

Marek Górka*
Ladislav Cabada**

Integration or disintegration? The Visegrad Group in the face of contemporary security policy challenges

Integracja czy dezintegracja? Grupa Wyszehradzka wobec wyzwań współczesnej polityki bezpieczeństwa

ABSTRACT:

The article analyses the political changes that have occurred since 2022 in the area of security and digital policy pursued by the Visegrád Group (V4) countries. By describing and analysing the main factors influencing the development of cyber potential and the political priorities outlined in strategic documents and V4 presidency programs, the study attempts to determine the positions of individual V4 members regarding digital policy. The comparative analysis allows the identification of conditions that may foster either integrative or disintegrative processes in the Central and Eastern European region.

KEYWORDS:

Visegrád Group (V4), regional integration, digital policy, cybersecurity, political integration and disintegration, digital transformation

* Marek Górka – Associate Professor, Koszalin University of Technology, Poland, ORCID: <https://orcid.org/0000-0002-6964-1581>, e-mail: marek_gorka@wp.pl.

** Ladislav Cabada – Professor, University of West Bohemia in Pilsen, Czech Republic, ORCID: <https://orcid.org/0000-0001-9604-0987>, e-mail: cabada@ff.zcu.cz.

STRESZCZENIE:

Artykuł analizuje zmiany polityczne po 2022 r., jakie zaszły w obszarze bezpieczeństwa i polityki cyfrowej prowadzonej przez państwa Grupy Wyszehradzkiej (V4). Opisując główne czynniki rozwoju cyberpotencjału oraz priorytety polityczne zapisane w dokumentach strategicznych i programach prezydencji V4, podjęta zostaje próba ustalenia postaw poszczególnych członków V4 w zakresie polityki cyfrowej. W wyniku przeprowadzonej analizy porównawczej możliwe staje się określenie warunków, które mogą sprzyjać procesom integracyjnym lub dezintegracyjnym w regionie Europy Środkowo-Wschodniej.

SŁOWA KLUCZOWE:

Grupa Wyszehradzka (V4), integracja regionalna, polityka cyfrowa, cyberbezpieczeństwo, integracja i dezintegracja polityczna, transformacja cyfrowa

Introduction

The integration processes within the Visegrád Group (V4) have experienced significant fluctuations over the years. Given the current state of cooperation, an essential question arises: Is it justified to declare the end of collaboration within the V4 format, or is such a conclusion still premature? To explore this, the article examines the security policies of V4 countries after 2022. Until now, security issues have been the common denominator uniting V4 policies. However, even this area has now become a field of political conflicts within the group.

Czechia and Poland have adopted a distinctly proactive stance toward threats posed by Russia, whereas Hungary has taken a more ambivalent approach, undermining unity not only within the V4 but also in the context of the EU and NATO. Following the 2023 elections in Slovakia, Robert Fico's government adopted a more pragmatic approach to cooperation with Hungary, leading to a split with the remaining V4 members and a shifting of the dynamics of collaboration toward more complex and often conflicting interests.

Furthermore, V4 countries differ in terms of technological development, which may influence their ability to cooperate effectively in security and cybersecurity. This is evident in varying levels of military expenditures, rankings in cyber power indices, as well as investments in research and development and the number of patents filed in emerging technologies. Have

these differences decreased among V4 members after 2022? And how do they compare to the broader EU? The article explores these questions as an illustration of the flexibility and dynamism of changes driven, in part, by the heightened sense of threat resulting from the war in Ukraine. If confirmed, this hypothesis would support the claim that security threats can serve as a catalyst for innovation in non-military security policies, including economic and technological development.

The main objective of this study is to answer the question of whether, after 2022, cooperation among the Visegrád Group countries in the area of cybersecurity is moving toward integration or disintegration. As part of the research analysis, the article will also address the following questions: How do political differences in the approaches of V4 countries toward Russia and the European Union affect their cybersecurity strategies? Do factors related to digitalisation development – such as the share of ICT in GDP, R&D expenditure, high-tech exports, and patents – foster the process of integration, or do they rather reflect the state of political disintegration within the V4? To what extent do the contents of the V4 presidency programs and national cybersecurity strategies confirm a commitment to joint actions, and to what extent do they emphasise national autonomy? Finally, is the sense of threat – particularly the war in Ukraine – a catalyst for integration or disintegration in the V4's digital policy?

The research analysis – particularly in the context of cooperation among the V4 countries and their relations with EU policy – fits within the framework of regional integration theory, which explores the nature of regionally structured processes, joint declarations, and formulated goals in the field of digital innovation¹. Moreover, the cooperation among the V4 countries in the areas of new technologies and cybersecurity, as presented in this study, is viewed as part of a broader digitalisation trend and is based on the theory of neofunctionalism². Therefore, it can be hypothesised that the convergence of positions regarding digital infrastructure leads to a deepening of political and strategic integration.

¹ M. Dangerfield, *Subregional Economic Cooperation in Central and Eastern Europe*, Elgar, 2001; V.A. Schmidt, *The future of differentiated integration: a 'soft-core,' multi-clustered Europe of overlapping policy communities*, "Comparative European Politics" 2019, vol. 17, pp. 294–315.

² P.C. Schmitter, *Ernst B. Haas and the legacy of neofunctionalism*, "Journal of European Public Policy" 2005, v. 12, no. 2, pp. 255–272, DOI: 10.1080/13501760500043951.

The analysis of the topic is based primarily on three research methods. The first is the comparative perspective, which, by juxtaposing data illustrating digital development and the positions expressed in the strategic documents of the V4 countries, makes it possible to identify similarities and differences among the individual states. The second method is content analysis of documents – particularly the V4 presidency programs (2019–2025) and national strategies – which allows the characterisation of each country’s approach to digital development and cybersecurity. The third method is both quantitative and qualitative analysis, which, through the use of economic indicators, illustrates not only the level of digital innovation among the V4 members but also identifies areas requiring improvement that may simultaneously act as barriers to building a common cybersecurity policy.

1. The evolution of V4 – between integration and tensions

Cooperation among the four Central European nations stems from their shared history of civil resistance against communist rule. Visegrád cooperation draws on the cooperation among opposition actors before 1989. These actors were elected to high political office following the democratic changes. The 1991 meeting of Presidents Havel and Wałęsa and Prime Minister Antall highlighted Central European solidarity. However, *Realpolitik* largely paralysed the political dimension of cooperation in the first seven years. Czechoslovakia was initially preoccupied with its own dissolution. Subsequently, the Czech Prime Minister, Václav Klaus, took a decidedly sceptical stance towards Central European integration. The Polish and Hungarian governments attempted to continue regional cooperation without the Czech Republic, but the return of Vladimír Mečiar to power in Slovakia brought an end to these efforts³.

The second phase, which covered the years 1998–2004, showed many signs of a strengthened willingness to cooperate. The first year of this phase was marked by significant changes in government: a pro-integration coalition was formed after the 1998 elections in Slovakia, while the new Prime Minister

³ Š. Waisová, L. Piknerová, *Twenty Years After Dissident Tradition in Czech Foreign Policy Matters*, “East European Politics and Societies” 2012, vol. 26, no. 1, pp. 162–165.

Zeman introduced a policy favourable to Visegrád cooperation. This policy mainly supported steps leading to Slovakia's membership of NATO and the EU, as well as helping it to catch up with its partners within the group. This became a reality in 2004, when Slovakia joined NATO and all the countries became EU members⁴.

The third phase begins with the V4 countries joining the EU. During the first five years after the 2004 EU-enlargement, the V4 gave the impression of an exhausted community that would fulfil optimistic forecasts (pro-Westernisation) or sceptical predictions (becoming geopolitically absorbed) on the dissolution of the Central European region. However, since the end of the 2000s, we can observe a fundamental turnaround, which was linked (among other factors) to V4's new profiling. East-Central Europe began to be perceived as a structure challenging various EU fundamental norms or customs. "After the economic crisis in 2008, the Europeanisation of ECE politics was rather quickly replaced with the politicisation of European integration fuelled mainly by nationalist and Eurosceptic politicians"⁵.

In addition to building its position as a model and mediator of "Europeanisation" and European policies toward the Western Balkans and Eastern Partnership nations, the V4 has attempted to promote itself as an additional/alternative group of countries that introduces agendas within the EU and profiles itself as a significant collective actor. After 2009, the V4 changed its rather defensive style and began to offer significantly more proactive stances "when it emphasised its ambition to become one of the needed and energising factors in the project of European integration as its goal"⁶.

However, this ambition has been undermined by Hungary's violations of the principles of the rule of law after 2010. In some respects, this has also been the case for Poland and Slovakia. Even more damaging has been the

⁴ M. Dangerfield, *The Visegrád Group in the Expanded European Union: From Preaccession to Postaccession Cooperation*, "East European Politics and Societies" 2008, vol. 22, no. 3, pp. 643–647.

⁵ V. Hloušek, *Linking European integration illiberalism: 'Laboratory' of Central-Eastern Europe*, "Politics in Central Europe" 2023, vol. 19, no. 2, p. 218.

⁶ L. Cabada, Š. Waisová, *The Visegrad Four as an ambitious actor of (Central-)European foreign and security policy*, "Politics in Central Europe" 2018, vol. 13, no. 2, pp. 12–13; M. Kořan, *Dvě dekády české zahraniční politiky a bezvýchodnost internacjonalistické hegemonie*, "Czech Journal of Political Science" 2012, vol. 13, no. 3, pp. 208–209.

transformation of the V4 into a regional populist format⁷. Gradually, the group found itself in isolation, as other countries of the region observed this linear trajectory. This separation was most significant in the case of Slovenia, steadily professing allegiance to the EU core, but also that of the Baltic states⁸.

The image of the V4 was clearly damaged during and beyond 2015 and the migration crisis. Nevertheless, the V4 was proposing important changes in EU policies: alongside migration and external border protection, energy security deserves a mention as well as further enlargement and focus on the Eastern Partnership. “Under the Visegrád umbrella, the member governments have signalled their support for moving forward with the EU’s energy union plan, completing an internal energy market, and completing the North-South gas Corridor”⁹. Also worth mentioning is the creation of the V4 EU Battlegroup in 2016.

Finally, emphasis must be given to the dramatic change after February 2022, which showed the potential of the new member states. It was precisely in this difficult situation that the Czech presidency of the EU Council took place in the second half of 2022, which led, among other things, to a new security consensus within the EU and at the same time to the gradual emptying of the V4 by the new Czech executive. However, fundamental disagreements regarding Russian aggression towards Ukraine have disrupted Polish-Hungarian relations in particular¹⁰. Following the change of government in Slovakia in autumn 2023, the V4 underwent a significant transformation, becoming an empty structure. Conversely, Czech-Polish and Hungarian-Slovak cooperation and coordination of procedures intensified markedly.

There is no doubt that Russia’s invasion of Ukraine presents a major turning point. From the perspective of the V4, “the increased salience of security also exposed the long-standing differences regarding Russia’s aggression across the member states. In the V4 group, such differences ranged

⁷ F. Söderbaum, K. Spandler, A. Pacciardi, *Contestations of the Liberal International Order. A Populist Script of Regional Cooperation*, Cambridge University Press, 2021.

⁸ L. Cabada, Š. Waisová, *Slovenia as an EU-member: a Euroenthusiastic society and political elite*, [in:] P. Drulák, Z. Šabič (eds.), *The Czech and EU Presidencies in a Comparative Perspective*, Dordrecht 2010, pp. 37–54.

⁹ A. Schmidt, *Friends forever? The Role of Visegrad Group and the European Integration*, “Politics in Central Europe” 2016, vol. 12, no. 3, p. 124.

¹⁰ E. Eihmanis, *EU transnational coalitions in polycrisis: the Visegrád-4 before and after the Russo-Ukrainian War*, “Journal of European Public Policy” 2024, vol. 31, p. 13, DOI: 10.1080/13501763.2024.2357268.

from harsh criticism in Poland, pragmatic friendliness in Hungary, and deep polarisation and volatility – depending on ruling incumbents – in Czechia and Slovakia. Against the backdrop of conflicting security stances between the four states, the V4 format became increasingly strained”¹¹.

A very clear element of change is the Polish – and partly also Czech – prioritisation of the hard security element, which clearly reflects Russia as a key threat. This perception brings Poland much closer to the Baltic countries (the 3+1 group), while among the Visegrád countries, only the Czech Republic has joined the Polish perspective under the new President Petr Pavel and government led by Prime Minister Petr Fiala (2021–2025). However, as in the past, the current format may undergo various changes, primarily due to domestic political developments. Following the autumn 2025 elections, a new Czech government based on the present opposition could adopt similar positions to those of Hungary and Slovakia. This was repeatedly emphasised during the election campaign by presumed returning Prime Minister Andrej Babiš and other opposition leaders, who Babiš is counting on for support for the new government. Conversely, a rise in support for the current Hungarian opposition could lead to further changes in the mini-coalitions within the V4. Poland, therefore, seems to be the only stable player, as there is no emotional polarisation between the government and the opposition regarding security policy, which also correlates with public attitudes.

They describe the evolution of the V4, noting that this process was shaped by numerous declarations and documents that became milestones in the policies of its members. Among the most significant historical events are, above all: the Declaration of 15 February 1991, on cooperation among the three (now four) countries on their path toward European integration, which simultaneously served as the founding document of the V4; the establishment of the International Visegrád Fund in 1999; and the Declaration on Cooperation of the Visegrád Group Countries after Accession to the European Union, signed on 12 May 2004, in Kroměříž.

An equivalent of similar importance in the field of cybersecurity policy can be found in documents that align with the general process of digitalisation, such as the *Joint Declaration of Intent of Prime Ministers of the*

¹¹ Ibid., pp. 12–13.

*Visegrád Group on Mutual Co-operation in Innovation and Digital Affairs*¹² from 2017 and the *Visegrád Group Joint Declaration on Mutual Cooperation in Digital Projects*¹³ from 2021. The first of these documents gave digitalisation political significance, resulting in new technologies – both in the military and non-military domains – becoming a visible priority for V4 governments. It also initiated further governmental declarations at the level of prime ministers and ministers in subsequent years. The second document, from 2021, represents another stage of integration among the V4 countries, as it emphasises the need to introduce important mechanisms for consultation and cooperation, including in the implementation of EU-funded digitalisation projects. A noteworthy achievement – considering divergences in other policy areas – is the identification of strategic innovation goals such as AI, IoT, blockchain, and combating disinformation. This demonstrates that the V4 can present itself as a unified bloc of interests within the EU and share a similar interpretation of new transnational threats. On the other hand, the content and outcomes of the declared objectives lack durable institutional translation (e.g., the absence of a joint V4 cybersecurity agency). Moreover, the document does not provide for mechanisms to enforce commitments. There are also visible differences in the approaches of V4 members toward the roles of the United States and China. Therefore, it is difficult to conclude whether the V4’s digital policy thus far serves as evidence of integration or disintegration among the member states in the area of digitalisation. Existing research also points to these divergences, indicating that the V4 more often formulates joint positions and cooperation programs rather than comprehensive, unified regional strategies¹⁴.

¹² Visegrad Group, *Joint Declaration of Intent of Prime Ministers of the Visegrad Group on Mutual Co-operation in Innovation and Digital Affairs*, <https://www.visegradgroup.eu/home/documents/selected-events-in-2017-170203/joint-declaration-of> [15.04.2025].

¹³ Visegrad Group, *Joint Declaration on Mutual Cooperation in Digital Projects*, <https://www.visegradgroup.eu/download.php?docID=458> [15.04.2025].

¹⁴ E. Eihmanis, *EU transnational coalitions in polycrisis: The Visegrád-4 before and after the Russo-Ukrainian war*, “Journal of European Public Policy” 2024, vol. 31, no. 10, pp. 1–25, DOI: 10.1080/13501763.2024.2357268; I. Tasheva, I. Kunkel, *In a hyperconnected world, is the EU cybersecurity framework connected?*, “European View” 2022, vol. 21, no. 2, pp. 186–195, DOI: 10.1177/17816858221136106.

2. Conditions for building a regional digital policy

The V4 members view the development of digital skills as an important factor – not only as a basis for national security but also as a guarantee of stable state development. In this context, it is worth considering whether, in order to achieve these goals, the countries seek common strategic solutions and are open to regional cooperation. An answer to this question may be provided by analysing the performance of individual countries in the process of digital transformation.

The approach of describing integration and disintegration processes through economic indicators serves as a way to address a research gap in the study of V4 cybersecurity policy. While there exists a substantial body of analyses concerning regional cooperation¹⁵ – and, in recent years, also on security¹⁶ – these studies do not fully account for technological factors, particularly those related to cybersecurity. Therefore, the proposed perspective of digital development presented below makes it possible to broaden the analytical framework to include this dimension, while also enriching the analysis through an examination of non-military aspects of cybersecurity.

2.1. The importance of the ICT sector in the economies of the Visegrád Group countries

An important illustration of a state's efforts to develop its digital potential is the role of ICT in the national economy. This reflects the significance that political decision-makers assign to the development and implementation of modern information and communication technologies.

¹⁵ P. Kaniok, V. Hloušek, *Visegrad four as an institution in times of EU crises*, "European Politics and Society" 2025, pp. 1–19, DOI: 10.1080/23745118.2025.2488815; E. Eihmanis, *EU transnational coalitions in polycrisis: the Visegrád-4 before and after the Russo-Ukrainian war*, "Journal of European Public Policy" 2024, vol. 31, no. 10, pp. 1–25; A. Poznar, V. Havlík, *From complementary and opportunistic sub-regionalism to anti-systemic attitudes? Exploring the post-2022 attitudes of Visegrad member states to cooperation*, "European Politics and Society" 2025, vol. 26, no. 4, pp. 937–954, DOI: 10.1080/23745118.2024.2446813.

¹⁶ K. Fridrichová, *Mugged by reality: Russia's strategic narratives and the war in Ukraine*, "Defense & Security Analysis" 2023, vol. 39, no. 3, pp. 281–295, DOI: 10.1080/14751798.2023.2201018; Y. Reykers, P. Rieker, *Ad hoc coalitions in European security and defence: symptoms of short-term pragmatism, no more?*, "Journal of European Integration" 2024, vol. 46, no. 6, pp. 861–879, DOI: 10.1080/07036337.2024.2349608.

Therefore, the higher the percentage share of the ICT sector in GDP, the greater the economic impact of this sector on the country's economy. It also indicates the presence of an economy based on modern technologies with significant innovation potential, often resulting in high exports of goods produced using advanced technologies.

Analysing the share of ICT in GDP among the V4 countries is also important for understanding the potential for integration processes in the Central and Eastern European region. If these countries exhibit significantly different shares of ICT in their GDP, this indicates a lack of coherence in economic development, which may lead to divergences in setting interests in cybersecurity policy. Another possible consequence is the insufficiently developed digital potential, which weakens the position of these countries in the joint European policy addressing global challenges.

Table 1. ICT Sector share in GDP (%)

	2020	2021	2022	2023	2024
Poland	3.73	3.94	4.03	4.15	4.25
Czech Republic	4.94	4.92	4.93	5.00	5.10
Hungary	5.95	5.76	5.48	5.60	5.70
Slovakia	4.61	4.62	4.47	4.55	4.60
V4 Average	4.81	4.81	4.73	4.83	4.91
EU Average	5.19	5.46	5.46	5.55	5.60

Source: Eurostat. Database, <https://ec.europa.eu/eurostat/data/database> [15.04.2025].

Data from 2020 to 2024 indicate that the share of the ICT sector in GDP in individual countries (with minor fluctuations in the cases of the Czech Republic and Slovakia) is steadily increasing. The upward trend among both V4 members and EU countries points to the growing importance of this sector in the European economy.

A relatively high share of ICT in the GDP may indicate the commitment of the authorities of all four countries to the development of new technologies and improving the efficiency of their economies. It may also make the V4 countries more attractive as investment destinations for companies representing new technologies. This is a positive phenomenon, as the gap in results between the V4 countries and the EU is shrinking over the years. It certainly also positively influences the image and standing of their economies, although it should be noted that the average performance of the

V4 countries is still lower than the European level. It is also worth emphasising, in this case, that the pace of development is not uniform among the individual countries, which may pose an obstacle to attempts to create a coherent digital policy in the region.

Development differences between the V4 countries may lead to divergent perceptions of interests, which will certainly be one of the challenges in seeking partners for building joint digital projects. The differing stages of development also mean that some entities may be much more focused on pursuing ambitious development projects that may not always align with the stance of other neighbours seeking possible support to maintain stable digital growth.

2.2. Investments in research and development as the foundations of digital competitiveness

The share of the ICT sector in a country's GDP also corresponds with the efforts of political decision-makers regarding research and development (R&D) activities, which additionally support building digital capacities within the economy and contribute to the development of security based on the application of new technologies.

During the analysed period, the V4 countries have increased their expenditures on R&D compared to previous years. Investments in this area can have a positive impact on the development of innovative solutions and the economic competitiveness of the countries, which in the long term can bring benefits both to the economy and to society as a whole.

Expenditures on R&D thus reflect the commitment of the V4 countries to the development of new technologies and the pursuit of innovation and competitiveness in the international market. They can also contribute to increased employment in the science and technology sector, as well as to the improvement of living and working conditions for the region's inhabitants through the development of new technological solutions.

Table 2. R&D expenditure (% of GDP)

	2020	2021	2022	2023	2024
Czech Republic	1.95%	1.93%	1.89%	1.83%	1.83%
Poland	1.37%	1.42%	1.44%	1.56%	1.60%
Hungary	1.58%	1.63%	1.39%	1.39%	1.40%
Slovakia	0.89%	0.90%	0.98%	1.03%	1.05%
V4 Average	1.45%	1.47%	1.43%	1.45%	1.47%
EU Average	2.28%	2.24%	2.23%	2.24%	2.25%

Source: Eurostat. Database, <https://ec.europa.eu/eurostat/data/database> [15.04.2025].

Similarly to the share of ICT in relation to GDP, the average R&D expenditure among the V4 countries is lower compared to the overall EU indicator. However, the trend in R&D investments across these countries is upward. It should also be noted that there is asymmetry within this category among the V4 members. Hungary and Slovakia significantly lag behind the Czech Republic, which leads in R&D spending, and Poland, which has been systematically investing in this area for the past five years. This phenomenon may hinder the processes of economic integration based on digitalisation within the region among the countries. Thus, differing definitions of investment needs distance the V4 members from the possibility of establishing common areas for conducting digital policy.

Low R&D expenditure may weaken the position of certain countries (particularly Hungary and Slovakia), which will be more compelled to conduct digital policies from the standpoint of expecting support and knowledge transfer from stronger entities, rather than from the position of technological leaders in the international environment.

2.3. High-tech exports as a measure of the region's technological advancement

A high R&D indicator also translates not only into building a competitive economy – exemplified by the creation of new patents – but also into increased interest from foreign entities in products manufactured based on those technologies. This process is illustrated by the export of goods produced using new technologies. This reflects not only the possession of advanced technologies by a given country but also how strong the country's market offering and position are internationally. Therefore, it can be concluded that

the higher the high-tech export indicator, the greater the country's resilience to economic shocks.

Table 3. Exports of high-technology products

	2020	2021	2022	2023	2024
Czech Republic	20.64	18.38	19.19	19.50	19.70
Hungary	16.82	14.94	14.77	14.60	14.40
Poland	8.97	8.77	9.14	9.40	9.60
Slovakia	9.18	8.17	7.44	7.20	7.00
V4 Average	13.90	12.56	12.64	12.68	12.68
EU Average	17.70	17.65	17.32	17.20	17.00

Source: Eurostat. Database, <https://ec.europa.eu/eurostat/data/database> [15.04.2025].

The data in the table indicate that the Czech Republic and Hungary recorded the highest shares of high-tech exports, consistently exceeding 14%, with the Czech Republic reaching 20% in 2020. The remaining countries – Poland and Slovakia – achieve lower results, ranging from 7% to 9%. Countries with a higher level of technological development, such as the Czech Republic, may pursue closer integration with the EU and, as a result, be more reluctant to participate in joint regional projects aimed at developing innovative solutions. In contrast, countries with weaker high-tech export performance may be more inclined to emphasise national autonomy in the area of economic development.

2.4. Patent activity as an indicator of digital innovation

Filing patents in the field of new technologies contributes to shaping the image of a country as a leader in innovation and advanced technologies. Patenting new solutions can serve as a source of revenue for the state, as these innovations may be sold or licensed to other countries and companies. This can help finance further investments in research and development, which in turn leads to even greater progress in the field of cybersecurity. Patent data in the area of new technologies serves not only as an indicator of digital technology development but also as an effective tool illustrating the state's ability to conceptualise strategic challenges.

Table 4. The total number of filed patents in the following areas: Computer technology, Telecommunications, Digital Communications, Audio-visual technology, IT methods for management, Semiconductors

	2020	2021	2022	2023	2024
Poland	20	24	12	22	27
Czech Republic	14	21	11	12	14
Slovakia	3	5	3	3	3
Hungary	9	8	3	7	8
V4 Average	11.50	14.50	7.25	11	13.50
EU Average	414.41	317.70	241.85	280.22	280.56

Source: Data based on the European Patent Office, <https://new.epo.org/en/statistics-centre#/customchart> [17.04.2025].

Compared to the EU average, the number of patents in new technologies filed by the V4 countries remains significantly lower, indicating a notable disparity. However, it should be taken into consideration that each country differs in terms of market size, the number of innovative companies, and other factors influencing the number of submitted innovative solutions.

There is also a noticeable trend that the higher the expenditures on R&D, the greater the ICT share in GDP, and the stronger the support from political decision-makers for innovation, the better the countries perform in terms of the number of granted patents.

Recent data show that Poland and the Czech Republic achieve the best results within the V4 when it comes to the number of patents granted by the European Patent Office, with the other countries performing significantly worse. The activity of Hungary and Slovakia in this field is two to three times lower than that of the other countries. This once again highlights the technological divide, which complicates reaching a common stance among these countries regarding challenges, particularly those related to implementing Industry 4.0 components or the dynamic changes stemming from the use of artificial intelligence. The data show that the Visegrád Group is diverse in terms of digital policy and lacks favourable conditions to express a joint position on technological development, which may act against further integration.

3. Digital policy of the V4 in light of presidency documents

To analyse how the countries formulate digital policy, the next goal of this work is to present the main programmatic assumptions of the Visegrád Group presidencies over the past five years. The research perspective will be based on the content recorded in successive V4 presidencies, which can be seen as the official stance of the countries regarding phenomena occurring in the digital, political, and economic environment.

Challenges resulting from digitalisation – with varying intensity and levels of engagement – have been repeatedly addressed during V4 presidencies by all members. The Czech presidency in 2019–2020, similarly to previous declarations by the Visegrád Group countries, also emphasised the importance of exchanging experiences in building cyber capabilities in the region. The Czech side stressed the integrative character of the V4 in the security dimension, which was to be based particularly on the region's coherence with EU policy, as well as its NATO membership in the context of securing the eastern border of the North Atlantic Alliance¹⁷. The Czech Republic promoted the idea of creating a V4 strategy for digital transformation, which would be based on research in the field of artificial intelligence (AI) development, joint actions in the digital market, and the implementation of digital infrastructure through initiatives such as Industry 4.0, smart cities, and startups¹⁸.

The next presidency of the Visegrád Group in 2020–2021 was held by Poland, which continued efforts to further develop security policy based on cooperation with countries in the Central and Eastern European region. During this period, the Polish presidency was eclectic in nature, as it attempted to combine the ideas of European community solidarity in facing challenges arising from the COVID-19 pandemic, digitalisation, and EU border defence, while strongly opposing the mandatory relocation of migrants within the EU¹⁹. The program emphasised the promotion of digitalisation and AI solutions that would facilitate the introduction of technological considerations in the public sphere, but as autonomous actions by the state without

¹⁷ *Czech Presidency 2019–2020*, <https://www.visegradgroup.eu/home/documents/presidency-programs/presidency-programs>, p. 2 [15.05.2025].

¹⁸ *Ibid.*, p. 4.

¹⁹ *Polish Presidency 2020–2021*, <https://www.visegradgroup.eu/home/v4-presidency>, p. 2 [15.05.2025].

strategic coordination with the rest of the EU²⁰. This demonstrates how the doctrinal attitudes of individual governments influence the hierarchy and priorities set during the V4 presidency.

In 2021–2022, Hungary took over the presidency of the Visegrád Group and largely distanced itself from the actions and declarations articulated in previous presidencies regarding the construction of a common policy, both at the regional and European levels. The priorities mainly focused on issues referring to national sovereignty²¹. This stance clearly challenged Hungary's integrative approach within the EU's common policy in sensitive areas such as migration and the rule of law. During Hungary's presidency, a situation analogous to that of the Polish presidency occurred, but with greater intensity and clarity, demonstrating how perceptions of the development of information and communication technologies can depend on political perspective. The government in Budapest limited itself to its own actions, emphasising the need to maintain national technological sovereignty at the expense of abandoning initiatives aimed at building common digital policy frameworks with the V4 countries²².

The subsequent V4 presidency, held by Slovakia in 2022–2023, focused – unlike the previous Hungarian leadership – on an integrative approach, promoting V4 unity in the face of external threats. This stance was particularly pronounced in the context of the Russian Federation's aggression against Ukraine²³. The program highlighted innovation as a crucial element for further cooperation in the field of cybersecurity. According to this direction, the digitalisation of the economy has become an important source of economic growth. However, to stimulate further development in this area, it was emphasised that future success will largely depend on the level of research and development as well as innovation carried out in the Visegrád countries²⁴.

Further development of the conceptual frameworks for building ties both at the regional and European levels was articulated during the Czech presidency in 2023–2024. During its tenure, attention was drawn to the

²⁰ Ibid.

²¹ *Hungarian Presidency 2021–2022*, <https://www.visegradgroup.eu/home/documents/presidency-programs/presidency-programs>, p. 5 [15.05.2025].

²² Ibid., p. 6.

²³ *Slovak Presidency 2022–2023*, <https://www.visegradgroup.eu/home/documents/presidency-programs/presidency-programs>, p. 2 [15.05.2025].

²⁴ Ibid., p. 5.

need to continue integration efforts, especially in the context of the response to the Russian-Ukrainian conflict. During this presidency, issues related to climate change and digital challenges strongly resonated as dimensions of contemporary security²⁵. The position of the Czech Republic indicates efforts aimed at deepening cooperation with the EU in the field of security and defence, as well as ensuring complementary relations with NATO based on the principle of partnership. A characteristic feature is the close linkage of security policy aspects with the development of technological and digital capabilities. Therefore, the Czech presidency assumed the initiation of the idea to develop a common digital infrastructure, which would simultaneously promote Central Europe as an innovation hub²⁶.

The Polish presidency in 2024–2025 demonstrates that government attention to cybersecurity is not only increasing, but that the area of cybersecurity policy itself is becoming increasingly complex. The promotion of the need to build a common policy aligned with the response to hybrid threats and information warfare²⁷. It is worth noting that in 2025, Poland's presidency of the Visegrád Group coincided with its presidency of the Council of the European Union, which provided an opportunity to strengthen the regionally articulated demands regarding cybersecurity on the European agenda. References were also made to the proposals previously articulated during the Czech and Slovak presidencies concerning scientific cooperation in the field of new technologies. The need for digital transformation – both in infrastructure and in the functioning of enterprises – was strongly emphasised, which can be seen as a continuation of earlier demands, particularly from the Czech side, related to the ideas of Industry 4.0, smart cities, and the implementation of solutions based on artificial intelligence in the public space²⁸.

The presidency of the Visegrád Group is largely declarative in nature, and due to its focus on cooperation within the V4 framework, much more attention is devoted to this issue. However, the declarations themselves are not binding and are not subject to the pressure of actual implementation; rather, they are proposals that provide guidance on possible, specific actions.

²⁵ *Czech Presidency 2023–2024*, <https://www.visegradgroup.eu/home/documents/presidency-programs/presidency-programs>, p. 14 [15.05.2025].

²⁶ *Ibid.*, p. 5.

²⁷ *Polish Presidency 2024–2025*, <https://www.visegradgroup.eu/home/documents/presidency-programs/presidency-programs>, p. 28 [15.05.2025].

²⁸ *Ibid.*, p. 14.

Although all four countries declare a willingness for regional cooperation, their stance largely depends on the political environment in power. Examples of this include Hungary and Poland, which, during their V4 presidencies in 2020–2021, adopted a strategy of selective integration, promoting the idea of a common policy while simultaneously avoiding sensitive areas such as migration and legislative sovereignty. Summarising the positions of all V4 members, it should be noted that the Czech Republic plays the role of the actor most strongly promoting the idea of integration and community both at the regional and European levels. In Poland's case, a shift can be observed, especially after the 2023 elections, indicating a much stronger pro-European Union stance. Nevertheless, it should be noted that Poland oscillates between openness and integration on one hand and national pragmatism – particularly on migration issues – on the other. The third country is Slovakia, which emphasises a willingness to cooperate at the regional level. However, the stance of certain political circles – especially those associated with Prime Minister Robert Fico – contributes to disintegration both within V4 relations and within the EU itself. His critical position, especially on migration, the sovereignty of member states, and sanctions against Russia, aligns him closely with the stance presented by Hungarian Prime Minister Viktor Orbán. These controversial positions are a major source of tensions among EU and NATO members and also contribute to a lack of trust among political elites, which translates into disintegration – especially in digital, legislative, and geopolitical matters within V4 cooperation.

4. Cybersecurity strategies of the V4 countries as an expression of integrative or disintegrative policy

Strategic documents present a vision of the cyber environment that corresponds both to existing threats and reflects the subjective stance of state authorities, thereby giving cybersecurity strategies an individual character. This allows for the characterisation of each country's attitude towards development and joint efforts in terms of assessing actions as integrative or disintegrative, both in the context of European relations and within the Visegrád Group itself. Furthermore, defining cybersecurity policy from this perspective can help better understand the conditions under which political decisions are made among the V4 countries. It may allow for a deeper explanation of

cooperation between the states and can also serve as an indicator of obstacles in mutual relations concerning cybersecurity at the international level.

Poland and the Czech Republic, in their strategic documents, represent a similar perspective on the role and tasks related to the V4. In the Polish document, the regional alliance is interpreted as a political tool to emphasise a common position towards the EU and NATO, as well as to further tighten cooperation, especially in the context of Russia's aggressive policies²⁹. The Czech strategy is also open to integration with the countries of the region; however, its authors view the V4 as a technical forum aimed at more effective cooperation in implementing infrastructure projects such as transport, energy, and educational initiatives³⁰. Both countries also distance themselves from the image of the V4 as a political opposition to EU policies, which contradicts the actions of the governments in Slovakia and Hungary.

This attitude also translates into the perception of the role of new technologies and their application in the political sphere, particularly in the context of digital sovereignty. The Polish and Czech documents emphasise the importance of political stances as well as technological solutions that should be compatible with the requirements of the EU and NATO. The difference between these countries lies in the perception of the use of cyber technologies. In Poland's case, cyber technology is expected to play a priority role in defensive actions, which is especially understandable in the context of the Russian threat³¹. In contrast, the Czech approach places emphasis on applications in the economy, which should be based on the development of domestic technologies in key areas (e.g., cloud computing, 5G infrastructure)³².

The Slovak strategy declares an ambition to build digital sovereignty; to achieve this, the authors point to solutions provided by the EU and NATO partners³³. The assumptions expressed in the cybersecurity strategy indicate that Slovakia tends to be more of a recipient of European funds and solutions.

²⁹ Poland: *The Cybersecurity Strategy of the Republic of Poland for 2019–2024*, p. 17, <https://www.enisa.europa.eu> [15.05.2025].

³⁰ Czech Republic: *National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025*, p. 11, <https://www.enisa.europa.eu> [15.05.2025].

³¹ Poland: *The Cybersecurity...*, p. 13.

³² Czech Republic: *National Cyber Security...*, p. 14.

³³ Slovakia: *The National Cybersecurity Strategy 2021–2025*, p. 7, <https://www.enisa.europa.eu> [15.05.2025].

Hungary, similar to other political actions, much more strongly emphasises its own autonomy. This is also reflected in its cybersecurity strategy, which highlights the need to develop the country's digital potential based on independently made technological decisions³⁴. Although Hungary formally declares membership in the EU and V4, the document – unlike the strategies of the other V4 countries – omits the government's commitment to EU values such as the rule of law or solidarity.

Each of these countries recognises the need to invest in the development of 5G networks and digital technologies to enhance the security of national communication infrastructure. However, Slovakia focuses particularly on the development of digital technologies and communication infrastructure due to the urgent need for remedial actions in this area³⁵. These points are also reflected in the Hungarian cybersecurity strategy, which emphasises the development of cybersecurity expert personnel³⁶. All countries also place strong emphasis on educating the public about cybersecurity. They highlight the importance of providing training and seminars for various groups, including entrepreneurs and public sector employees.

Each of the documents emphasises the need to invest in projects focused on developing digital platforms and implementing technologies such as blockchain, IoT, and smart city solutions. These efforts aim to improve the efficiency and quality of public services as well as enhance the security of digital infrastructure. The documents highlight the importance of electronic platforms that facilitate communication between citizens and public administration, with the goal of improving public services. The difference is that the Polish, Czech, and Slovak documents also emphasise the importance of ensuring the security of digital public services, which requires respecting privacy and protecting personal data³⁷.

The analysis of the documents also shows that differences between the countries are particularly evident when the development and implementation of elements of cyber capabilities are influenced by political attitudes

³⁴ Hungary: *Action in the Field of Cybersecurity 2024*, p. 5, <https://www.enisa.europa.eu/15.05.2025>].

³⁵ Slovakia: *The National Cybersecurity...*, p. 9.

³⁶ Hungary: *Action...*, p. 60.

³⁷ Poland: *The Cybersecurity...*, p. 5; Czech Republic: *National Cyber Security...*, p. 6; Slovakia: *The National Cybersecurity...*, p. 6.

that diverge from EU principles, or when the perception of threats depends on the views of individual political decision-makers.

The differing formulation of political objectives by the governments of Hungary and Slovakia creates divergence not only within the V4 but also within the European Union. Evidence of this can be seen in the decision of the Hungarian government not to impose a complete ban on Huawei's participation in 5G development. The lack of a clearly defined prohibition stands in contrast to EU policy³⁸. Reports and analyses note direct correlations between foreign policy orientation and decisions related to technology³⁹. This greater tolerance for technological partnerships with authoritarian states is also characteristic of the Slovak government, which has declared that it has no evidence of any threat associated with Huawei⁴⁰. Another example is the expansion of the Paks II nuclear power plant in Hungary, which demonstrates Russia's influence over the development direction of the country's strategic sectors, including energy and technology. The project is being implemented by the Russian state-owned company Rosatom under a bilateral intergovernmental agreement signed in 2014, with an estimated value of around 12 billion EUR, largely financed by a loan from the Russian Federation⁴¹. The governments in Budapest and Bratislava show a greater tendency to prioritise economic and commercial interests over maintaining political coherence within the region.

³⁸ F. Venne, *China in Hungary: Real Threat or False Alarm?*, CEPA, <https://cepa.org/comprehensive-reports/china-in-hungary-real-threat-or-false-alarm/> [11.03.2025].

³⁹ *Huawei in Central and Eastern Europe: Trends and Forecast*, https://chinaobservers.eu/wp-content/uploads/2021/01/briefing-paper_huawei_A4_o3_web-1.pdf [15.04.2025]; A.E. Gale, *Hungary, Russia, the West, and the Rest: Orbán's Hedging Strategy*, Global Policy Journal, <https://www.globalpolicyjournal.com/blog/05/12/2023/hungary-russia-west-and-rest-or-bans-hedging-strategy> [17.04.2025]; *Hungary's New Cybersecurity Strategy*, CEE Legal Matters, 11 April 2025, <https://ceelegalmatters.com/briefings/29288-hungarys-new-cybersecurity-strategy> [15.04.2025].

⁴⁰ *Slovakia has no evidence of Huawei security threat – prime minister*, Reuters, 30 January 2019, <https://www.reuters.com/article/technology/slovakia-has-no-evidence-of-huawei-security-threat-prime-minister-idUSKCN1PO1TO/> [15.04.2025]; O. Göndör, *5G regulation and law in Slovakia*, CMS Law, 4 March 2025, <https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/slovakia> [12.04.2025].

⁴¹ I. Gizińska, *Dark clouds over Paks II: no approval for Hungary's state aid*, OSW, <https://www.osw.waw.pl/en/publikacje/analyses/2025-09-17/dark-clouds-over-paks-ii-no-approval-hungarys-state-aid> [4.10.2025].

Conclusion

Political differences between the countries tend to favour the pursuit of an individual path to building their own digital potential, carried out through initiating actions and cooperating with the EU and within its framework, rather than on the level of regional alliances. Differences in threat perception – especially in the context of the Russian Federation – also appear to be one of the reasons for the inability to build a regional digital strategy for the V4. There is also a lack of institutional mechanisms for coordinating activities in the area of digitalisation and cybersecurity.

It is also worth noting that, in addition to differing political attitudes in threat perception among V4 members, there are differences on the institutional level. Governments in Poland and the Czech Republic base their cybersecurity, among others, on specialised agencies such as NÚKIB in the Czech Republic and NASK/CSIRT in Poland. Meanwhile, in Hungary and Slovakia, the organisations responsible for cybersecurity have weaker institutional backing, which results in much less frequently updated strategic programs, lower transparency, and an inability to obtain data concerning, among others, cyber incidents.

Differences in the pace of implementing digital innovations and disparities in the level of development between countries may lead not only to weakened digital resilience but also to weakened cooperation among regional entities, fostering competition, for example, over investments in digital infrastructure.

Although digitalisation could serve as a platform for integration, the V4 does not undertake coordinated actions – such as creating joint institutions or knowledge exchange – that could strengthen community ties in the region. The lack of a coherent policy in building the digital economy, as well as differing perceptions of cybersecurity areas, indicates that the V4 countries are far more divided than in the 1990s. Existing differences in digitalisation and security may lead to choosing individual development paths and seeking strategic partners among other EU countries, which will certainly contribute to deepening the V4's disintegration.

Poland and the Czech Republic more frequently achieve higher scores in digital policy than the other Visegrád Group members. For these countries with higher digital development indexes, Western European states may appear as more attractive partners for cooperation. Meanwhile, Hungary and

Slovakia may opt for actions aimed at emphasising their autonomy and independence within the framework of European economic and digital policy. Such differences may cause tensions among the V4 countries and lead to weakening their common position on the European stage.

The divergences – particularly regarding the war in Ukraine and the assessment of Russia's aggressive policy – have contributed to a significant decomposition of the previously trust-based partnership among the V4 members. This, in turn, has affected the outcomes of cooperation, especially in the development of a regional cybersecurity policy. However, this does not mean that joint efforts in this area have ceased entirely. The initiatives undertaken still hold importance in articulating shared ideas and objectives. They help to build common frameworks – also in terms of meaning – that are valuable, for instance, in fostering a unified perception of digital challenges, which is not often the case even among other EU member states. Nevertheless, these actions are largely declarative in nature. This is certainly due to the fact that cyberspace is a highly sensitive area of both military and non-military competition, which, in the context of the war in Ukraine, requires a particularly high level of trust among partners. It may, therefore, be reasonable to interpret the existing statements as a prelude to future joint institutional and legal activities that would consolidate the established norms and commitments among the states – provided that a common assessment of threats posed by external actors can be achieved.

References:

- Cabada L., Waisová Š., *Slovenia as an EU-member: a Euroenthusiastic society and political elite*, [in:] P. Drulák, Z. Šabič (eds.), *The Czech and EU Presidencies in a Comparative Perspective*, Dordrecht 2010, pp. 37–54.
- Cabada, L., Waisová Š., *The Visegrad Four as an ambitious actor of (Central-)European foreign and security policy*, “Politics in Central Europe” 2018, vol. 13, no. 2, pp. 9–20.
- Czech Presidency 2019–2020*, <https://www.visegradgroup.eu/home/documents/presidency-programs/presidency-programs>, p. 2.
- Czech Presidency 2023–2024*, <https://www.visegradgroup.eu/home/documents/presidency-programs/presidency-programs>, p. 14.
- Czech Republic: National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025*, <https://www.enisa.europa.eu>.

- Dangerfield M., *Subregional Economic Cooperation in Central and Eastern Europe*, Elgar, 2001.
- Dangerfield M., *The Visegrád Group in the Expanded European Union: From Pre-accession to Postaccession Cooperation*, "East European Politics and Societies" 2008, vol. 22, no. 3, pp. 630–667.
- European Patent Office, <https://new.epo.org/en/statistics-centre#/customchart>.
- Eihmanis E., *EU transnational coalitions in polycrisis: the Visegrád-4 before and after the Russo-Ukrainian War*, "Journal of European Public Policy" 2024, vol. 31, pp. 1–25, DOI: 10.1080/13501763.2024.2357268.
- European Commission, *Digital Decade Country Report 2024: Poland, Czechia, Slovakia, Hungary*, <https://digital-strategy.ec.europa.eu/en/factpages>.
- European Commission, *Europe's Digital Decade*, <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>.
- Fridrichová K., *Mugged by reality: Russia's strategic narratives and the war in Ukraine*, "Defense & Security Analysis" 2023, vol. 39, no. 3, pp. 281–295, DOI: 10.1080/14751798.2023.2201018.
- Gale A.E., *Hungary, Russia, the West, and the Rest: Orbán's Hedging Strategy*, Global Policy Journal, <https://www.globalpolicyjournal.com/blog/05/12/2023/hungary-russia-west-and-rest-orbans-hedging-strategy>.
- Gizińska I., *Dark clouds over Paks II: no approval for Hungary's state aid*, OSW, <https://www.osw.waw.pl/en/publikacje/analyses/2025-09-17/dark-clouds-over-paks-ii-no-approval-hungarys-state-aid>.
- Göndör O., *5G regulation and law in Slovakia*, CMS Law, 4 March 2025, <https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/slovakia>.
- Hloušek V., *Linking European integration illiberalism: 'Laboratory' of Central-Eastern Europe*, "Politics in Central Europe" 2023, vol. 19, no. 2, pp. 217–234.
- Huawei in Central and Eastern Europe: Trends and Forecast*, https://chinaobservers.eu/wp-content/uploads/2021/01/briefing-paper_huawei_A4_03_web-1.pdf.
- Hungarian Presidency 2021–2022*, <https://www.visegradgroup.eu/home/documents/presidency-programs/presidency-programs>, p. 5.
- Hungary: Action in the Field of Cybersecurity 2024*, <https://www.enisa.europa.eu>.
- Hungary's New Cybersecurity Strategy*, CEE Legal Matters, 11 April 2025, https://ceel-egalmatters.com/briefings/29288-hungarys-new-cybersecurity-strategy?utm_source=chatgpt.com.
- Kaniok P., Hloušek V., *Visegrad four as an institution in times of EU crises*, "European Politics and Society" 2025, pp. 1–19, DOI: 10.1080/23745118.2025.2488815.
- Kořan M., *Dvě dekády české zahraniční politiky a bezvýchodnost internacionalistické hegemonie*, "Czech Journal of Political Science" 2012, vol. 13, no. 3, pp. 195–217.
- Lien L., Timmermans B., *Crisis-induced innovation and crisis-induced innovators*, "Industry and Innovation" 2023, vol. 31, no. 2, pp. 183–217, DOI: 10.1080/13662716.2023.2228739.
- Poland: The Cybersecurity Strategy of the Republic of Poland for 2019–2024*, <https://www.enisa.europa.eu>.
- Polish Presidency 2020–2021*, <https://www.visegradgroup.eu/home/v4-presidency>, p. 2.

- Polish Presidency 2024–2025, <https://www.visegradgroup.eu/home/documents/presidency-programs/presidency-programs>, p. 28.
- Poznar A., Havlík V., *From complementary and opportunistic sub-regionalism to anti-systemic attitudes? Exploring the post-2022 attitudes of Visegrad member states to cooperation*, “European Politics and Society” 2025, vol. 26, no. 4, pp. 937–954, DOI: 10.1080/23745118.2024.2446813.
- Reykers Y., Rieker P., *Ad hoc coalitions in European security and defence: symptoms of short-term pragmatism, no more?*, “Journal of European Integration” 2024, vol. 46, no. 6, pp. 861–879, DOI: 10.1080/07036337.2024.2349608.
- Schmidt A., *Friends forever? The Role of Visegrad Group and the European Integration*, “Politics in Central Europe” 2016, vol. 12, no. 3, pp. 113–140.
- Schmidt V.A., *The future of differentiated integration: a ‘soft-core’ multi-clustered Europe of overlapping policy communities*, “Comparative European Politics” 2019, vol. 17, pp. 294–315.
- Schmitter P.C., Ernst B. *Haas and the legacy of neofunctionalism*, “Journal of European Public Policy” 2005, vol. 12, no. 2, pp. 255–272, DOI: 10.1080/13501760500043951.
- Slovak Presidency 2022–2023, <https://www.visegradgroup.eu/home/documents/presidency-programs/presidency-programs>, p. 2.
- Slovakia has no evidence of Huawei security threat – prime minister*, Reuters, 30 January 2019, <https://www.reuters.com/article/technology/slovakia-has-no-evidence-of-huawei-security-threat-prime-minister-idUSKCN1PO1TO/>.
- Slovakia: The National Cybersecurity Strategy 2021–2025*, <https://www.enisa.europa.eu>.
- Söderbaum F., Spandler K., Pacciardi A., *Contestations of the Liberal International Order. A Populist Script of Regional Cooperation*, Cambridge University Press, 2021.
- Tasheva I., Kunkel I., *In a hyperconnected world, is the EU cybersecurity framework connected?*, “European View” 2022, vol. 21, no. 2, pp. 186–195, DOI: 10.1177/17816858221136106.
- Venne F., *China in Hungary: Real Threat or False Alarm?*, CEPA, <https://cepa.org/comprehensive-reports/china-in-hungary-real-threat-or-false-alarm/>.
- Visegrad Group, *Joint Declaration of Intent of Prime Ministers of the Visegrad Group on Mutual Co-operation in Innovation and Digital Affairs*, <https://www.visegrad-group.eu/home/documents/selected-events-in-2017-170203/joint-declaration-of>.
- Visegrad Group, *Joint Declaration on Mutual Cooperation in Digital Projects*, <https://www.visegradgroup.eu/download.php?docID=458>.
- Waisová Š., Piknerová L., *Twenty Years After Dissident Tradition in Czech Foreign Policy Matters*, “East European Politics and Societies” 2012, vol. 26, no. 1, pp. 162–188.