# Seeking Opportunities and Mitigating Risks

## The Way Forward for Central and Eastern Europe's Digital Transformation

CENTER ZA EVROPSKO PRIHODNOST
CENTRE FOR EUROPEAN PERSPECTIVE
CEP

# Seeking Opportunities and Mitigating Risks

## The Way Forward for Central and Eastern Europe's Digital Transformation

CENTER ZA EVROPSKO PRIHODNOST
CENTRE FOR EUROPEAN PERSPECTIVE
CEP

# Introduction

Much has changed in transatlantic relations and digital cooperation since we began working on this publication in early 2024. Despite some caveats, there was broad consensus that the US and the EU were strategic partners in the field of digital cooperation—an idea we have consistently promoted in our past publications on digital transformation of Central and Eastern European (CEE) region.[1]

However, shifting geopolitical dynamics and the new US administration have drastically altered the nature of this relationship. European Commission President Ursula von der Leyen has described the current era as one of harsh geopolitical competition. Despite these challenges there is space for cooperation in key areas, particularly in advancing digital transformation and ensuring that Europe remains a strong and competitive player in the global economy.

The CEE region has an important role to play in this process. As it seeks to strengthen its position in the global digital economy and the intensified geopolitical environment, it must navigate a landscape filled with both opportunities and challenges. While the region has demonstrated remarkable ambition and talent, turning potential into tangible progress requires strategic policymaking, investment in digital infrastructure, and a commitment to fostering innovation at all levels of society.

The aim of this publication is to explore different areas where the countries of the CEE region could play a more prominent role in advancing digital transformation and strengthening the EU's competitiveness. All articles in this publication conclude with policy recommendations, offering policymakers some ideas on how to navigate this changed environment. In an era where digital leadership is closely tied to geopolitical influence, Europe and the CEE region cannot afford to stand still. Although written in a seemingly different era, these contributions remain highly relevant and provide valuable insights.

Two major reports on improving EU's competitiveness published last year, one by Mario Draghi and another by Enrico Letta, have set out ambitious strategies for Europe's digital and economic progress. But the key question remains: will these ideas translate into real change? **Barbara Matjašič** tackles this challenge in her article, arguing that while Europe has no shortage of high-level strategies, the real issue lies in implementation. Without effective action, the gap between ambition and reality will only widen.

Beyond policy debates, the practical dimensions of digital competitiveness are also at stake. **Radu-Cristian Muşetescu and Mihai Sebe** explore how CEE countries can contribute to and benefit from Europe's digital transformation. They emphasize the need for a balance between fostering local innovation and scaling up digital industries to compete globally.

One of the most pressing questions is whether the EU and the US can maintain a functional digital partnership despite these shifts. In her article, **Andrea G. Rodríguez** examines whether the EU-US Trade and Technology Council (TTC) can still serve as a viable platform for cooperation. With uncertainty surrounding the TTC's future, Rodríguez highlights the key dilemmas that need to be addressed to prevent transatlantic digital policy from becoming another casualty of global tensions.

Looking toward the future, **Wiktor Sędkowski** discusses the role of 6G and immersive technologies in bridging the digital divide and ensuring that Europe remains at the forefront of technological innovation. His article outlines how investments in connectivity, AI-driven

services, and digital infrastructure can create a more inclusive and competitive digital ecosystem.

Finally, no digital transformation strategy can succeed without robust cybersecurity. **Ewelina Kasprzyk** presents a case study on cybersecurity cooperation in the CEE region, highlighting how stronger regional frameworks and international partnerships can enhance resilience against growing cyber threats.

## Endnotes

1 CEP, Strategic partnership for a secure and digital Europe, 2022, https://www.cep.si/wp-content/uploads/2022/11/CEP-Publication-Strategic-partnership-v07.pdf

CEP, Paving the Digital Path in Central and Eastern Europe - Regional perspectives on advancing digital transformation and cooperation, 2021, https://www.cep.si/wp-content/uploads/2022/11/CEP-Publication-Strategic-partnership-v07.pdf

CEP, The Transformative Power of Digital - Central and Eastern Europe's leap towards greater prosperity, innovation and resilience, 2021, https://www.cep.si/wp-content/uploads/2022/11/CEP-Publication-Strategic-partnership-v07.pdf

# Contents




**Title:** Seeking Opportunities and Mitigating Risks **Subtitle:** The Way Forward for Central and Eastern Europe's Digital Transformation **Publisher:** Centre for European Perspective (CEP), Grajska cesta 1, 1234 Loka pri Mengšu, Slovenia **Language editing:** Teja Kavičič **Design and prepress:** MapDesign d.o.o. **Cover photo/photos:** Shutterstock, Commons Wikimedia **Print run:** 300

Ljubljana, Februar 2025

# Keep the Momentum Going

## From Pledge to Implementation

**By Barbara Matijašič**, MBA, Researcher and Project Director, Institute for Strategic Solutions

**If Europe cannot become more productive, we will be forced to choose. We will not be able to become, at once, a leader in new technologies, a beacon of climate responsibility, and an independent player on the world stage. We will not be able to finance our social model. We will have to scale back some, if not all, of our ambitions. This is an existential challenge.[2] One that demands more than ambition—it demands effective implementation.**

The vision is clear, and the goals are well-defined. But success requires more than good intentions—it demands motivation, collaboration, bridge-building, and, most of all, tangible action. Political incentives, no matter how thoughtfully designed, will have little real impact unless they are felt and realized on the ground, in the economy itself, and among citizens of the European Union. This is where focused efforts in strategic sectors and data-driven SMEs come into play. This brief analysis explores their specific needs in the CEE region, recognizing that digital transformation is far from a straightforward, linear process. Implementation more closely resembles a dynamic and complex caravan—moving together, adapting, and evolving along the way.

Without effective digital transformation and implemented innovations, pressure on labour market, health and social care systems, public finances, and pension entitlements[3] will become too overwhelming. Addressing this requires a comprehensive response: improving infrastructure, embracing innovation, aligning policy with economic realities, as well as protecting both citizens and consumers. Success depends on building an ecosystem in which elements function cohesively, driving progress instead of stagnation.

### Europe knows what to do

The problem is not that Europe lacks ideas or ambition. As Mario Draghi pointed out, we have the talent, researchers, entrepreneurs, and patents to lead globally. Yet innovation often falters in the transition from concept to application. Draghi emphasizes the need for sharper focus, shared resources, and better coordination. Enrico Letta's report underscores the value of open public infrastructure and data-sharing frameworks, which are crucial for enabling innovation. Increasing connectivity, along with next-generation technologies, such as 5G and fibre optics, require EU-wide policy adjustments and consolidation to create an environment that supports advanced digital infrastructure without being anti-competitive or harming consumers.

For example, the Slovenian telecommunication system is very fragmented and one of the most competitive in Europe, considering the number of operators relative to its population[4]. Larger companies have better access to capital and can benefit from **economies of scale**, allowing them to invest more efficiently in infrastructure and technology. This market dynamic highlights the importance of aligning EU-wide policies to ensure that all member

countries can benefit from next-generation technologies.

There is significant potential in investing estimated EUR 200 billion[5] in next-generation technologies such as 5G and fibre optic expansion. Building expertise and advancing workforce development in technological and engineering sectors is a strategic priority for the EU, enabling secure data management, the development of services, and further innovation. In words of Tomislav Čizmić, CEO of Telemach Slovenia, their focus is on **modernizing networks** to better meet the growing demand for data among both consumers and businesses, thereby supporting the transformation into smart cities and driving innovation in the Internet of Things (IoT) within the region.

Furthermore, Europe's pharmaceutical industry exemplifies the consequences of delayed implementation. Only two of the top ten best-selling biological medicines in 2022 originated from EU companies, compared to six from the US. The CEE region, in particular, has the potential to become a **pharmaceutical innovation hub**, but it requires decisive action to unlock this opportunity. Letta and Draghi's recommendations need to be implemented by the European Commission, which should promote new policies to simplify regulations and remove red tape for businesses that want to access European markets, mobilize public and private capital to drive investment in life science technologies, and create the necessary conditions, particularly related to intellectual property rights, to attract innovators back to Europe. Roche outlined a path forward, advocating for simplified regulations, targeted investments, and reforms to the Public Procurement Directive. Proposals such as the Critical Medicines Act could reduce pharmaceutical dependencies and increase competitiveness. Concluding negotiations on the revision of the General Pharmaceutical Legislation is also critical for balancing innovation with patient access. These steps, if implemented, could strengthen Europe's position in global life sciences.

Advances in science, technology, and data mean innovation can do more to improve citizens' lives and the efficiency of our public health systems than ever be-

fore. Governments have been slow to **embrace innovation as a solution**. Regulatory reforms often create new barriers to medical research and biopharmaceutical innovation —historically strengths of the CEE region. According to Eva McLellan, General Manager at Roche Slovenia: "We have the ability to change if we act now. Europe's citizens deserve a strong R&D sector. We need to close the competitiveness gap and make sure that Europe is as attractive for healthcare R&D investment as other regions of the world. If we do not succeed, homegrown medical breakthroughs will become increasingly difficult to achieve. This is the time for European policymakers to act before it is too late. Europe's economy, its health systems, and, most importantly, its patients should not miss out on innovation. Europe's citizens deserve an innovation strategy that centres on the importance of health for productivity and prosperity, and enables strategic investments in innovative healthcare solutions."

## Competitiveness requires consistency and long-term focus

The new Commission is responsible for making sure that regulatory interventions and implementation plans are based on evidence, not reflex. Konstantinos Komaitis, senior researcher and non-resident fellow at the Lisbon Council as well as senior resident fellow at the Democracy and Tech Initiative at the Atlantic Council, in his feature **It's time to move on**, sounded a warning: "When markets are skewed by regulatory favouritism, consumers lose." He described how ongoing market and technological evolutions present great opportunities—for example, offering communication services across borders without the need to deploy infrastructure, as it can be leased from other neutral actors, or focusing on the strengths of certain companies, whether in service or network

management. This can benefit both company profitability through economies of scale and consumer choice, and can be applied to other sectors.

In many CEE countries, SMEs make up about 99% of all enterprises and are vital for employment and economic stability. To support these businesses, regulatory expectations and implementation plans should focus on creating solutions that leverage specific technologies in our economy and environment. In short, we need to place greater emphasis on utilizing domestic expertise and know-how. "It

is essential to invest more in local digital tools, especially in the public sector and economy. This is widely acknowledged as a priority in the CEE region," commented Igor Zorko from the ICT Association of Slovenia. R&D must be translated into real-world solutions for the economy; otherwise, there will be no meaningful increase in productivity or competitiveness.

Smart implementation is gradual, grounded in innovative pilot projects, clear standards, and a focus on strategic goals while ensuring consumer protection. This does not mean that we should underestimate a (more) rapid introduction of changes, as this helps to reduce costs and prevents the exhaustion of everybody involved. Implementation also demands a broader perspective. Change will not happen without a shift in mindset.[6] Empowering youth, reimagining education, and building partnerships among governments, businesses, and other stakeholders are vital. We must harness data and digitalization to optimize business processes, models, and tools for both the government and companies, while empowering the new generation through digital education and promoting shared responsibility.[7]

Achieving ambitions demands deliberate and motivated efforts. By prioritizing implementation and keeping long-term focus on competitiveness, Europe will not only navigate its current challenges, but also position itself to thrive in the global landscape. Quick, decisive responses to change are essential to minimizing negative impacts and maximizing success.

## Policy recommendations:

- encourage investments in digital infrastructure through regulatory frameworks promoting economies of scale and consumer choice;
- establish guidelines and standards for cybersecurity while fostering innovation-friendly regulations for AI;
- advance Europe's digital transformation through initiatives to enhance 5G networks, promote digital literacy, and develop technical skills within the workforce;
- adopt a comprehensive EU Life Sciences Strategy: EUR 131 billion is the annual contribution of the pharmaceutical industry to European economies—among the highest of any sector in Europe;
- appoint a European Commission Executive Vice President for Industrial Competitiveness to oversee strategic industrial policies;
- define clear standards, implement open development programs, and actively collaborate with innovative companies.

## Endnotes

2 https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf

3 https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Ageing_Europe_-_statistics_on_population_developments

4 As of November 2024, Slovenia has had an estimated population of approximately 2 118 697 people. The market is primarily dominated by three major operators, including Telekom Slovenia, A1 Slovenia, and Telemach, but there are several mobile virtual network operators that provide services by leasing network access from the main operators.

5 https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf

6 Many thanks to Aleksander Bastl, owner and director of BASS, a leading company specializing in software solutions for mass billing and digital transformation. As a co-author of Slovenian eDocument standards and a technical consultant for eInvoice at the European Community, he offers insights into the digital transformation of businesses that are invaluable.

7 Many thanks to Igor Zorko from the ICT Association of Slovenia for his expert perspectives and assistance in this brief analysis, particularly for his insights into the expectations of SMEs in the field.

# Digital Competitiveness from a Central and Eastern European Perspective.

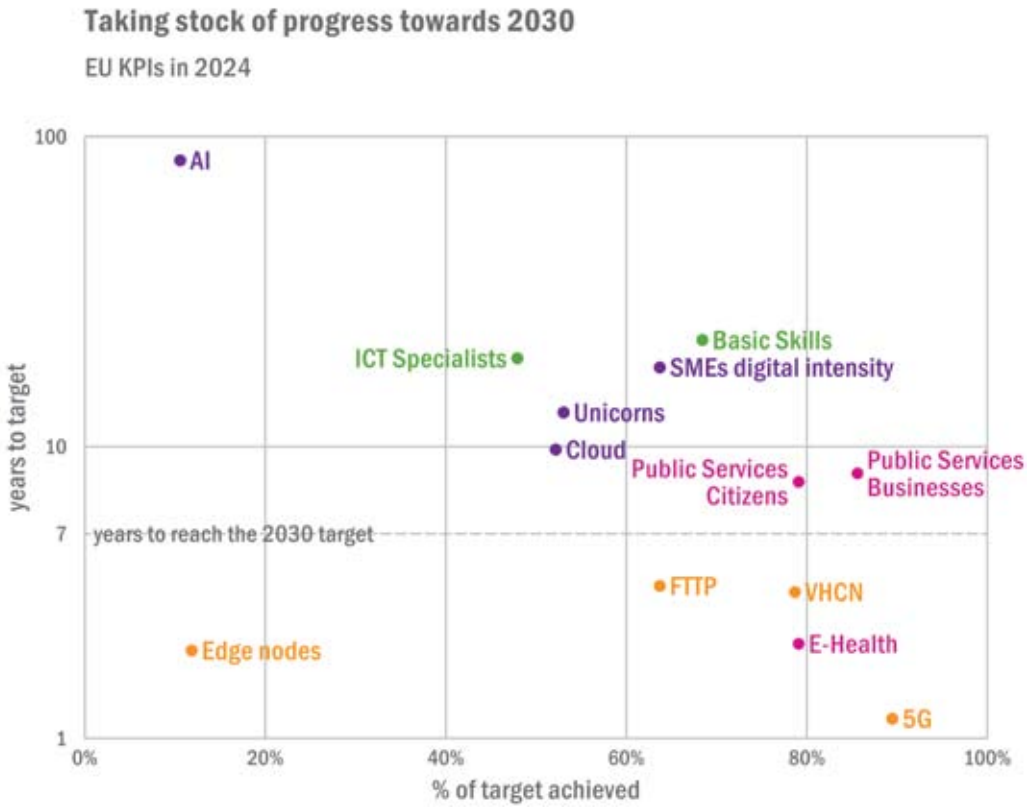
## Can We Do More at Regional and National Levels?[8]

**By Radu-Cristian Muşetescu**, PhD, Professor of International Business and Economics, Bucharest University of Economics
**Mihai Sebe**, PhD, Head of the European Affairs Department, European Institute of Romania, Lecturer, University of Bucharest

**The European Commission has championed digital competitiveness through reforms and policies, emphasising data use, technology investment, and infrastructure improvement, all based on a sound ethical background. However, the situation is complicated, and the EU seems to recognise that it can no longer win the digital race on the basis of past experience. The EU's digital competitiveness depends on significant investment, a balance between scale and innovation, and better coordination. Key areas include financing, digital literacy, technological infrastructure, and flexible regulation to promote long-term growth and competitiveness. The current article wants to present a short overview of the existing situation as well as a series of recommendations for the way ahead toward greater digital competitiveness.**

**The importance of digital competitiveness has not been lost on the European Commission, which has been stressing the need for a strong digital economy for more than a decade.** As ICTs had been behind the EU's productivity gains, the EC warned that measures were needed, such as developing high-speed internet access, improving both the citizens' skills and their level of confidence in the digital world, and, last but not least, supporting ICT innovation[9].

From this reference point, the EU has implemented a series of reforms and policy actions, reflected in the State of the Digital Decade 2024 Communication. It has been a period of steady progress as the EU, through a series of regulatory and non-regulatory measures, has moved forward in creating a governance framework and its own vision of the digital future. The year 2030 has been the main timeline reference. Despite the achievements of the EU as a global policy innovator in promoting a more assertive digital policy framework and progress in the digital industrial base, the situation is challenging as we are dealing with "insufficient progress in reaching the objectives and targets and significant fragmentation across Member States".[10]




Projected time to target based on the last annual average progress for each KPI
Source: European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions: State of the Digital Decade 2024, COM/2024/260 final.

## Digital competitiveness at the level of the EU

In this context, the 2024 elections for the European Parliament and the new European Commission have put competitiveness issues on the broader European agenda. One of the key documents setting the tone is the Strategic Agenda 2024–2029 adopted by the European Council on 27 June 2024. It sets out the importance of a competitive Europe and emphasises the importance of a successful digital transition: "We will exploit the untapped potential of data, promote data interoperability, and encourage investment in game-changing digital technologies in Europe, advancing their application throughout the economy, while ensuring privacy and security. This will require cutting-edge digital infrastructure. Building on the EU digital identity, we will create new EU-wide high-quality e-services."[11]

These ideas are echoed by the newly appointed European Commission, whose guidelines mention the "insufficient diffusion of digital technologies" and the need to "exploit the untapped potential of data" while increasing investment and promoting research.[12]

At the same time, we have a number of commissioners whose portfolios relate to digital competitiveness, such as that of Teresa Ribera, the Commission's Executive Vice-President in charge of a clean, fair, and competitive transition. Her job is to "address the challenges and dynamics of digital markets, including platform economies and data-driven business models".[13] Her attributions are complemented by those of Henna Virkkunen, the Commission's Executive Vice-President in charge of technological sovereignty, security, and democracy. She is responsible for the Digital and Frontier Technologies portfolio and will "oversee our path towards achieving Europe's Digital Decade goals by 2030"[14]. These attributes are further complemented by those of Roxana Mînzatu, the Commission's Executive Vice-President in charge of social rights and

skills, quality jobs, and preparedness. She will "develop an action plan on basic skills and a strategic plan on STEM education to address two of the most glaring shortages. This should be supported by the review of the Digital Education Action Plan, together with the adoption of a roadmap on the future of digital education and training"[15].

## Are there regional solutions for the digital area?

In this context, we need to explore whether this newly announced Commission and the strategic documents that frame its operation could add more value to improving digital competitiveness, or whether we should also look closer to home at regional initiatives within the EU that can help develop it.

For this to happen, we can look more to **the Three Seas Initiative[16] as a possible solution to the problem of digital competitiveness**. As one of the three areas of regional cooperation in 3SI, digital infrastructure is an important element that the participating countries want to develop, along with energy and transport. As the data show, there are significant asymmetries on the one hand and a huge potential for harmonisation and coordination on the other[17].

Digital cooperation in this format has advanced as the war against Ukraine has underlined the importance of cybersecurity and critical infrastructure as such. Moreover, countries in the region such as Poland and Romania have a good track record in cooperation with American big tech companies in the context of the transatlantic partnership (although, for example, the close cooperation between Hungary and China in areas such as 5G has raised several concerns). The Three Seas Initiative provides a framework for a number of important regional initiatives, such as the Smart Connectivity vision, which aims to "expand digital components in key infrastructure, which in turn will support new business models and technologies"[18]. Unfortunately, even in this theoretically favourable climate, only 10% of the total 143 projects are about the digital. The situation is better if we consider that, of the 89 priority projects, 15% are in the digital field[19].

## The way ahead for greater digital competitiveness

**In fact, we are already familiar with the main issues and a number of recommendations, as the Draghi report on competitiveness highlights the challenges facing the industry and businesses in the single market, making a number of recommendations and stressing issues to be addressed.** The document highlights the importance of digitalisation: "The EU's competitiveness will increasingly depend on the digitalisation of all sectors and on building strengths in advanced technologies, which will drive investment, job, and wealth creation". The situation is even more dramatic as "the EU relies on third countries for over 80% of its digital products, services, infrastructure and intellectual property (IP)," and "compared to US and Asian counterparts, EU technology companies currently lack the scale to support R&D and deploy investments in telecoms, cloud services, AI, and semiconductors". In this context, the report highlights the need for significant funding to be invested in areas such as high-speed/capacity broadband networks and related equipment and software, computing and AI, and semiconductors.[20]

**In this context, we recognise the need for a complex approach to digital competitiveness at national, sub-regional and EU levels.** A number of analyses have highlighted **the delicate balance between scale and innovation in the digital sector.** In the face of strong competition from outside the EU, the dilemma for economic policy in 2025 is whether we should focus on scaling up to ensure that EU companies become digital champions, or whether we should focus on competition between small and medium-sized companies to foster innovation[21]? This is a complex issue, as the present authors also believe **that we should strike a balance between competition and innovation policy objectives.** We should be careful not to favour one at the expense of the other, and we should design a flexible European legislative and regulatory framework[22].

The EU is in a challenging position of trying to develop digital competitiveness in a context

where large American tech companies dominate the European markets and sometimes seem to use this privileged position without restrictions. Their strategies and approaches have led to sensitive relations with the EU's competition authorities. Starting decades ago with Microsoft and Intel, the modern European competition approach is challenged by Apple, Google, Amazon, and Meta. Moreover, on the horizon are Chinese giants such as ByteDance and its well-known platform TikTok or various Chinese AI players.

This brings us to the second aspect of possible action—**political (geopolitical) aspects of digital competitiveness**, especially in relation to aspects such as artificial intelligence. In the recent years, the development of artificial intelligence has become a matter of geopolitical competition. The EU has developed a comprehensive, ethics-based approach—developing research and industrial capacity while taking into account human rights[23]. While this approach is noteworthy, some of its limitations have become apparent as the EU lags behind other major players[24]. The AI race has recently been complicated by divisions within EU member states over the access to AI chips—out of 27 member states, 17 would have limited access to US AI chips, leading to fragmentation of EU AI development and affecting the single market, as not all EU member states would be able to rely on US AI chips[25]. This has caused several national reactions, but so far, they seem to have had the desired effect[26]. In addition, under the new US administration, a number of decisions have been taken that have opened up competition and encouraged a number of large-scale investments[27]. The above facts lead to another recommendation—better coordination at national and EU levels and a re-evaluation of existing policies. Are they appropriate to the current context? And if not, what should be done? Deregulation in some aspects, as well as a stronger public-private partnership, may be one solution.

We also come **to the issue of regulatory burden and the lack of capital**. A number of studies have shown the need for easy access to finance. To this end, facilitating investment in the digital sector on behalf of pension funds and insurance companies is a must. It is also important to analyse **tax facilities for the ITC sector**—several facilities can be adopted, either at the European level or at the regional or national level, which can provide sufficient incentives for companies to invest further. The facilities should be agreed on a stable basis to ensure long-term business plans.

Europe needs **a better technological infrastructure**. This requires a number of actions, such as securing supply chains for all the products needed (rare elements, chips, etc.) and better networks across the continent. Where necessary, facilities could be set up for network operators across the EU.

Last but not least, the elephant in the room seems to be **the need for less burdensome laws and regulations**. We need to properly evaluate the legislation in place, see its benefits and limitations, and then analyse whether more rules are needed, or whether we need to remove or rephrase some parts of the legislation[28].

Based on our experience as educators, there is one recommendation that should be thoroughly followed—**the need to improve the digital literacy of European citizens**. This is a need on several levels. In addition to basic digital skills, we also need to increase citizens' awareness of cybersecurity. Furthermore, we need to debate the role of new technologies in society and create informed citizens who can critically assess the impact of artificial intelligence on a case-by-case basis. As the social impact of digital technologies is becoming more apparent, preparing for an orderly digital transition that leaves no one behind is crucial for their acceptance and for digital competitiveness as such.

## Endnotes

8 The opinions expressed are solely those of the authors and should not be taken as representative of the official position of their respective institutions.

9 Ministry of Industry and Trade, Czech Republic, The European Commission published its Digital Competitiveness report, 27.05.2010, https://mpo.gov.cz/en/e-communications-and-postal-services/electronic-communications/european-union/the-european-commission-published-its-digital-competitiveness-report--74549/

10 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: State of the Digital Decade 2024, COM/2024/260 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DC0260.

11 European Council, Strategic Agenda 2024–2029, https://www.consilium.europa.eu/en/european-council/strategic-agenda-2024-2029/.

12 Ursula von der Leyen, Europe's Choice. Political guidelines for the next European Commission 2024–2029, https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf.

13 Teresa Riber, Executive Vice-President (2024–2029) for clean, just, and competitive transition, European Commission, https://commission.europa.eu/about/organisation/college-commissioners/teresa-ribera_en.

14 Hanna Virkkunen, Executive Vice-President for tech sovereignty, security and democracy, European Commission, Mission Letter, https://commission.europa.eu/document/download/dd306c3d-06bc-4550-ab79-c638b7a87b61_en?filename=mission-letter-virkkunen.pdf.

15 Roxana Mînzatu, Executive Vice-President (2024–2029) for social rights and skills, quality jobs, and preparedness, European Commission, https://commission.europa.eu/about/organisation/college-commissioners/roxana-minzatu_en.

16 The Three Seas Initiative, https://3seas.eu/.

17 Octavian-Dragomir Jora, Marius-Cristian Neacşu, Cezar Teclean, Rolul mecanismelor regionale de cooperare în contextual geopolitic actual. Oportunități şi provocări pentru România [The role of regional cooperation mechanisms in the current geopolitical context. Opportunities and challenges for Romania], The European Institute of Romania, 2024, http://ier.gov.ro/wp-content/uploads/2024/01/Studiul-SPOS-nr.-3_Mecanisme-regionale-de-cooperare_final.pdf.

18 Three Seas Initiative, Smart Connectivity, https://3seas.eu/about/smart-connectivity.

19 Three Seas Initiative, Status Report of 2024, https://projects.3seas.eu/report.

20 European Commission, The future of European competitiveness, Part B: In-depth analysis and recommendations, September 2024, https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf.

21 European Parliament, "Balancing scale with innovation for productivity", in Ten issues to watch in 2025, 2025, https://www.europarl.europa.eu/RegData/etudes/IDAN/2025/767186/EPRS_IDA(2025)767186_EN.pdf.

22 OECD, "Competition and Innovation: A Theoretical Perspective", OECD Roundtables on Competition Policy Papers, No. 294, OECD Publishing, Paris, 2023, https://doi.org/10.1787/4632227c-en.

23 European Commission, European approach to artificial intelligence, https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

24 European Commission, AI Watch landscape, https://web.jrc.ec.europa.eu/dashboard/AI_WATCH_LANDSCAPE/index.html?bookmark=overview.

25 Pietr Haeck, "US limits on AI Chips split EU", Politico, 14 January 2025, https://www.politico.eu/article/eu-warns-back-against-us-artificial-intelligence-chip-export-china-limits/.

26 Polish Press Agency, Poland seeks clarity on US AI chip export restrictions, 15 January 2025, https://www.pap.pl/en/news/poland-seeks-clarity-us-ai-chip-export-restrictions.

27 Fact Sheet: President Donald J. Trump takes action to enhance America's AI leadership, White House, 23 January 2025, https://www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-president-donald-j-trump-takes-action-to-enhance-americas-ai-leadership/.

28 Marcus, J. Scott, Rossi, Maria Alessandra, Strengthening EU digital competitiveness : stoking the engine, EUI, RSC, Research Project Report, 2024, Centre for a Digital Society- https://hdl.handle.net/1814/76877

# Beyond Uncertainty

## Three Dilemmas to Solve to Consolidate EU-US Trade and Tech Relations

**By Andrea G. Rodríguez**, Associate Research Fellow, Centre for European Policy Studies (CEPS)

**When the EU-US Trade and Technology Council (TTC) was set up, the European Union was in the middle of the most intense regulatory periods in the field of digital policy in its history. At the point of establishment of the TTC in spring 2021, the EU had already put forward major regulations to curb the power of big tech platforms, proposed the first law governing AI models, and established important rules to foment data sharing and reuse.**

The TTC was born out of a climate of renewed trust, from which both parties were able to benefit on multiple scales. First, on the diplomatic level, announcing the TTC was a sign of revitalisation of the transatlantic partnership after President Biden was elected. Closer EU-US cooperation in technology would be the necessary push to export a vision of democratic and responsible tech governance in a world increasingly seduced by Chinese technology.


US-EU Trade and Technology Council Ministerial Strategic Session, in Luleå, Sweden, 31 May 2023.
Photo by Chuck Kennedy, U.S. Department of State, via Wikimedia Commons.

Second, at the industry level, the establishment of the TTC was a sign to stakeholders that necessary conversations were taking place to prevent fragmentation and improve trade. As the EU advanced its regulatory agenda, the Biden administration failed to put in place a vision for the US digital agenda. Therefore, the TTC would help align priorities and harmonise approaches to make transatlantic tech trade as easy as possible for companies.

Third and last, at the technical level, the TTC would be a useful instrument to align the creation of standards. During the first meeting, ten working groups were set up, in which EU and US officials would sit down over the year to discuss the nitty-gritty of policymaking. This approach joining EU and US staff, not politicians, to work together has already yielded positive results, such as a deal for e-vehicle chargers, but it has not shone as it could.
With political uncertainties about what the next US administration would look like and the poor capacity to find solutions for high-pressing topics (e.g., clean technologies), the TTC risks becoming another failed transatlantic cooperation forum. Consolidating the TTC as a technical forum to discuss emerging governance issues is necessary to future-proof the TTC. Poor results of the TTC meeting held in January 2024 and low ambition shown in the Leuven TTC meeting of April 2024 show that there is still a long road ahead to consolidate EU-US trade and tech relations.

## Losing steam in Washington

Despite the scarce delivery of concrete results, closer cooperation has borne fruit in the way that the transatlantic community approaches emerging tech challenges. The **Joint AI Roadmap**[29] is probably the most ambitious, by size, of the deliverables of the TTC and a case in point of how concerted efforts to find common ground on pressing issues can yield results. The Roadmap highlights three areas of action: definitions and taxonomies, emerging risks, and standards. And though some deliverables could be harder to implement than others—the EU, for instance, is about to sign into law the AI Act, in which multiple definitions have been agreed—for many others the TTC is still on time: standards.

Despite discussions advancing on the three areas, no new advancement was announced in the TTC meeting on January 30, which also ended up with no publication of a joint communiqué, as in the previous times. Moreover, the readouts published by the White House and the European Commission showed a decreased intensity of the conversations and an unwillingness to discuss pressing issues in a year as sensitive as 2024. This, plus the several months' delay of the meeting, usually taking place in spring and at the end of the year, is a warning sign of the weakening attention of the EU and US executives for the TTC and of its reduced speed in producing outcomes.

## (Unsuccessfully) calming the waters in Leuven

While the Washington TTC finished without a joint statement, European and American leaders knew that they needed to show renewed commitment in Leuven if they wanted to convince the public of the strength of EU-US relations.
The sixth TTC, celebrated under the auspices of the Belgian presidency of the Council of the EU in Leuven, was a call for calmness. While no disruptive advancements of different working groups were announced, this time leaders did publish a joint statement underlying their commitment to continue working under the TTC framework, calling it an "operational forum for cooperation" on strategic matters. However, with no new date in sight for a seventh TTC, whether this last statement was a benchmark for the future or a last plea is yet to be seen.

## Addressing the elephant in the room

The TTC's success comes from a mix of momentum and cooperation at the right level. In addition to this, the TTC has proved to be the most successful in aligning visions around emerging issues still not so well established in their political agendas, such as the case of AI. However, the lack of concrete deliverables and the poor involvement of the stakeholder community add additional pressure on the TTC to become another failed initiative. This is **the TTC's main dilemma**[30].

As EU and US leaders prepare for a post-election TTC era, necessary decisions need to be made if the TTC is to have a seventh meeting in the US after the presidential elections and the renewal of the EU Parliament and Commission.

*Choice 1: Either the TTC commits to solving current issues or focuses on long-term impacts*

Since its conception, it was evident that the TTC could become an instrument for helping thaw EU and US relations. However, because of that, it has been better equipped to build from a place of common interest rather than solving controversial issues high on the agenda, such as ensuring transatlantic data flows after **Schrems II**[31]. But infusing optimism in the governance of digital technologies without addressing the elephant in the room can often decrease the speed at which the TTC delivers. Moving forward, there is a decision to be made: either the TTC consolidates itself on focusing only on areas where the EU and US postures are still undefined, or it becomes the place to address irritants and controversies.

*Choice 2: Either the TTC remains vague, or it reforms its structure*

The main dilemma the TTC is facing is that, while it has proven to be best suited to build consensus in areas that are pre-regulation, the lack of regulatory agency of the TTC and the lack of involvement of the stakeholder community have put at risk its very existence. Aligning on how to face issues is certainly a good tool to eventually land in the creation of effective instruments to deal with them, but it precisely leaves action to the free will of the leadership involved. Several actors have written about the need to reform the TTC, with some of them even asking to **"legalise"**[32] it through the establishment of a permanent structure that would ensure that ideas are channelled into the creation of relevant policies. As the year unfolds, that is another choice that EU and US policymakers must face: either the TTC convinces stakeholders of the wins of its loose structure, or it goes big.

*Choice 3: Either the TTC focuses on politics or on technical issues*

Paradoxically enough, the most impactful deliverables of the TTC have not been foreseen by the agenda of the working groups, but are a result of international geopolitics. The TTC was a major factor in helping the EU and the US align sanctions after Russia illegally invaded Ukraine in February 2022. International crises have been unintentionally part of the TTC agenda. The first meeting took place in the middle of the COVID-19 pandemic, Russia's war of aggression against Ukraine has been part of the agenda since the second meeting, and the Israel-Hamas war has also been addressed already. It is arguably a good time for EU and US leaders to convene in a TTC meeting and discuss how to use the EU and US economic power to force desired ends, but this takes the spotlight away from the work done by the TTC in other, technical matters. In addition, because of the political weight that the TTC is gaining due to its messages sent during major crises, there are questions about whether a leadership less favourable to transatlantic cooperation would see the TTC as a disposable forum. Hence, there is another choice to make: either the TTC fuses with other political encounters like the EU-US Summit, or it becomes fully technical; boring for politicians, but useful to the industry.

## The way ahead

Both the EU and the US had their own vision for the TTC: for the Americans, it was a way to convince the Europeans to be tougher on China, and for the Europeans—with a pinch of hope—it was a way to seduce the Americans with their vision of regulating innovation and boosting trade.

This loose objective of the TTC has proven plastic enough to be agile, but also an obstacle to yielding concrete results at a speed that satisfies stakeholders and politicians. For this reason, as the year advances, both Europeans and Americans must reflect on the value of the TTC and prioritise the communication of positive outcomes.

Whereas there are clear gains in establishing the TTC as an independent entity, there are emerging areas relevant to international trade and geoeconomics in which the TTC could be of true impact. While the implementation of the Joint AI Roadmap will be a test case to see how far the TTC can go in influencing regulation, there are issues on which the TTC could act that are currently out of the agenda.

Though increased cooperation in quantum technologies was part of the communication distributed after the Luleå TTC meeting, there are only weak signs of advancing conversations about anticipatory issues affecting quantum innovation, including the societal impact. It is yet to be seen how the new Quantum Task Force advances on this matter at a moment where both the EU and the US look at quantum technologies through the lens of economic security—whether they use this terminology or not. Similarly, as digitalisation and space innovation advance, so do the economy and security of the EU and the US depend on space assets. There are clear opportunities in the TTC to discuss governance frameworks for NewSpace, such as moon mining or LEO constellations. As the electoral year unfolds, a TTC reform will be the only way ahead to ensure it remains immune to political change, stakeholder impatience, and international geopolitics.


US-EU Trade and Technology Council meeting in Leuven, Belgium, 4 and 5 April 2024.
Photo by Andrew Rogers, U.S. Mission to the European Union, via Wikimedia Commons.

## Endnotes

29 Joint AI Roadmap, https://digital-strategy.ec.europa.eu/en/library/ttc-joint-roadmap-trustworthy-ai-and-risk-management

30 TTC's main dilemma, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/us-eu-ttc-record-on-data-technology-issues/

31 Schrems II, https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

32 "legalise", https://cepa.org/comprehensive-reports/transatlantic-trade-and-technology-partners-or-rivals/

# Bridging the Digital Divide

## The Role of 6G and Immersive Technologies in Future Connectivity

**By Wiktor Sędkowski**, Expert, Warsaw Institute

### Introduction

The manner in which we communicate and access information has been transformed by the advancements in cellular technology. Recent decades brought about a remarkable evolution of mobile networks, from the earliest 2G cellular networks, which facilitated basic voice and text services, to the most recent 5G networks, which provide high-speed, low-latency connectivity. Through the introduction of 3G and 4G, there have been substantial advancements in the field, which have enabled the development of new mobile applications and services by facilitating faster data speeds and enhancing connectivity.

The digital world's increasing demands are presently being addressed by the 5G network, the current generation of mobile network technology. Although 5G rollout has not yet been globally completed, the 6G is in the research[33] and development phase, and is not anticipated to be completely operational until at least 2030. In comparison to 5G, the sixth generation of the network is expected to provide a wider spectrum of frequencies, **more reliable connections, lower latency, faster speeds, and improved security and privacy** features. It will facilitate the development of new capabilities, including holographic communications, virtual reality, high-resolution imaging and sensing, and ultrahigh-definition video streaming. These capabilities are essential for a new generation of mobile networks to support further evolution of technologies, such as artificial intelligence, virtual reality, haptics, and augmented reality.

Virtual reality, which has been in existence since the 1990s, is perhaps the best-known immersive technology. The reader may find it surprising, but the first VR machine was patented in 1962. The cubicle forming Sensorama[34] machinery was spacious enough to accommodate up to four individuals simultaneously. It integrated a variety of technologies to elicit a range of sensory responses, including colour 3D video, audio, vibrations, scent, and atmospheric effects such as wind. However, it was only in the past decade that VR became a more significant part of our personal and professional lives. VR is now used in a wide range of applications, from employee training to exceptional immersive entertainment experiences. 60 years after the invention of Sensorama, we are using head-mounted displays (HMD) with two near-eye displays used to supplant the user's surroundings with a digital environment in virtual reality (VR). This is a 3D environment that is entirely immersive and enclosed. And although this kind of VR is suitable for both industrial applications and creative experiences that incorporate novel narrative techniques, it will be further enhanced.

By merging the actual and the virtual worlds, augmented reality (AR) generates an immersive experience for users. The devices which have emerged in the current decade are capable of comprehending the "real world" in both spatial and semantic senses by utilizing computer vision and machine-learning algorithms. To some extent, AR already enables users to overlay digital objects in a physical space, thereby seamlessly merging the digital and physical realms.

AR and VR have the potential to be powerful instruments that can assist numerous disparate industries in providing more comprehensive and effective services to their customers and clients. Numerous AR and VR applications can influence better outcomes and stronger

connections with service providers and favourite brands. Both of these technologies can also provide safe and accessible ways to delve into a variety of new experiences, from life-changing healthcare applications to immersive ways to teach and learn[35].

Another set of immersive technologies is related to haptics, frequently referred to as kinaesthetic interaction or 3D touch. Unlike other immersive technologies, haptics employs tactile feedback, such as pressure, vibrations, and movements, to allow the user to "touch" the virtual environment, thereby enhancing the level of interaction to encompass multiple senses. Haptic feedback is classified into two primary categories: tactile and kinaesthetic. Kinaesthetic feedback is a term used to describe the forces and motions that influence the position and movement of the user's body or limbs. For instance, a force feedback joystick can offer kinaesthetic feedback by resisting or facilitating the user's movement. The sensations that impact the user's skin surface are referred to as tactile feedback. For instance, a vibrating phone can stimulate the user's contact receptors, thereby providing tactile feedback[36]. Obvious use cases for this technology are related to medicine, training, and entertainment. Through telemedicine or telesurgery systems, **haptic technology can facilitate remote diagnosis, treatment, or surgery**, enabling physicians to examine or operate on patients from a distance with haptic feedback. Haptic technology can facilitate virtual reality or augmented reality simulations for medical education or training, which could enable students or professionals to practice skills or procedures with haptic guidance or appraisal. It is probable that haptic technology will be one of the primary methods by which users will interface with applications and content in future computing paradigms, whether it be in the metaverse or spatial computing.

## Technology integration

Digital technologies, including haptics, AR, and VR, which were previously mentioned, can be summarized as extended reality (XR) and are classified as immersive technologies. XR technologies will have a substantial impact on the future of spatial computing, facilitating the transition from a current global data network with flat or restricted dimensions to an emergent immersive global data ecosystem that enhances performance and senses by providing virtual features to actual objects, and vice versa. To achieve this, enhancements both in policy and networking areas are needed. By implementing them, we will be able to establish a sustainable and secure physical world that is both digitalized and programmable, where humans are aided by intelligent devices and the Internet of Senses. E-healthcare, smart agriculture, Earth monitor, digital siblings, collaborative robots (cobots), and robot navigation are only examples taken from a long list of significant 6G use cases. The Internet of Senses, connected intelligent devices, a connected sustainable world, and their applications of course depend highly on the capabilities of the underlying network. Hence, the objective of the ongoing research on 6G is to develop solutions that are anticipated to deliver peak data rates of up to 100 Gbps, a tenfold increase compared to the current 5G standard. It is also estimated that latency will be substantially reduced, with 6G networks ensuring latency of less than 1 millisecond, which is five times lower than that of the fifth-generation network. This would facilitate the development of new applications that necessitate real-time data transfer, including remote surgery and fully self-driving vehicles. The utilization of new-spectrum frequencies and the optimization of signal efficiency (i.e., the primary objective of 6G networks, which will facilitate quicker and more dependable data transmission) are anticipated to result in superior coverage for 6G in comparison to 5G, enabling consumers in rural locations to access the developed XR services.

## New reality

One of the key challenges in deploying the 6G technology across the EU is the substantial infrastructure development required. This includes not only enhancing existing telecommunication networks, but also building advanced infrastructure to support higher-spectrum frequencies and ultralow latency requirements. Remote and rural areas, where locals already face connectivity challenges,

will need targeted investments to ensure equitable access. European research on 6G has been ongoing for several years already. Hexa-X, the European Commission's flagship research initiative for 6G, was officially launched in January 2021 under the leadership of Nokia. The project continues for the second iteration under the name Hexa-X-II[37] with a goal to establish Europe as a leader in 6G. High-tech advancements are pursued, with a focus on advancing technologies that contribute to a zero-carbon footprint, minimizing both energy consumption and the use of materials. The 6G project aims to increase connectivity for underserved populations, such as those in developing countries and marginalized communities within developed societies, in order to foster inclusion. Additionally, Hexa-X-II is dedicated to guaranteeing trustworthiness by emphasizing the robustness of network infrastructure, security, privacy, and data transparency. Thanks to those bases, the **immersive communication of 6G will provide the complete telepresence experience, eliminating distance as a restriction on interaction**. High-data rates and capacity, spatial mapping with precise positioning and sensing, and low latency end-to-end with periphery-cloud processing will allow multiple use cases related to extended reality technology to provide human-grade sensory feedback.

On the demand side, fostering innovation in business models and use cases will be crucial. There is a need to actively support start-ups and small-to-medium-sized enterprises that can leverage 6G's capabilities, such as holographic communications or ultrahigh-definition video streaming, to create compelling consumer applications. This includes promoting a vibrant ecosystem where new and traditional industries collaborate to develop scalable use cases.

The new form of service delivery to the end user will also require changes in the user equipment environment. Access to experiences and actions that are situated at a distance will be facilitated by personal immersive devices that are capable of precise bodily interaction, thereby better supporting human communication requirements. Simultaneously, **6G networks will introduce entirely new communication modalities** that are subject to strict control over access and identities.

## Policy recommendations

To bridge the global digital divide, we must **implement policies that prioritize connectivity for underserved populations**. This includes rural and remote areas in developed countries as well as communities in developing nations. The EU should support a **comprehensive digital inclusion initiative that leverages the advancements of 6G technologies to ensure equitable access to high-speed internet and emerging immersive services like extended reality (XR)**. This initiative must involve collaboration between public and private sectors, incentivizing investments in critical infrastructure for marginalized regions to promote inclusivity and equal opportunities in the digital economy.

Measures such as **digital skilling programs and targeted policy initiatives can play a pivotal role in driving user adoption of 6G-enabled services**. Programs like digital voucher schemes could incentivize businesses and individuals to invest in new technologies, while pan-European campaigns could raise awareness of the potential benefits of 6G. Such programs should be aligned with the European Union's 2030 Digital Decade targets to establish a strategic framework guiding 6G development. These targets emphasize universal gigabit connectivity and aim for a significant portion of the population to possess advanced digital skills. Aligning 6G development with these goals can amplify the impact.

With the proliferation of 6G networks, safeguarding data privacy and cybersecurity will be critical. The **EU should introduce robust policies that enforce stringent security protocols in network architecture, data processing, and storage**. This includes implementing end-to-end encryption, strong user authentication, and decentralized data governance frameworks. Additionally, 6G networks must incorporate advanced threat detection systems to pre-emptively mitigate cyber threats. Public awareness campaigns should educate citizens about digital safety, ensuring transparency and trustworthiness in handling personal and sensitive data.


Integrating 6G rollout with the EU's digital inclusion and sustainability initiatives should ensure that no region or demographic would be left behind. Moreover, the focus on green and energy-efficient technologies within 6G development needs to support the EU's broader climate goals.

By providing financial and regulatory support to start-ups and academic institutions focused on XR and other immersive technologies, the EU can position itself as a global leader in this field. Collaborative efforts between the private sector and educational institutions must be fostered to accelerate the commercialization and adoption of these technologies across all industries. Similarly to the proposed dedicated AI research initiative[38], the EU should create a program across all member states to establish research and implementation offices inside existing technological centres. Such offices would provide assistance to start-ups and academia with XR development or implementation.

## Endnotes

33 3GPP, 3GPP Commits to Develop 6G Specifications, https://www.3gpp.org/news-events/3gpp-news/partner-pr-6g, access: 8. 10. 2024.

34 Unsung History, The Sensorama—The Precursor to Virtual Reality Technology, https://www.youtube.com/watch?v=zf61nlyBC3M, accessed: 8. 10. 2024.

35 Forbes, AR And VR For A Better CX, https://www.forbes.com/councils/forbestechcouncil/2024/01/29/ar-and-vr-for-a-better-cx-15-tech-experts-on-practical-use-cases/, accessed: 8. 10. 2024.

36 Stanney Joseph, The Innovation and Application of Haptic Technology, https://medium.com/@staneyjoseph.in/the-innovation-and-application-of-haptic-technology-8daa45327764, accessed: 8. 10. 2024.

37 Hexa-X-II, the second phase of the European 6G flagship initiative, https://hexa-x.eu/hexa-x-ii-the-second-phase-of-the-european-6g-flagship-initiative/, accessed: 8.10.2024.

38 Mario Guvo, Europe between Globalization and Localization, Improving Europe's Competitiveness, CEP 2024.

# ‘C’ in CEE Stands for ‘Cyber’

## Case Study of Cybersecurity Cooperation in the Region

**By Ewelina Kasprzyk**,Expert, Kościuszko Institute

With the growing importance of cybersecurity and its global recognition as a key challenge, we have observed the establishment of many frameworks and initiatives focusing on international and intersectoral cooperation. Many of these include the CEE countries; however, none seem to be focused specifically on regional cybersecurity. From NATO and EU, through the Three Seas Initiative, to bilateral frameworks—the CEE countries strive to somehow find their place and identity within those diverse partnerships with oftentimes different experience and interests.

The CEE region can—and should—leverage its potential to create a safer and more resilient cyber ecosystem. Cooperation with international partners is one way to do so, but it is time to see whether and why purely regional efforts may be a viable alternative. This carries an even bigger meaning in the context of Ukraine, as the CEE could become the link that helps Ukraine in its EU accession processes, which include a variety of cyber and ICT preconditions.

The region has the potential to become a cyber power, but this can only be done through cooperation. This chapter examines selected cooperation frameworks engaging CEE countries and characterizes their cybersecurity activities. It also attempts to answer the following question: does the CEE need its own regional cybersecurity initiative?

CEE has many faces—and many definitions. The list of countries considered to be part of the region varies from source to source, and in many cases depends on the context and perspective. For the purposes of this article and data use, we will define the CEE region as consisting of the following countries as listed by the OECD: Albania, Bulgaria, Croatia, the Czech Republic, Hungary, Poland, Romania, the Slovak Republic, Slovenia, and the three Baltic States: Estonia, Latvia, and Lithuania. The article will also include Ukraine, as a natural partner of the region and, hopefully, with its accession to the EU, soon a member of the community.

### The Many Faces of Cybersecurity Cooperation

Cybersecurity has become a key item on the agenda of existing organisations and also a driver behind the establishment of new initiatives focusing primarily on cyberspace. The CEE countries are involved in quite a few of them on varying levels.

#### 1. NATO

Cyber defence is one of NATO’s core tasks, aiming to build cyber capabilities, provide a platform for consultation and information sharing, and also enable collective action (including the potential cyber article 5).

NATO has employed a variety of mechanisms to strengthen its cyber potential and commitment to promoting peaceful cyberspace, for example through the recognition of cyberspace as a domain of operations, the Cyber Defence Pledge, or the Comprehensive Cyber Defence Policy.

A key component of NATO’s cyber posture is the **NATO Cooperative Cyber Defence Centre of Excellence**, established after the 2007 cyberattacks on Estonia. All 12 CEE countries considered in this article are among 30 Sponsoring Nations of the NATO CCDCOE, while Ukraine holds a contributing partner status (as a non-NATO member).

At the 2023 NATO Summit in Vilnius, Allies launched a new initiative called the **Virtual Cyber Incident Support Capability**, which aims to support member states in their re-

sponse to malicious cyber activities through real-time cooperation. The VCISC was tested during the Summit itself, engaging Spain, Norway, Belgium, Netherlands, Turkey, and 6 CEE countries: Lithuania, Poland, Slovakia, Slovenia, Estonia, and Albania.

Cybersecurity is also one of the technology domains of the **Defence Innovation Accelerator for the North Atlantic**. Currently, one CEE country is home to a DIANA accelerator (Estonia), and test centres are located in nearly all CEE countries (besides Albania, Croatia, and Czechia), with six of them set to specialize in cyber and cybersecurity (Estonia, Lithuania, Poland, Slovakia, Hungary, and Slovenia).[39]

Solutions created through DIANA may be eligible for funding from the **NATO Innovation Fund**, established by 22 NATO countries (including Bulgaria, Czechia, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, and Slovakia). The NIF will prioritise projects by countries participating in the Fund, so the CEE region may count on big investments from NATO.

### 2. European Union

The EU is also heavily engaged in building cyber capabilities and fostering cooperation in this field. Through policies and legislations, such as **the Cybersecurity Strategy, the NIS2 Directive, the Cyber Resilience Act, and the Cyber Solidarity Act**, the EU aims to build national and collective capabilities and ensure that all member states have the means to protect themselves and the Union as a whole against potential threats in cyberspace.

With regards to cooperation, the European Commission has released **the Blueprint for Rapid Emergency Response and the Cyber Diplomacy Toolbox**. The **Joint Cyber Unit** will serve as a platform for coordinating the response to cyberattacks and assist member states in recovery. Within **Permanent Structured Cooperation (PESCO)**, there are a few cyber-focused projects, such as Cyber Rapid Response Teams and Mutual Assistance in Cyber Security, which engage CEE countries like Lithuania, Poland, and Slovenia. **The EU Policy on Cyber Defence** also highlights the need for stronger cooperation between member states, in particular military and civilian cyber communities, as well as the private sector.

Cooperation is also the key to **cyber capacity building efforts in third countries**, including Western Balkan and Eastern Partnership states which are oftentimes considered part of the CEE region.

The CEE countries are recognized as key players in the EU's efforts, thanks to the region's potential and capabilities. A symbolic sign of that was the establishment of the **European Cybersecurity Competence Centre** in Bucharest, Romania, which aims to enhance regional cooperation through the Network of National Coordination Centres (NCCs). The Network so far consists of most CEE countries, which are also EU member states, besides Hungary.

**Cooperation in the EU equals community**. Therefore, most activities aim to establish swift communication—between member states, cyber response teams, actors like private companies, universities, and NGOs. Public-private partnerships are a part of that, which is proven by the activities performed by organizations like **ECSO** and **Women4Cyber**, which also engage CEE countries.

### 3. Three Seas Initiative

Probably the closest thing to a CEE-wide framework handling cybersecurity issues is the **Three Seas Initiative**. As of 2023, it has consisted of 13 member states—Austria, Bulgaria, Croatia, Czechia, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia, Slovenia, and the latest addition Greece, while Moldova and Ukraine hold the partner-participant status.

The Three Seas Initiative is based on three pillars—transport, energy, and digital. Among projects developed under the 3SI, we can find many digital programs; however, none of them is focused solely on cybersecurity.

**The COVID pandemic and the war in Ukraine have changed the Initiative's perception of cybersecurity. The former brought a realiza-**

**tion of how truly vulnerable to digital and cyber threats we are as a society, while the latter has highlighted both the threats and the new security role of the region in the face of Russian imperialism enhanced by hybrid warfare.**

With the rise of threats from the Kremlin, more and more regional experts have been calling for an increased interest in cyber resilience of the region. Minister Janusz Cieszynski underlined the need for collaboration in the face of new challenges on the digital front: "Since the war in Ukraine broke out, cybercrime has been on the rise in Poland and other countries of the region. We need to protect our citizens from relentless attacks from Russian-funded hacking groups. To fight cybercrime effectively, we need to cooperate and share information[40]." His words were echoed by Paweł Jabłoński, former Plenipotentiary of the Polish Government for the Three Seas Initiative, who highlighted both promoting emerging cybersecurity solutions made in the region to the global level and fostering closer collaboration between IT sectors to achieve regional goals as priorities for the 3SI.[41]

Despite those calls and a seemingly united stance on cybersecurity being a priority for the 3SI, we have yet to see a program within the Initiative that focuses on this specific goal. Moreover, due to the lack of success with projects (some of which have been ongoing for years without achieving any goals, or put on hold), many experts view the 3SI as a weak initiative with no real power. It is, still, the one platform that focuses on the CEE region and its needs.

## 4. Other regional initiatives

**The Central European Cybersecurity Platform (CECSP)** was established a decade ago and consists of five countries: Czechia, Austria, Slovakia, Hungary, and Poland. The platform was supposed to enhance cooperation in cybersecurity, mostly through the exchange of information and know-how, to build national capabilities, but also strengthen the group's position in the international setting. However, the last mentions of the CECSP are from 2020 and 2021[42], with no further updates about its activities.

Then, there is **the Visegrad Group**, whose main goal is to coordinate policy at a sub-regional level. Cybersecurity is not an area of activity of the V4 group, as the countries focus more on transport, energy security, or environmental protection. As EU and NATO member states, and also creators of their own national cybersecurity strategies, the V4 see no need to issue group cybersecurity laws. Instead, the V4 released joint declarations, such as the Warsaw Declaration, which highlighted the role of cybersecurity in ensuring stable economic growth for the region.[43] The last few years, however, have been quite challenging for the V4, as the group differed on a variety of issues, from migration policies to their stance on Russia, building tensions in the CEE and between the region and the EU.

## 5. Multi- and bilateral initiatives

Some CEE countries are involved in other international initiatives focusing on cooperation in the field of cybersecurity. A notable example is the **Tallinn Mechanism**, formalized on December 20, 2023. The Mechanism was established with one goal in mind—to help Ukraine fight Russia on the cyber front. It aims to do so by coordinating civilian cyber capacity building (CCB), complementary to military CCB. Activities within the Mechanism will be carried out in full coordination with Ukraine and with respect for international laws.

The Tallinn Mechanism was endorsed by Canada, Denmark, France, Germany, the Netherlands, Sweden, United Kingdom, the United States, as well as Estonia and Poland, both of which had been closely cooperating with Ukraine even before the Russian invasion. While Poland has established the back office of the Mechanism in Warsaw, Estonia runs the front office in Kyiv and has already announced plans to allocate EUR 500 000 from the 2024 development cooperation budget.[44] The EU and NATO will act as Observers in the Mechanism, with private sector and non-governmental actors also invited to contribute to the mission.

In addition, as for bilateral and multilateral initiatives, CEE countries signed many MoUs on cybersecurity cooperation, such as:

• the Memorandum of Understanding on the pooling and sharing of their respective cyber range capabilities (part of the Cyber Ranges Federation Project run by the European Defence Agency)—signed by Austria, Belgium, Estonia, Finland, Germany, and Latvia;
• Memorandum of Understanding on Cooperation in Cybersecurity—signed by Estonia, Latvia, and Lithuania;
• Memorandum of Understanding, a broad framework for cooperation in the area of cybersecurity in addressing threats posed in cyberspace—signed by Romania and Slovakia.

**In the past few years, however, most activities and mechanisms built with cybersecurity cooperation in mind were created on the EU or NATO grounds. This brings us to the following question: does the CEE need to have a separate set of cybersecurity cooperation projects?**

## The case for cybersecurity cooperation in CEE

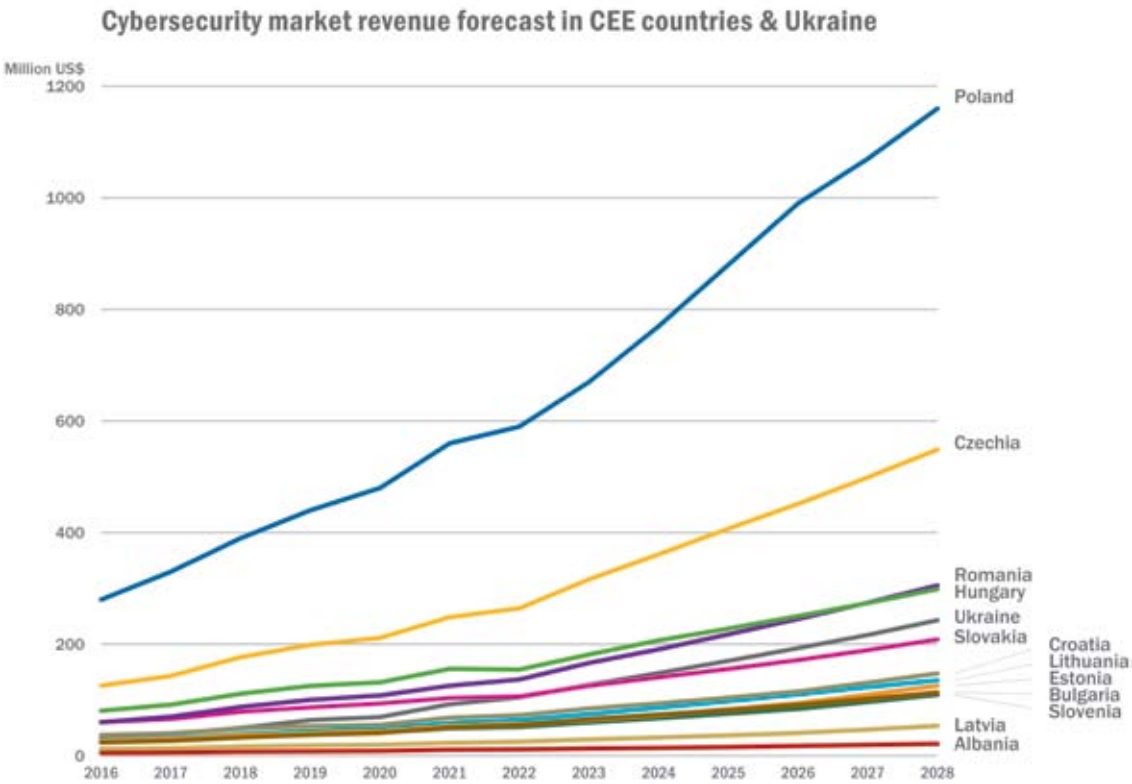
Most of the CEE countries from the OECD list are EU and/or NATO members. However, if we take a broader look at the region and notice countries like Ukraine, Moldova, Armenia, or Georgia, which match geographically, but are not members of neither the EU nor NATO, that is where it gets complicated. Moreover, Russia and Belarus could also be considered CEE countries and, as of now, most countries cannot imagine closer cooperation with any of them, not when Ukraine is still being attacked in its physical and cyber realms. Therefore, one thing that could potentially be an obstacle in drafting and developing cybersecurity cooperation in the region is its definition.

Then, we need to take into consideration the maturity of cybersecurity environments in the region—which varies from country to country. For example, the National Cyber Security Index positions for the CEE countries in 2023[45] looked as follows:

| Rank | Country | Index points |
|---|---|---|
| 2 | Lithuania | 93.51 |
| 3 | Estonia | 93.51 |
| 4 | Czechia | 90.91 |
| 6 | Romania | 89.61 |
| 11 | Poland | 87.01 |
| 18 | Croatia | 83.12 |
| 19 | Slovakia | 83.12 |
| 24 | Ukraine | 75.32 |
| 25 | Latvia | 75.32 |
| 28 | Bulgaria | 74.03 |
| 37 | Hungary | 67.53 |
| 38 | Slovenia | 67.53 |
| 54 | Albania | 62.34 |

The e-Governance Academy has updated its methodology and is currently working on the new ranking for 2024—based on preliminary data from first country entries, we can expect a few CEE states to change their positions in the ranking, with Poland likely entering the top five. Still, there are two points to be made here: one, the gap between the countries that are at the top and at the bottom of the list is quite significant; and two, countries from outside the OECD list are close to the ranks of the 12 CEE states (Serbia—rank 21, Kosovo—rank 34, Georgia—rank 44, and Moldova—rank 62).

We can see similar disparities in the economic aspects of cybersecurity, as CEE countries generate steadily growing, but varying revenues (based on Statista's data[46]):




Statista's forecasts for the next four years also show varying CAGR, ranging from 14.62% to 9.63%, which speaks volumes about the maturity of the markets, their potential, and their attractiveness to investors:

| Country | CAGR 2024-2028 | Revenue by 2028 US$ |
|---|---|---|
| Estonia | 14.62% | 125.70M |
| Ukraine | 13.84% | 243.03M |
| Latvia | 13.02% | 53.65M |
| Slovenia | 13.02% | 109.40M |
| Romania | 12.48% | 305.20M |
| Lithuania | 11.98% | 135.50M |
| Croatia | 11.93% | 147.70M |
| Czechia | 11.65% | 549.00M |
| Poland | 11.60% | 1160.00M |
| Bulgaria | 11.48% | 113.50M |
| Albania | 10.87% | 21.58M |
| Slovakia | 10.33% | 208.50M |
| Hungary | 9.63% | 298.70M |

When it comes to the maturity of cybersecurity markets, the CEE countries seemingly have one thing in common—the level of awareness and preparedness for cyber threats. The approach to cybersecurity is changing, with more and more companies investing in technical cybersecurity measures, employing dedicated teams, and training their staff. A PWC report suggests significant progress in areas like operational technology security, value and efficiency of cyber resources, and, finally, the embedding of security and privacy into new products and services. Furthermore, nearly half of the businesses plan to increase their cybersecurity budgets.[47]

However, there is still a lot of room for improvement. In the same report, PWC claims only 31% of surveyed CEE businesses feel very confident in their current risk mitigation strategies. Experts underline that especially small private sector companies tend to be unaware of the risks and lack key cybersecurity competences. "Only one in five SME companies in Europe have informed or trained their employ-

ees on cyber threats," said Michał Kanownik, President of the Digital Poland Association.[48] Capacity-building is one of the key goals of cooperation initiatives, and perhaps it should be a driver of cooperation in the region.

When considering the case for cybersecurity cooperation in the CEE, we have to also acknowledge its evolution. For years, the region was seen as the source of cheap labour for global companies and Western Europe. With time, the CEE started to showcase its potential as a technology hub, full of blooming start-ups and SMEs, and a great talent pool. More recently, with the increasing tensions and then Russia's full-scale invasion of Ukraine, the CEE has become a frontline for cyber and hybrid warfare, which has broader security implications for the EU and NATO.

Now, regional cooperation in the CEE is more security-oriented than technology-based. Russia's invasion of Ukraine caused NATO's centre of gravity to shift towards the Eastern Flank, which includes many of the CEE countries, namely Estonia, Latvia, Lithuania, Poland, Slovakia, Hungary, Romania, Bulgaria, and the newest addition to the Alliance —Finland.

Perhaps this new security-oriented cooperation in the CEE region will shape its identity. This, however, could further isolate some countries from the conversation—countries which need to catch up in terms of tech development and economic growth, or focus more on the internal and neighbouring issues instead of broader regional or global perspectives. Membership in the EU and NATO has allowed some states to progress in a way that other countries may only dream of. New standards have been set, many of which are currently unattainable to those outside the EU and NATO.

Countries of the broader CEE region share many experiences, history, social issues, and economic trends. The direction they have taken—whether towards or away from the EU and NATO—has shaped their present. Cooperation through capacity-building, information-sharing, and exchange of best practices may shape their future.

## Conclusions

The CEE region is very diverse, despite shared experiences. Capacity-building, information-sharing, joint cyber exercises, shared projects and investments, establishing working relations, and close communication can help minimize those differences. This is only attainable through cooperation, which can be achieved in three ways: through broader platforms like the EU or NATO, through regional initiatives focusing on the region like the 3SI, or by expanding beyond the EU/NATO membership and collaborating with other countries from the region, such as the Western Balkans. To ensure that the CEE realizes its full potential, the three ways should be treated as complementary and equally important.

There is no need to create new organisations or platforms for regional cooperation. The Three Seas Initiative, supplemented by EU and NATO efforts, is good enough—but the member states need to push for more cooperation, stronger focus on cybersecurity, and inclusion of other countries, especially neighbours and partners. Cybersecurity is a team game—the more like-minded countries and actors decide to cooperate and build common cyber capabilities, the more secure cyberspace gets.

## Policy recommendations

• organize cooperation in a more institutionalized way. Combine the opportunities provided by the EU, NATO, and 3SI platforms to not only discuss cybersecurity challenges, but also establish effective cooperation in the region—and for the region;
• ensure international and intersectoral cooperation with trusted partners. Cybersecurity cooperation in the CEE should engage credible public, private, NGO, and academia players. Leverage the presence of global tech companies, while promoting technology made in CEE;
• focus on Ukraine. Cybersecurity projects in the region should engage Ukraine, leading to closer cooperation, exchange of best practices, and capacity-building, but also positioning the CEE as the enabler and supporter of Ukraine's activity and membership in international organizations;
• strive for broader regional cooperation. Western Balkan and Eastern Partnership countries should not be left out, as cooperation may not only advance their national capabilities and open the door to closer cooperation with the EU or NATO, but also increase the regional cyber resilience;
• secure funding. Besides national budgets, the CEE countries should try to leverage EU funds as well as investments from like-minded partners outside the region to secure funding for cybersecurity projects;
• attract young talents. Cybersecurity projects should focus on promoting innovation among young professionals, bridging skill gaps, and building trust in digital solutions, to ensure the influx of high-trained workers.

## Endnotes

39 NATO DIANA, DIANA Network: Test Centres, Map from July 20, 2023, https://www.diana.nato.int/resources/site1/general/maps/diana-test-centres-en_v5.pdf.

40 CEE Digital Summit, Cybersecurity is a priority for the Three Seas Initiative. The region's authorities and private sector discussed digital threats during a conference held in Bucharest, https://ceedigitalsummit.com/Cybersecurity-is-a-priority-for-the-Three-Seas-Initiative-The-regions-authorities-and-private-sector-discussed-digital-threats-during-a-conference-held-in-Bucharest.html.

41 Ibidem.

42 Sejm, Meeting of the Speakers of V4 Parliaments—report, https://www.sejm.gov.pl/Sejm9.nsf/v4Komunikat.xsp?documentId=E8F3F7FFD693E85CC12586C00027D857&lang=EN.

43 Federica Cristani, Building up Cybersecurity Policies in the Visegrad Region: Which Cooperation?, https://www.iir.cz/building-up-cybersecurity-policies-in-the-visegrad-region-which-cooperation.

44 Ministry of Foreign Affair, Republic of Estonia, Tallinn Mechanism, https://www.vm.ee/en/international-law-cyber-diplomacy/cyber-diplomacy/tallinn-mechanism.

45 E-Governance Academy, National Cyber Security Index, 2023 edition, https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1.

46 Statista, Cybersecurity—Worldwide, https://www.statista.com/outlook/tmo/cybersecurity/worldwide.

47 PWC, CEE findings from the 2023 Global Digital Trust Insights Survey, https://www.pwc.com/c1/en/2023-cee-digital-trust-insights.html.

48 CEE Digital Summit, op.cit.

CENTER ZA EVROPSKO PRIHODNOST

CENTRE FOR EUROPEAN PERSPECTIVE

CEP

www.cep.si


CENTER
ZA EVROPSKO
PRIHODNOST
CENTRE
FOR EUROPEAN
PERSPECTIVE
CEP