az idő rövidsége miatt – a csoport immanens tudásának, hogy felszínre törjön. Sokkal jobban megjegyzik a résztvevők a saját maguk által kimunkált igazságokat, mint a trénertől készen kapottakat. A résztvevői hozzászólások mennyisége kulcsfontosságú. Kezdetben csak a legbátrabbak mernek megszólalni, majd az általuk elmondottakra tudnak rákapcsolódni az óvatosabb résztvevők, de akár egyetértenek, akár nem a korábban elhangzottakkal, igényük keletkezik arra, hogy ők is elmondhassák, ami

eszükbe jutott. A folyamat olyan, mint a pattogatott kukorica a mikrohullámú sütőben. A trénernek az elején türelmesen kell várni a megnyilvánulásokat, nem szabad feladnia, túl aktívvá válnia, bírnia kell a csendet, ha kínos is. Amikor aztán beindulnak a hozzászólások, termékeny szakasza következik a megbeszélésnek. Ha viszont már kezdik ismételgetni a már elhangzottakat, nem jönnek új, eredeti gondolatok, érdemes véget vetni a megbeszélésnek és új témába kezdeni, mert unalmassá válik, elvész a dinamika (az analógiára vonatkoztatva: megég a kukorica). Jó arány- és ütemérzék szükséges e folyamat szabályozásához.

Mindezekből látható, hogy a tréneri szerepkör bizonyos szempontból sokkal nagyobb felkészültséget igényel, mint az előadói. A trénernek észlelnie és kezelnie kell minden résztvevő reakcióit, amihez magas szintű érzelmi intelligenciára van szükség. Érzékenynek kell lenni a nonverbális jelzésekre, rezdülésekre, észre kell venni, ha valaki lemaradt, nem érti vagy nem ért egyet. A kezeletlen kétkedőket menet közben könnyű elveszíteni. A „kognitív válasz" elmélet értelmében[15] nem arra emlékszünk, ami elhangzott, hanem arra, amilyen gondolatot az kiváltott belőlünk. Ha az ellenvéleményre nem kapunk megnyugtató választ, csak annyi fog megmaradni, hogy a trénernek nem volt igaza, és mi tudtuk jobban. Ha viszont a tréner veszi a fáradságot és vállalja a kockázatot, hogy feltárja a kétkedő résztvevő gondolatmenetét, kognitív sémáit, hiedelmeit, és megkeresi benne azt a pontot, ami hiányzik az új gondolat megértéséhez, akkor segíthet abban, hogy helyre kerüljenek az ismeretek, és valami új szempontot sikerüljön beépítenie a kevéssé nyitott résztvevőnek. Ehhez mély empátia, tapintat, tisztelet kell, hogy a meggyőzés során valóban létrejöjjön a résztvevőben a ráébredés, és ne csak kényszerű igazodás történjen részéről a konfliktus elkerülése érdekében.

A tréning során a résztvevők lelki egészségéért a tréner a felelős. A tanulás érdekében ki lehet tenni a résztvevőt „keményebb" helyzeteknek, de csak a teherbírása erejéig. Az énképet kell egy kicsit feszegetni, de nem lehet durván szembesíteni, hiszen nyilvános helyzetről van szó. A folyamat elején a működési szabályok megbeszélése során mindig elhangzik, hogy tiszteletben tartjuk egymás érzéseit, véleményét, nem bántunk meg senkit, csoporttitokként kezeljük az elhangzottakat. Ez a trénerre különösen vonatkozik. A tréner a csoport vezetője, ám ezt szelíd eszközökkel kell elérnie, sosem a domináns és nem együttműködő tagok rovására, velük konkurálva és őket letörve. Sokkal eredményesebb az ilyen csoporttagokkal a közös nevezőt megkeresni, és ezek mentén megerősíteni a kapcsolódási pontokat, tiszteletben tartva a presztízsigényüket, meghagyva informális vezetői szerepüket. Az ilyen módon pozitív, támogató szerepbe emelt csoporttagok rengeteget tudnak adni a csoportnak, hiszen tekintélyük a tanulás szolgálatába áll, mintát adnak arra, hogy lehet véleményt változtatni, mert az nem a gyengeség jele, hanem éppen hogy a fejlődésre való képességé, az erőé.

A tréner tehát a személyiségével dolgozik. A tréner mint a csoport vezetője csak akkor lehet eredményes, ha önazonos, hiteles. Hibázhat. De tudnia kell elismerni ezt. Önreflexívnek vagy akár önkritikusnak kell tudnia lenni. Hiszen ezt várja a tréningen részt vevőktől is. Nemcsak tanít, hanem példát is mutat. Valamilyen mértékben transzparenssé kell válnia, fel kell tárnia a saját személyes véleményét, élettörténetét, gyarlóságát, hibáit, erőfeszítéseit, eredményeit. Ettől lesz hiteles, így mutatja meg, hogy ő is ember,

[15] Petty–Cacioppo 1981.

így csökkenti a görcsöt a résztvevőkben, hogy ők vajon képesek lesznek-e majd fejlődni. A megközelíthetetlen, elérhetetlen, omnipotens tréner képe egyenesen destruktív. A trénernek kell élen járnia azokban a kérdésekben, amelyeket tanít. Ha önismereti vakfoltjai vannak, könnyen belesodródik és belemerevedik konfliktusokba; ha nincs önbizalma, egy-egy provokáció kapcsán megsértődhet, ami ebben a szakmában megengedhetetlen, mert erősen korlátozza további nyitott önfeltárás és visszajelzés lehetőségeit csoporton belül. Hiába papol egy tréner és sorolja az asszertív kommunikáció szabályait, ha aztán gyakorlati szituációkban alámegy a helyzetnek, vagy pedig agresszívan letorkolja valaki ellenvéleményét. A trénernek nemcsak a szavai, hanem a tettei is a résztvevők fejlesztését szolgálják, hiszen a személyes példa erősebb, mint a kimondott szavak, az utánzáson alapuló tanulás erősebb, mint a hallott ismeretek beépítése, a példaképpel való azonosulás pedig még ennél is mélyrehatóbb változásokat képes előidézni.[16]

Ugyancsak alapfeltétel a lelkesedés. „Égni kell, ha gyújtani akarsz." Csak olyan terméket tudsz hitelesen értékesíteni, amiben hiszel, amit te is használsz, amiről tudod, hogy értékes és jó, ami megéri az árát. Mert a résztvevőknek árat kell fizetniük a tanulás során. El kell engedniük azokat a biztonságot adó megoldási módjaikat, amelyeket eddigi életük során elsajátítottak, amelyekbe kapaszkodhatnak. Ahhoz, hogy ezt megtegyék, tudniuk kell, hogy amit kapnak, jobb. Látniuk kell egy sikeres embert, aki ezeket alkalmazva boldogul az életben. És ezt a sikert nem lehet megjátszani, előadni, valamilyen szinten karizmatikusnak is kell lenni. A trénernek valóban – és a szó szoros értelmében – boldogulnia kell azzal a szociáliskompetencia-csomaggal, viselkedési eszközkészlettel, tudáskinccsel, amellyel házal. Ezt a sikert és elégedettséget kell hogy sugározza a fellépése, megjelenése, testi-lelki fittsége, harmóniája. Nem státuszszimbólumokról van szó, hanem személyes stílusról. Ez lehet hivatalos, komoly, tudományos vagy közvetlen, szabados, humoros, a lényeg, hogy belülről fakadó, ne pedig felvett legyen.

A kreativitás, problémamegoldás ugyancsak nélkülözhetetlen tréneri erény. Sok esetben nem ideálisak a feltételek, nem áll rendelkezésre minden feltétel, ahogy az életben sem. Tudni kell abból főzni, ami van. Ha például épp nincs tábla a teremben, nem állhat meg az élet, az ajtóra is fel lehet fogatni a flipchart papírt. Az ilyen megoldások üzenete a csoport számára, hogy nincs kifogás. Minden megoldható, csak akarni kell. A siker nem a tárgyi feltételrendszer függvénye, ki lehet lépni a megszokott megoldások köréből. A tréneri szerepkör egyfajta rugalmasságot igényel, ami megnyilvánul a keretek szabályozása során is. A tréner felelőssége, hogy a tréning mederben maradjon, de vannak helyzetek, amikor tudni kell eltérni a tervezettől. A keretek biztonságot adnak, de korlátokat is jelentenek. Van, hogy beindul egy ígéretes, nem várt folyamat, aminek teret kell engedni, de ez azzal jár, hogy el kell térni a tervektől. Van egy tanulság, ami körvonalazódott ugyan, de nem teljesen vált érthetővé, ezért kell még egy gyakorlat, ami megerősíti azt, és nem volt tervben. Különösen akkor nehéz jól (a tagok számára észrevétlenül) menedzselni egy ilyen helyzetet, ha két tréner együttműködésével valósul meg a tréning. Ilyenkor a ko-trénernek majdhogynem szavak nélkül kell tudnia érteni, mit fog kihozni a helyzetből a társa. Ez nem lehetetlen, ha ugyanazok a szakmai sémák állnak a rendelkezésükre, mindketten értik a folyamatot, és ugyanarra a következtetésre jutnak. A két tréner ilyenkor kvázi „szavalókórusban" tud együttműködni. Az egyik feldobja a labdát, a másik lecsapja. Az egyik figyel a feladat levezetésére, a másik

[16] Ranschburg 2014.

a résztvevők reakcióira. Ketten együtt, rugalmasan igazodva a helyzethez új szintre tudják emelni a képzést, hiszen összhangjuk önmagában is példa a csoportnak az együttműködésre.

Összefoglalva: a tréning mint képzési módszer sokkal kevésbé szapora, mint az előadás, de sokkal mélyrehatóbb attitűd- és viselkedésváltozást képes előidézni. Különösen a fiatal munkavállalók szocializációjának támogatása során van ennek jelentősége, de a vezetőképzés is olyan szerepváltást támogat, amelynek óriási jelentősége van a szervezet jövője szempontjából, így megéri energiát fektetni az akciótanuláson, kooperativitáson alapuló kompetenciafejlesztésbe.

Nem betenni, hanem kivenni, avagy szemléletváltás az angol nyelv oktatásában

Az angol nyelv mára univerzális kommunikációs kapocs lett a nemzetek között. Bolygónk 8 milliárd lakója közül 360 millió beszéli anyanyelvként, és további egymilliárd ember második nyelvként használja, elterjedt és meghatározó a szerepe a tudományban, technológiában, művészetben, szórakoztatóiparban.[17]

Munkahelyi kontextusban azért nélkülözhetetlen az angol nyelv ismerete, mert a partnerszolgálatokkal való kapcsolattartás, az EU-munkacsoportokban való aktív részvétel, a beszerzett speciális eszközökhöz kapcsolódó oktatások, a felhasználói útmutatók jellemzően angol nyelvűek. A szervezeten belüli nyelvoktatás előnye, hogy célirányosan, testreszabottan készít fel a nyelvhasználatra, figyelembe veszi a szakmai közeget, annak egyedi terminológiáját, élethelyzeteit, tipikus idegen nyelvi kihívásait, illetve szervezeten belül – a titkosság és konspiráció kritériumára tekintettel – azért lehet a munkáról is beszélni.

Az alfejezet címe magyarázatot igényel. A tanulási folyamatnak három fontos szakasza van. Az első a kódolás, ezt követi a tárolás, majd végül az előhívás.[18] A hagyományos nyelvoktatás az első kettőre helyezi a hangsúlyt, és a harmadik szakasz jellemzően a számonkérés során jelenik meg, noha a nyelv gyakorlati felhasználásának szintjén éppen az előhívás kerül fókuszba, így ezt is külön gyakorolni kell. Olyan ez, mint amikor egy hosszú útra készülődvén az utazó igyekszik mindenre gondolni, teljeskörűen bepakolni, gondosan hajtogatva, tömörítve, semmit sem kifelejtve, maximalista hozzáállással elvégezni a feladatot. Amikor aztán az utazás során szükség van valamire, akkor hiába keresi, túrja fel a bőröndöt, nem tudja, hol keresse a szükséges tárgyat, így tulajdonképpen feleslegesen dolgozott, mert mire megtalálja, már késő. Így van ez a nyelvi tudással is. Gondosan tanuljuk a nyelvet, bevéssük, majd részletekben megtanuljuk előhívni (témazáró dolgozat, szódolgozat, felelés), de amikor hirtelen alkalmazni kellene egy élethelyzetben, nem tudjuk, hirtelen hova nyúljunk. Mert nem csak pakolni, „betenni" kell, hanem azt is gyakorolni kell, hogyan lehet előhívni, azaz „kivenni" a tudást. A nyelvtanfolyamok

[17] Lyons 2021.
[18] Melton 1963.

ezt a mozzanatot is célul tűzhetik ki, hiszen ez sem ér kevesebbet, mint a bevésés, sőt, nélküle nem is lehet teljes a tanítás.

A szervezeten belüli angol nyelvi képzések terén 20 évvel ezelőtt még jellemző volt, hogy kezdő szinttől kellett felépíteni a nyelvtudást, ezért munkaidőben 400-500 órás nyelvtanfolyamok indultak, heti kétszer fél napra kivonva a résztvevőket munkafeladataikból. Előzetes nyelvismeret hiányában a jellemzően fiatalfelnőtt-korú résztvevőknek nehéz volt bármihez is kötni a nyelvtani szerkezeteket, szavakat, így komoly erőfeszítést igényelt részükről a nyelvtanulás, amely kereskedelmi forgalomban kapható kurzuskönyvek felhasználásán alapult, a bevésést támogatta. A tanfolyam zárásaként kötelezettség volt a nyelvvizsga megszerzése, a további nyelvhasználatot azonban nem támogatta a szervezet.

Mára megváltoztak a körülmények, a lehetőségek és a felhasználói igények is. Nőtt az általános leterheltség, kevesebb lehetőség van tartósan kimaradni a munkafolyamatokból, emellett a fiatalabb generációk jellemzően kevésbé hosszabb távon gondolkodnak, instant megoldásokat keresnek a tartós energiabefektetés helyett.[19] Ugyancsak jellemző, hogy az iskolarendszert elhagyó fiatal munkatársak már eleve használható nyelvtudással rendelkeznek, így nem a tudásfelépítés, hanem a szinten tartás, a szaknyelvi jelleg és a nyelv gyakorlati alkalmazása került előtérbe.

Eközben a nyelvvizsga helyett a gyakorlati helyzetekben használható tudás lett a fontos. Korábban a nyelvvizsga révén bizonyos szempontból mérhetővé vált a tudásgyarapodás, és elszámoltathatóvá tette a résztvevőket; a munkáltatótól megkapott támogatások fejében tanulmányi szerződés megkötésével, visszafizetési kötelezettség mellett kellett vállalniuk a sikeres nyelvvizsgát. Ez egyrészt görcsös, stresszes felkészülést eredményezett, másrészt pedig a megszerzett tudás életszerűségét rontotta. A nyelvvizsga-felkészítés ugyanis egy egyetemi vizsgára való felkészítéshez hasonlít, ahol tételeket kell kidolgozni és megtanulni, feladattípusokat kell begyakorolni a siker érdekében, de az már nem szempont, hogy egy gyakorlati élethelyzetben milyen lesz a spontán beszédprodukció. Érdekes tapasztalat, hogy a nyelvvizsga-kötelezettség mellőzése nem rontotta a tanfolyamok sikerét. A résztvevők oldottabban tanulhattak és kvázi „mellékhatásként" minden esetben ugyanúgy le tudták tenni a nyelvvizsgát, hiszen használható nyelvtudásra tettek szert a hosszú tanfolyamok alatt.

A hosszú tanfolyamokon azonban a szűk oktatói keresztmetszet miatt csak kevesek jutottak hozzá a belső nyelvi képzéshez, meg kellett várni, míg kifutnak a csoportok, így évekig tolódhatott a beiskolázás, noha a szükség a nyelvtudásra folyamatosan fennállt. Az elmúlt 10 évben kialakított új tanfolyamtípusainknak köszönhetően kéthetes és háromnapos szuperintenzív szinten tartó angol nyelvi kurzusokon, illetve egyéni és páros felkészítéseken rotálva már a korábbi létszámok többszöröse jut nyelvi képzéshez. A szinten tartás alapfeltétele persze az, hogy legyen egy előzetes tudásszint, így minden kurzus első lépése a szintfelmérés, azaz egy standardizált feladatsor önálló kitöltése, valamint egy szóbeli elbeszélgetés a nyelvtanárokkal. E felmérések eredményei alapján osztjuk be a tanulócsoportokat, amelyek ideális esetben hatfősek. Ez egyrészt a tantermeink kapacitásához igazodik, másrészt ekkora létszám mellett biztosítható csak, hogy minden résztvevő aktívan bevonható legyen a kommunikációba. A nyelvtanárok a csoportok összeállítása során a tudásszint mellett odafigyelnek

[19] Belényesi et al. 2018.

a szakterületek keveredésére, a résztvevők személyiségjegyeire, nemi összetételére is, hiszen a csoportdinamika is része a tanulási folyamatnak. Ha például túl sok introvertált, egyoldalú érdeklődésű, hasonló szemléletű vagy azonos nemű tag van a csoportban, az csökkentheti a beszélgetés változatosságát, gördülékenységét. A hatfős létszám lehetőséget ad a kiscsoportos és a páros feladatok végrehajtására is, helyet kapnak az egymásra odafigyelést, ráhangolódást segítő érzékenyítő gyakorlatok is, de vannak versengést elősegítő, dinamikát fokozó helyzetek is, amelyeket szükség szerint lehet adagolni. A cél, hogy a csoportdinamika optimális szinten maradjon, ne legyen se túl csekély, se túl intenzív, azaz fenn lehessen tartani a csoport optimális működését, a kommunikáció életszerűségét és folytonosságát.

Az eddigiekből látható, hogy az angolnyelv-tanár ebben a szerepkörben kvázi tréneri szemlélettel vezeti a csoportot. Nem egy esetben magyar nyelvű tréninggyakorlatokat dolgoztunk át angol nyelvre, hiszen a cél mindkét esetben ugyanaz: gyakorlati feladatok helyezetin keresztül kommunikálni és közösen tanulni.

A nyelvtanár szerepe eközben átalakult. Már nem az a cél, hogy a nyelvtani szerkezeteket elmagyarázza, megmondja, melyik szó mit jelent, dolgozatokat írasson és javítson, és pláne nem az, hogy a beszéd közben felmerülő helytelenségeket menet közben kijavítsa, amivel csak a gátlásokat erősítené. Sokkal inkább az, hogy stimulusokat adjon, alkalmat teremtsen a beszélgetésre vagy akár vitára, amelyekbe a résztvevők önként és kényszer nélkül be akarnak vonódni, pusztán azért, mert érdekes a téma, és artikulálni akarják a véleményüket, be akarnak szállni a beszélgetésbe. Mert így működik a nyelv, erre való. Így lesz életszerű az oktatás is. Eközben a tanár feladata, hogy olyan feladathelyzeteket teremtsen, amelyek játékos formában bevonják a résztvevőket, illetve kérdéseket dobnak be, kérdezésre biztatják a résztvevőket, hogy egymást szólítsák meg, ne a tanáron legyen a figyelem fókusza. Olyan feladatok is vannak, amelyek az elakadások kezelésére tanítanak, például egy elfelejtett szót körülírni, hogy aztán folyhasson tovább a beszélgetés, ne kelljen kiszólni a helyzetből, a tanár segítségét kérve, hiszen erre nincs lehetőség a való életben sem. Több esetben csodálkoznak rá akár alacsonyabb nyelvi szinten álló csoportok tagjai is utólag, hogy észre sem vették, de három napig megállás nélkül, folyamatosan angol nyelven beszélgettek. És közben rengeteget fejlődnek, hiszen nem az számít, hogy a mondatszerkezet döccent-e, vagy a megfelelő szót, a megfelelő igeidőt alkalmazták-e, hanem az, hogy el tudták-e mondani, amit akartak, és a többiek megértették-e, tudtak-e kapcsolódni hozzá. Ennek a megtapasztalása az, ami katartikus erejű, és igazi paradigmaváltást hoz a nyelvhasználat terén.

Ez persze nem jelenti azt, hogy teljesen elmaradnak a tanári magyarázatok. Egy-egy nyelvtani szerkezet, igeidő, témakörhöz tartozó szókincs ugyanúgy tárgya az oktatásnak, de már nem ez az elsődleges, illetve ezeket nem feltétlenül kell a tanfolyam hasznos idejéből elvenni.

A kurzusok közötti időszak is a tanulási folyamat része, de ahhoz, hogy a tanár felügyelete és jelenléte nélkül is folyamatos legyen a tanulás, motivációt kell teremteni. Az egyik ilyen motiváció, hogy a következő jelenléti tanfolyamokon a „házi feladatként” feladott anyagok ismerete, alkalmazása szükséges ahhoz, hogy a résztvevő be tudjon kapcsolódni, és ne csak a fejét kapkodja, hogy a többiek miről beszélnek. Emellett persze az anyagok felépítése is azt támogatja, hogy a tanulás önjutalmazó jelleget öltsön a sikert jelző vizuális és hangeffektek alkalmazásával, ahogy teszik azt a népszerű internetes oldalak is.

Érdekességek, aktualitások, videómegosztókról kiválasztott tartalmak, kvízalkalmazások színesítik a kínálatot, számtalan gamifikált megoldás (például Wordwall, Kahoot, Quizlet). Több olyan felület áll a résztvevők rendelkezésére, ahol a tanár folyamatosan tananyagokat, hasznos linkeket, kvízeket oszt meg, ösztönözve az önálló felkészülést (például Redmenta, Classroom, Teams). A résztvevők az alkalmazások chatfelületén motiválják egymást és adnak visszajelzést a tanárnak, általuk fellelt hasznos tartalmakat, például közösségi videómegosztó portálok professzionális és szórakoztató tartalmait ajánlhatják egymásnak. Azaz azt teszik, amit az új generációk maguktól is szoktak: „nyomkodnak" és élvezik. A nyelvtanulás ilyen formában nem kényszer, hanem hobbi, amit lehet folytatni, ha van öt szabad perc, amit egyébként üresjáratban töltenének a szabadidejükben.

Az oktatásnak alkalmazkodnia kell a valós felhasználói igényekhez és kihasználni a technika adta lehetőségeket. Az interneten elérhető szolgáltatások fejlődésének köszönhetően az is átalakul, mire van valójában szüksége egy átlagos felhasználónak, munkatársnak, nyelvet tanulónak. Az online fordító alkalmazások, mesterségesintelligencia-szolgáltatások mára lehetővé teszik, hogy a levelezés során például kevésbé mély nyelvtudással is megértse egymást két különböző országban élő, más nyelvet beszélő együttműködő szakember, így ki lehet váltani az idő- és energiaigényes nyelvoktatás egy részét olyan készségek kialakítása révén, amelyek már inkább a digitáliskompetencia-fejlesztés körébe tartoznak. Tehát már nem feltétlenül kell mindent mélységében megtanulni a boldoguláshoz. Célirányosan lehet koncentrálni azoknak a nyelvi kompetenciáknak a fejlesztésére, amelyek közvetlen emberi interakciókhoz kapcsolódnak és egyelőre nehezen támogathatók instant technikai megoldásokkal, illetve a kommunikáció kapcsolati szintjének biztosításához nélkülözhetetlenek, mint például a beszédértés és beszédkészség. A nyelv eszköz a kapcsolódáshoz, így ezt a funkcióját kell erősíteni, hiszen ezt nem fogja tudni kiváltani gépesített megoldás.

Kritikaként merülhet fel, hogy ez a fajta, adott csoport igényeihez igazodó „kézműves" képzési tartalomfejlesztés rengeteg energiát igényel, amire a leterhelt tanároknak nincs idejük. Sokkal egyszerűbb készen kapott kurzuskönyvek, munkafüzetek jól felépített feladatsorai mentén megoldani az oktatási feladatokat. A válasz erre az, hogy a mai technikai lehetőségek mellett már csak a tanár digitális kompetenciájának hiányosságai szabnak gátat a tartalomfejlesztésnek. Temérdek anyag érhető el ingyenes formában az interneten, felhasználóbarát felületek támogatják a tanári munkát, a tananyagmegosztást, és már bárki számára elérhető mesterségesintelligencia-szolgáltatás, ami „asszisztensként" segítheti a tanári munkát, állíthat össze megadott egyedi tananyagból teszteket, feladatsorokat, és ezeket automatizáltan javíthatják online kérdőívkezelő alkalmazások, felszabadítva az értékes oktatói kapacitást olyan feladatokra, amelyek kevésbé automatizálhatók. Ezzel átalakul a nyelvtanári szerepkör, feleslegessé válnak olyan régen alapértelmezett munkaköri feladatok, mint például a tesztjavítás, ehelyett azonban elvárásként fogalmazható meg a képzések színvonalának fejlesztése, az interaktivitás, a kommunikációcentrikusság előtérbe helyezése.

Elektronikus megoldások az oktatás szolgálatában

Már a szakirodalom áttekintése során is láthattuk, hogy a 2020. évben kibontakozó világjárványnak nem csak negatív hatásai voltak. Mivel az új munkatársak rendszerbe illesztése nem állhatott le, ám nem lehetett az oktatókat és a hallgatókat fizikailag egy térben elhelyezni, a pandémia kényszerű szociális deprivációja katalizátorként hatott az elektronikus megoldások terjedésére az oktatásban is. E megoldások egy része a hagyományos, élő előadóval folyó oktatások elektronikus közvetítésén, a másik ága pedig az automatizált megosztású elektronikus tananyagok létrehozásán alapszik.

Az előadások szervezése során mára természetessé vált, hogy chatalkalmazások segítségével egymástól távol lévő emberek is fejlesztő interakcióba kerülhetnek egymással, kihasználva, hogy a verbális mellett a nonverbális kommunikációs eszközök nagy része ugyanúgy érvényesülhet a képernyőn keresztül is, mint élőben. A pandémiás korlátozások idején még kisebb létszámú tréninget is tartottunk ily módon, kihasználva, hogy a csoportmunka-támogató alkalmazások révén a résztvevők párokra vagy kisebb csoportokra oszthatók voltak, imitálva a jelenléti tréningek tipikus megoldásait. Az oktató és a résztvevők megoszthatták egymással a képernyőiket, közösen dolgozva a feladatok megoldásain, majd prezentálhatták ezeket a csoport számára, miközben az üzenőfalon azonnali visszajelzéseket, szavazásokat lehetett lebonyolítani. A jelenléti tréningek természetesen sokkal gazdagabb interakciókat tesznek lehetővé, így a kényszerhelyzet elmúltával már nem szervezünk online tréningeket, de érdekes tapasztalat volt, hogy még így is lehetett 70-80% hatékonyságú tréninget tartani, a résztvevőket a virtuális térben is csapattá lehetett kovácsolni.

Az elektronikus közvetítésekkel a tudáshoz való hozzáférés lehetőségei kibővültek. Mára minden szakmai tanfolyami előadást alapértelmezetten közvetítünk a belső hálózaton, így szervezeten belül – a továbbképzési pontgyűjtő kötelezettségének teljesítése érdekében – bárki bekapcsolódhat a folyó előadásokba. Ezzel javult az esélyegyenlőség, amennyiben például a központban dolgozó angolnyelv-tanárok szolgáltatásai is elérhetővé váltak a más objektumokban szolgálatot teljesítő munkatársaink számára. A megyei kirendeltségeken dolgozó új munkatársaknak sem kell már például a szakmai tanfolyam ideje alatt hónapokra elszakadniuk a családjuktól, nem kell minden héten több száz kilométert utazniuk és szállást foglalni a részükre, hiszen távolról is nyomon követhetik az előadásokat, elérhetik az e-learning-anyagokat, teljesíthetik a vizsgákat. Jelentős összegeket, valamint utazási időkiesést lehet tehát megtakarítani az online megoldások révén, amelyek a pandémia elmúltával is népszerűek maradtak.

Az előadások elektronikus felületen történő közvetítése mellett az intranetes felületeken közzétett tananyagok is hozzájárulnak a tudás széles körű hozzáféréséhez. A korábban papíralapon zárt kör részére sokszorosított és kiosztott felkészülési segédletek, szakmai jegyzetek helyett mára természetessé vált, hogy belső elektronikus felületeken osztjuk meg ezeket az anyagokat, jelentős mennyiségű papírt megspórolva, a környezettudatosság jegyében.

A tananyagok puszta megosztásán túl, a Moodle rendszer segítségével a tananyagokat kurzusokba rendezve, tudásellenőrző kérdéssorokkal támogatva, videóanyagokkal színesítve, elégedettségi kérdőívvel minőségbiztosítva kaphatják meg a hallgatók. A hosszú, összefüggő szövegből álló szakmai jegyzetek helyett a mai világban megszokott webes

tördeléssel, böngészhető formában, felbontva lehet az ismereteket átadni. Az írott anyagok mellett releváns témákban saját gyártású interjúk, podcastek is elérhetők, hiszen ezeket élvezetesebb feldolgozni, mint a hosszú, írott szövegeket.

Az írásbeli számonkérések ugyancsak erre a felületre kerültek át, így azokat – a vizsga tisztasága érdekében – vezetőjük ellenőrző jelenléte mellett saját szolgálati helyükön teljesíthetik. Előnye e megoldásnak, hogy – szemben a korábbi hosszadalmas kézi javítással – azonnali visszajelzést kapnak az eredményességről, a további tanfolyami szintekre bocsáthatóságról. A tesztsorok feladattípusai igen változatosak, a véletlenszerűsített feladatkiosztás révén pedig mindenki egyedi vizsgafeladatsorral szembesül.

Komplett tanfolyami szintek kerültek ezen a módon automatizálásra, így például a szervezetbe lépők önálló ismeretfeldolgozással, rugalmas időbeosztással készülhetnek fel a legalapvetőbbeket felölelő bevezető képzésük vizsgájára. Mivel ezt a képzést a felszerelést követően minél hamarabb kell elérhetővé tennünk mindenki számára, az elektronikus felületre való áthelyezés révén lényegesen leegyszerűsödött és személyre szabottá vált a folyamat, hiszen nem kell várni a szervezésre.

Az oktatásszervezők által összeállított Moodle kurzusok hasznos, könnyen módosítható eszközök, ám az automatizált ismeretátadás csúcsa a profi szakemberek által összeállított komplett e-learning-tananyagok világa. Ezek gondos előkészítést és nagy szakértelmet kívánnak. Az elméleti tananyagból képernyőkre bontott forgatókönyv készül, amely interaktív feladatokra bontja az egymásra épülő ismereteket, gazdagon illusztrál, bevon, gamifikált megoldásokkal versenyre ösztönöz, szórakoztat. Előnye, hogy a szolgálati feladatok mellett bármikor végezhető, menet közben megszakítható, majd rugalmasan folytatható. Nem igényel tantermet, oktatót, mégis tömegeknek biztosít akár rövid idő alatt is élvezetes, több érzékszervre ható, interaktív, gyakorlatias ismeretátadást. A Moodle rendszer részletesen naplózza a felhasználói tevékenységeket, így személyekre bontva vagy statisztikailag összesítve is kimutatás végezhető az eredményekről.

A szervezeti tanulástól a tanuló szervezetig

A személyzetfejlesztés és a szervezetfejlesztés kéz a kézben jár. Az egyik a szervezeti tanulás feltételeit teremti meg, a másik pedig a tanuló szervezetét. A tanuló szervezet a szervezeti kultúra sajátossága, a változó körülményekhez való alkalmazkodás képességét jelenti, a fejlődési potenciált, alkalmazkodó képességet szervezeti szinten.[20] Ennek ugyan része az, hogy a szervezeten belül döntési helyzetben lévők tanuljanak például korszerű menedzsmentismereteket, de a lényegi eleme mégiscsak az, hogy a szervezeten belüli emberi kapcsolatok lehetővé tegyék a közös célokért való önzetlen együttműködést, az egyéni érdekkörön túlmutató, bajtársias szemléletet. Ez nem áll távol a rendvédelmi szervek ethoszától.

A közelmúltban lezárult *Felhatalmazás kultúrája* projekt a példája annak, hogy az oktatás és a szervezetfejlesztés milyen szorosan összekapcsolódik. E-learning-anyagok, tréningek és roadshow jellegű interaktív előadások, belső normamódosítások, valamint a belső hálózaton közzétett, szervezet vízióját és küldetését artikuláló főigazgatói interjú együttesen

[20] Senge 1998.

teremtette meg az alapját annak, hogy a döntési szintek lejjebb szállhassanak a szervezeten belül, fejlődhessen a dolgozói felelősségvállalás, a „jó gazda" szemlélet, az innovációra való nyitottság. A szervezeti elemek szociometrikusan központi pozícióit betöltő munkatársainak részvételével megszervezett „véleményvezér"-tréningeken 10 csoportban több mint 100 fő mondhatta el őszintén a véleményét, hogy min változtatna szervezeti szinten. Javaslataik közül mindazokat, amelyek reálisan megvalósíthatók voltak, a felső vezetés tudatosan menedzselte, aminek köszönhetően mára a gyakorlatba ültettünk számos újítást. Az egyik ilyen a „Főigazgató válaszol" fórum, ahol anonim módon lehet szervezeti szinten közérdeklődésre számot tartó kérdéseket feltenni, amelyeket a főigazgató belső webes közvetítéssel megválaszol. Ez a fórum közvetlen kapcsolatot jelent a munkatársak számára a felső vezetéssel, megérthetik a szervezeti szintű szempontokat, ezáltal javul a kommunikáció és az elégedettség. A vezetés számára a problémák közvetlen megértése, az állomány számára pedig a vezetői gondoskodás megtapasztalása segíti egy élhetőbb, szerethetőbb szervezet kialakítását.

Összegzés

A polgári nemzetbiztonsági szolgálatok közös képzési és továbbképzési rendszere lehetőséget biztosít arra, hogy minden elektronikus vagy jelenléti, külső vagy belső tanfolyam, oktatás, konferencia részvételét elszámoljuk a pontgyűjtési kötelezettség keretein belül. Nagy kihívást jelent a képzési szakterületek számára a minőségi tartalomgyártás, illetve az egyre gyorsabban frissülő tudáskincs naprakész hozzáférhetővé tétele az állomány számára. Ha az elméleti tudás fejlesztésén túl akarunk mutatni, a mennyiségi követelmények mellett a minőségi kihívásoknak is meg kell felelnünk. Érdemi kompetenciafejlesztést csak gyakorlatias, életszerű, teljes személyiséget bevonó képzési formák alkalmazásával lehet elérni, ám ezek rendkívül erőforrás-igényesek. Idő, pénz, felkészült és elhivatott oktatói gárda, képzési infrastruktúra szükséges hozzájuk. Mára eljutottunk oda, hogy a polgári nemzetbiztonsági szolgálatok képzésért felelős munkatársainak már nem kell bizonygatniuk a felső vezetés felé, hogy a képzés fontos és munkáltatóként áldozni kell rá, hiszen minden támogatást megkapnak ehhez. De ez önmagában nem elég. Az állományban is ki kell hogy alakuljon az igény a képzésben való önvezérelt részvételre, a fejlődésre. A képzési szakterület feladata nem elsősorban a képzésekre kötelezés, hanem az érdeklődést keltő képzés lehetőségeinek megteremtése. Nem a mindent tudás és ismeretátadás, hanem a szakterületeken dolgozó tapasztalt szakemberek oktatásmódszertani és képzésszervezési támogatása, hogy minél hatékonyabban oszthassák meg munkatársaikkal a tudásukat. Az oktatás poroszos, hierarchikus felfogása helyett a partneri, kooperatív modell gyakorlatba ültetése.

Ennek szellemében a jövőben cél lehet például az open book vizsgarendszer bevezetése. Ennek lényege, hogy a szakmai tanfolyam záró szóbeli vizsgáján nem tételkifejtés, azaz a szakmai jegyzetben foglalt elméleti ismeretek emlékezeti tárból való előidézése a feladat, hanem gyakorlati feladathelyzetek megoldása a források felhasználásával. A való életben ugyanis nincs szükség arra, hogy valaki fejből előadást tartson egy-egy elméleti témakörből. Az ilyen tudás gyorsan megfakul, hiszen felesleges. Sokkal inkább arra van szükség, hogy ezt a tudást alkalmazni tudja a gyakorlatban, hogy a megoldás kidolgozása során tudja,

hol kell utánanézni a lényeges ismereteknek. Tehát a vizsgán egy szakmai helyzetet kap, a megoldásához használhatja a tananyagot, hiszen az életben is van ideje szakmai tervet készíteni. Ehhez tudnia kell, hogy a tananyag, a jogi szabályozók mely részei relevánsak, meg kell tudnia indokolni, miért azt a megoldást javasolja. El kell tudnia magyarázni, miért úgy kombinálta az ismereteket, miért azt az eszközkészletet látja célravezetőnek a helyzet megoldásához. Előzetes felkészülés nélkül szűk időkorlátok között ez nem megy, tehát tanulni továbbra is nélkülözhetetlen a vizsgára, de nem egy üres lap felett ülve kell felidéznie az egyes szakterületek szolgáltatásait, eljárásait, hanem életre kell tudni kelteni a tanult ismereteket, ahogy a megrendelőkkel való együttműködés során is képesnek kell lenni a szolgáltatások komplex szemléletű alkalmazására. Ez a vizsgaelrendezés szakít a vizsgabizottság hatalmi pozíciójával, ugyanis nem vitathatatlan ismeretanyagot kell visszaadni, hanem szakmai véleményt kialakítani és érvekkel alátámasztani a grémium előtt, ami sokkal demokratikusabb, partneribb viszonyt feltételez a hagyományos szituációhoz képest.

Felhasznált irodalom

Adamik Zsolt Leon et al. (2021): A pandémia okozta digitális átállás tapasztalatai a rendészettudományi oktatásban. *Rendvédelem,* 10(2), 185–221. Online: https://epa.oszk.hu/03300/03353/00018/pdf/EPA03353_rendvedelem_2021_2_185-221.pdf

Barnucz Nóra – Uricska Erna (2021): Kiterjesztett valóság és közösségi oldalak alkalmazása a nyelvoktatásban – különös tekintettel a rendészeti szaknyelvre. *Rendvédelem,* 10(2), 4–49. Online: https://doi.org/10.1556/2063.29.2020.4.9

Belényesi Emese et al. (2018): *Pedagógiai módszertani ismeretek a közszolgálati pályaorientációs képzés oktatói számára.* Budapest: Nemzeti Közszolgálati Egyetem. Online: http://hdl.handle.net/20.500.12944/12735

Fekete Márta – Bajnok Andrea – Hegedűs Judit (2023): Akciókutatás a rendészeti felsőoktatásban: egy tantárgyfejlesztés reflexiója. *Neveléstudomány,* 11(2), 20–31. Online: https://doi.org/10.21549/NTNY.41.2023.2.2

Havasi Sándor (2021): Az egyéni tanulás, gyakorlás és alkalmazás irányítása és segítése digitális eszközökkel. *Rendvédelem,* 10(2), 49–76. Online: https://real.mtak.hu/127283/1/Rendvedelem_2021_2_.pdf

Horváth Ferenc (2015): A pályaszocializáció pszichológiai kérdései a Nemzetbiztonsági Szakszolgálatnál. *Nemzetbiztonsági Szemle,* 3(1), 82–114. Online: http://hdl.handle.net/20.500.12944/10200

Horváth Ferenc (2018): *A közszolgálati etika elméleti és gyakorlati kérdései a Nemzetbiztonsági Szakszolgálatnál.* PhD-disszertáció. Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola. Online: https://doi.org/10.17625/NKE.2018.021

Horváth, Ferenc (2022): „From Top to Toe": Choosing the Appropriate Training Method. *Nemzetbiztonsági Szemle,* 10(3), 44–56. Online: https://doi.org/10.32561/nsz.2022.3.4

Kertai Bendegúz et al. (2021): Online tanítási – tanulási módszerek a rendészeti képzés gyakorlatába a COVID-19 járvány alatt. *Rendvédelem,* 10(2), 137–185. Online: https://epa.oszk.hu/03300/03353/00018/pdf/EPA03353_rendvedelem_2021_2_137-184.pdf

Lyons, Dylan (2021): How Many People Speak English, And Where Is It? *Babbel,* 2021. március 10. Online: https://www.babbel.com/en/magazine/how-many-people-speak-english-and-where-is-it-spoken

Lyons, Sean – Kuron, Lisa (2014): Generational Differences in the Workplace: A Review of the Evidence and Directions for Future Research. *Journal of Organizational Behavior,* 35(1), 139–157. Online: https://doi.org/10.1002/job.1913

Melton, Arthur W. (1963): Implications of Short-Term Memory for a General Theory of Memory. *Journal of Verbal Learning and Verbal Behavior,* 2(1), 1–21. Online: https://doi.org/10.1016/S0022-5371(63)80063-8

Molnár Katalin (2021): *4D. Diskurzus a digitális didaktikai diverzitásról.* Beszélgetőkönyv. Dunakeszi. Online: www.nyelvilektoralas.hu/wp-content/uploads/2012/05/4D-Besz%C3%A9lget%C5%91k%C3%B6nyv.pdf

Paksi-Petró Csilla – Stréhli Georgina (2021): Coaching szemléletű fejlesztés a közszolgálatban: Jó gyakorlatok, fejlesztési potenciálok a rendvédelemben és a közigazgatásban. *Belügyi Szemle,* 69(12), 2167–2187. Online: https://doi.org/10.38146/BSZ.2021.12.7

Petty, Richard E. – Cacioppo, John T. (1981): *Attitudes and Persuasion: Classic and Contemporary Approaches*. Dubuque: W.C. Brown Company Publishers.

Ranschburg Jenő (2014): *Szeretet, erkölcs, autonómia.* Budapest: Saxum.

Senge, Peter M. (1998): *Az ötödik alapelv.* Budapest: HVG.

Stréhli Georgina (2022): *Új utakon a közszolgálati vezetőképzés – Az action learning módszerének alkalmazási lehetőségei a közigazgatásban és a rendvédelemben*. PhD-disszertáció. Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola. Online: https://doi.org/10.17625/NKE.2023.017

Tartalom