

Artificial Intelligence in the Visegrad 4: Emerging Strategies, Uncoordinated Approaches

Alex Hardy

Abstract

Contemporary research has hailed the ‘transformative potential’ of artificial intelligence (AI) across all aspects of society (Stevens, 2021 & Payne, 2018). Yet many states are either underprepared or lack the proper legal frameworks to address the challenges of AI in the public sphere. This paper presents a comparative overview of the current Visegrad state’s (V4) AI landscape, charting key political and organisational developments, as well as highlighting key public sector actors. Existing research on the use of AI for public services has indicated that it can be used to make existing processes more efficient and accurate (Berryhill et al, 2019). The paper focuses on the key AI policy goals of each state, illuminating existing AI use cases across government and other areas of society.

This paper also offers reflections on where the AI policy of the Visegrad states currently stands comparatively, and how it intertwines with national security concerns. It notes the social, economic, political, and regulatory upheaval that the increased use of AI presents to the V4, and identifies the potential risks this poses. Findings are drawn from a series of interviews conducted with participants from some of the region’s key public institutions and research groups. It concludes that while AI policy in the Visegrad states remains in its infancy, it would be best served by developing further regional collaboration and following the recommendations of OECD reports which suggest that all public-facing AI services ought to be guided by the principles of ethics, transparency, and security (Berryhill et al, 2019).

This analysis was produced within the Think Visegrád Non-V4 Fellowship programme.

Think Visegrád – V4 Think Tank Platform is a network for structured dialog on issues of strategic regional importance. The network analyses key issues for the Visegrád Group, and provides recommendations to the governments of V4 countries, the annual presidencies of the group, and the International Visegrád Fund.

For more information about Think Visegrád and its members visit www.thinkvisegrad.org.

Introduction

The rapid growth of artificial intelligence (AI) globally poses a number of key challenges to many states. These challenges include ethical challenges of how AI should be used, regulatory challenges of how AI should be governed, and security challenges of how risks posed by this rapid advancement of technology might be countered. While all states face such dilemmas, small and medium-sized states are particularly susceptible to the risks posed by artificial intelligence or digital innovation more generally, as they face numerous issues such as a limited talent pool, limited budgets, and low control of the supply chain (Burton, 2013). This is primarily due to the nature of technological innovation as being primarily driven by larger states. In the case of AI, the United States and China. Conversely, however, small states can also drive innovation, acting as ‘norm entrepreneurs’ and expanding their influence through specialisation in specific policy areas (Adams, 2019).

This research paper outlines some of the policy options available to the Visegrad states (V4) relating to the use of AI in the public sphere. It provides an overview of AI in the V4, noting some of the region’s key active use cases. It also highlights some of the risks to the region, and ways in which those risks might be mitigated. To achieve this, the research accesses numerous policy documents, secondary data, existing research, and conducted a number of informal interviews with figures from government, civil society organisations, and research institutes. Participants were posed questions such as ‘What can the Visegrad governments do to facilitate better AI development?’, ‘What are the biggest risks the Visegrad states face in the field of AI?’, and ‘Which states should the Visegrad states seek closer collaboration with? And which should they avoid?’. These answers, alongside supporting data, inform the subsequent analysis of this paper.

It is important to note that the AI landscape of the V4, as with many other European states, is rapidly changing. This research was conducted between October and November of 2021 and reflects the AI landscape of the V4 at the time of writing. The paper offers a number of conclusions relating to the current AI landscape and potential risks and offers a number of policy recommendations for the V4 states going forward.

Current AI in The V4:

Whilst in their infancy in the V4, public-facing AI services can hold many potential benefits, which are similar to the benefits of conventional digitalised public services (Robinson, Hardy & Ertan, 2022:

forthcoming). These include the reduction of public sector costs, the reduction of bureaucracy, decreased response times, and the enhancement of existing public services.

| State | National Strategy | Active Use Cases | Notable Civil Society Organisations | Notable Research Groups |
|-------|---|------------------|--|---|
| SK | Published July '19 (as part of wider digitalisation strategy) | 7 | AI Slovakia, KInIT | Department of Cybernetics and AI, University of Košice, KInIT |
| HU | Published September '20 | 1 | Hungarian AI Coalition | MTE-SZTE Research Group on Artificial Intelligence |
| PL | Published December '20 (Polish only) | 10 | AI Poland, Digital Poland Project Centre | AI Tech Scientific Consortium (Collaboration between Universities of Warsaw and Jagiellonian University [Krakow] and AGH University [Krakow]) |
| CZ | Published May '19 | 3 | Czech Invest, AI Czechia | The AI Centre, CTU (Czech Technical University) |

Figure 1: Diagram illustrating current AI Landscape of the V4 (For statistics, see Misuraca, 2020)

As illustrated in figure 1, the AI landscape of the V4 is very much a work in progress and rapidly developing. All of the V4 states implemented their first national AI strategy between 2019-2020. There are some noteworthy caveats. Poland, for example, has authored a full strategy, however, this is only available in Polish. Slovakia, meanwhile, has a strategy for AI within its much larger Digitalisation Strategy. The Czech Republic was the first of the V4 states to introduce an AI strategy in May 2019, and Poland was the last in December 2020.

Much of these documents are perhaps striking by their similarity. Some basic content analysis of the strategies highlights a number of shared strategic goals and common ground between the four countries. This includes the prioritisation of, and investment in research and education, the development of additional public services, and building closer collaboration with allied nations. That said, as illustrated in Figure 1 above, there are notable disparities in existing public-facing AI

services. It is also noteworthy that there is little mention of collaboration with each state's Visegrad neighbours. Only the Slovak and Polish strategies mention Visegrad collaboration at all. The Slovak and Czech strategies place a far greater emphasis on collaboration at an EU level, whilst only Poland mentions NATO.



Figure 2. What the EU's Capitals think of the AI Act (Heikkilä, 2021)

Additionally, the EU-wide 'AI Act' is currently in its legislative stage. As illustrated in Figure 2 below, there is also a lack of coordination on desired goals for this Act among the Visegrad states. Reports suggest that Slovakia, for example, is more cautious in terms of the regulation of private AI developers. Poland strongly favours a focus on innovation and small-medium enterprises. The Czech Republic and Hungary are outspoken in their opposition to facial recognition technology. These diverging priorities reflect a situation generally across Europe, and confirmed by interview participants, that as things stand, artificial intelligence remains a state-level concern, and few states are thinking across the internal borders of the European Union in terms of developing citizen-facing AI solutions.

AI scientific publications

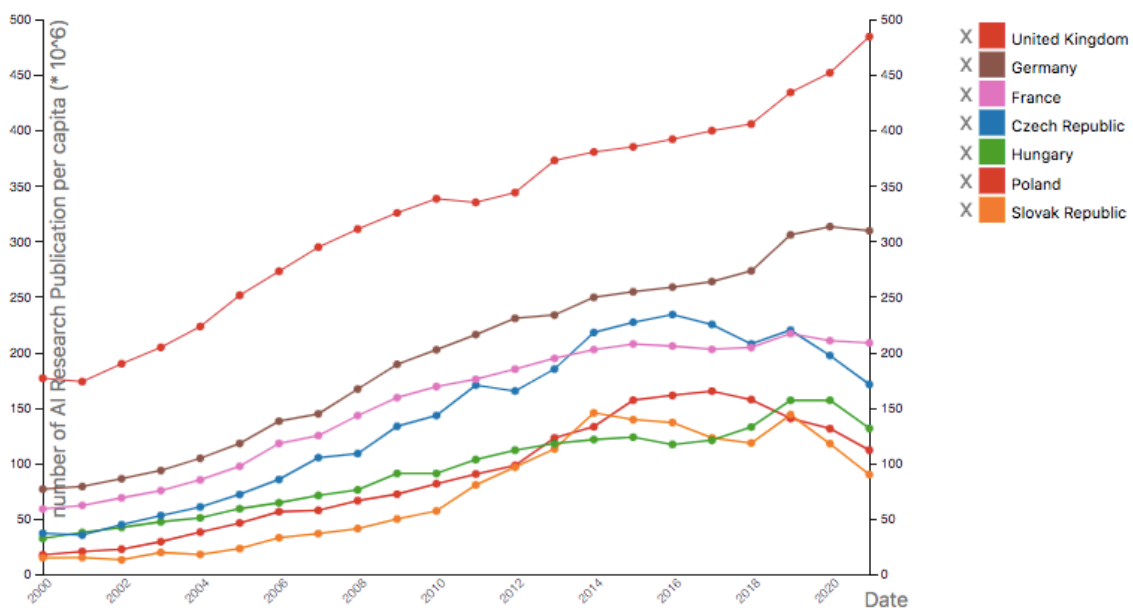
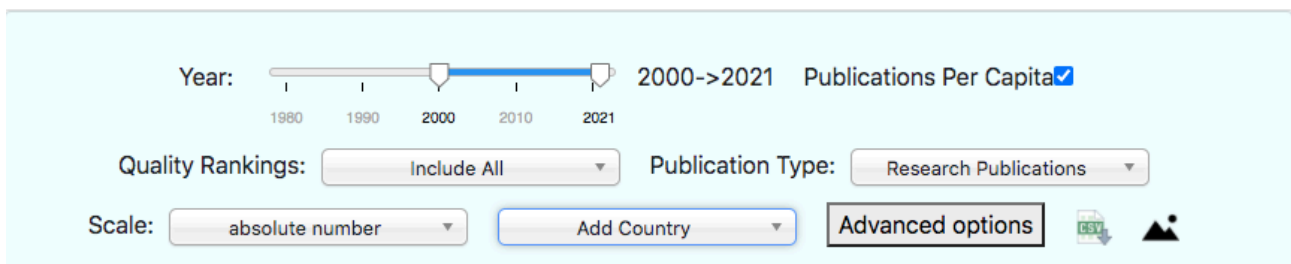


Figure 3. AI Research Publications - An East/West Divide? Source: OECD.AI

Whilst all of the V4 states place significant emphasis in their strategies upon education and innovation through research (a common cause identified by all research participants as something that the V4 ‘could do better’), when the research output of the V4 states is compared to the rest of Europe (per capita), there is significant ground to make up. As might be expected, there is something of an ‘East-West’ divide within Europe in terms of research output, as illustrated in Figure 3 above. There is also some disparity between the V4 countries, with the Czech Republic publishing the most AI-focused research per capita, and Slovakia the least.

It is also important to note that there are a relatively limited number of public-facing and active use cases within the region (A use case being a single scenario or instance in which technology is used). Below, some notable existing use cases are highlighted in Figure 4.

| Use Case | State | Detail |
|--|-------|---|
| Covid-19 Chatbot | CZ | Automated chatbot designed to answer common questions about the Covid-19 pandemic and relay important information |
| Semantic Concept-Discovery Solution | SK | Tool for natural language processing (NLP)- this use case helps users browse and locate relevant data. Speeds up governmental processes and aids classification. |
| 1818 Public Administration Chatbot | HU | Automated chatbot Provides information regarding public administration (both local and national level). |
| Unemployment Profiling [Now Abandoned] | PL | Algorithmic decision-making to direct unemployed persons towards potential employment - Targets groups which may have been out of work for some time such as women following pregnancy, 'low-qualified' individuals |

Figure 4. Examples of AI Use Cases from the V4 (Misuraca & Van Noordt, 2020 & Csótó et al, 2021)

It is important to note that, right now, the most common public-facing AI use cases are quite unsophisticated and simple chatbots (Around 25% of all AI services EU-wide are chatbots, and these are highlighted above in the Czech Republic and Hungary). However, the list of services is ever-expanding and includes predictive analytics, robotics, autonomous vehicles, and more. An overview of these public-facing services across the EU can be found at Misuraca & Van Noordt (2020).

The V4 strategies are all ambitious in further expanding services and providing public-facing AI soon. Hungary promises to expand its chatbot customer service, while also offering precision agriculture applications, forecasting maintenance systems, medical diagnostics, as well as the introduction of public-facing KIOSK's (service terminals), where citizens can access a plethora of automated services (See Csótó, Rupp, and Petényi, 2021 for further information on the Hungarian AI landscape). In order to further facilitate the development of AI in the public sphere, all of the V4 states have supported and invested in the development of civil society organisations promoting the use of AI across society.

These organisations are also recipients of EU funding. In Slovakia, these organisations include KInIT and AI slovakIA. The Czech strategy outlines an exhaustive list of institutions working with AI in Czech Rep, including a number of Public-Private Partnerships (PPP's). It also promotes the use of 'new regional cooperation platforms' (but does not mention enhanced Visegrad cooperation). Prg.Ai promotes a vision of the city of Prague as a potential 'AI hub'. In Poland, 'Poland AI' seeks to 'promote the Polish AI ecosystem' and forward 'collaboration with foreign entities'. Poland, as noted in Figure 1, currently leads the V4 in terms of public-facing service implementation, and is seeking active collaboration using Polish approaches.

As established earlier, public-facing AI in the V4, as across Europe, is in its infancy. There are a number of benefits and potential services that this section has highlighted. Nevertheless, there are also a number of risks posed by the growing use of AI in the public sector, as outlined in the following section.

Notable challenges

An OECD report by Berryhill et al (2019) notes three key challenges of AI development in the public sphere. Notably that it be ethical, trustworthy, and secure. This is contested in terms of service implementation. A recent investigation of Polish unemployment profiling (a use case highlighted in the prior section of this paper) found that while supposed safeguards had been put in place to check the automated decision making within the service, this was being undertaken on less than 1% of all decisions (Kuziemski & Misuraca, 2020). This study found that those responsible for safeguarding did not feel like they could challenge the process as it was supposedly 'objective'. Many unemployed people complained that the system was unfair. Subsequently, this use case has now been abandoned and serves as an important reminder of the importance of oversight, ethics, and trust in service provision.

When discussing public services, security should also form a crucial part of the decision-making process. This relates to the security of the service itself, the security of citizen/users, and national security. This research unearthed a number of key security concerns or perceived risks. These included, notably, the perceived risk of Chinese influence via an increased reliance upon Chinese technology. Notably, there has been a development of links between Košice Technical University and Huawei (Central Register Slovakia, 2021). The Hungarian government has similarly signed a 'memorandum of agreement' with Huawei (Budapest Business Journal, 2021). Some reporting has highlighted this is problematic, particularly noting Huawei's role in developing facial recognition

technologies for the Chinese government to identify the racial features of the Uyghur — a noted minority said to be ‘at risk’ of persecution (Šimalčík, 2021). The United Kingdom has insisted that telecommunications providers must not install Huawei equipment on the nation’s 5G network. Huawei has been classified by the UK as a ‘high-risk vendor’ due to close links to the Chinese state (BBC News, 2021). Similarly, the United States has declared Huawei ‘inseparable’ from the Chinese Communist Party (Ovide, 2021).

Many of the concerns over Huawei and the role of the Chinese government are related to supply chain security and that weaknesses could exist, undetected, allowing for potential espionage. Likewise, there has been some concern over Huawei officials. In a recent incident, a Huawei employee was arrested on spying charges in Poland (Cilluffo & Cardash, 2019) furthering suspicions of close links between the state and Huawei. There are also wider concerns that allowing Huawei to invest heavily in projects creates a dependency, and thus represents a security risk. Similarly, the spread of Chinese expertise expands the influence of the Chinese state in an increasingly multipolar world.

Of other noted potential risks, Russia is perhaps the state most commonly seen as a threat to European security in many spheres (including cyber security), yet is generally not considered as a threatening actor in the world of AI. Existing research suggests that Russia lags far behind the United States and China in developing AI solutions of its own, and is not particularly keen on overseas investment (Markotkin & Chernenko, 2020). Instead, whilst Vladimir Putin has highlighted the importance of AI development, Russian interests in AI have generally focused on the military sphere, including the development of autonomous fighter jets (Bennett, 2021).

Converse to risks identified above, some of the regional experts the research consulted felt that challenges lay closer to home, and were often less geopolitical in nature. Some participants suggested that existing national legislation was too prohibitive and ‘stifled innovation’ in the region. There was also a feeling expressed that the tech community was not consulted generally in the process of developing norms and that Europe (and as a consequence, the V4 states) would fall further behind the US and China competitively. This, it was acknowledged, was a risk, but was considered secondary to the monopolisation of the market by large corporations, which created a reliance on certain software. One participant felt that the V4 was too reliant upon the US generally. Most stressed the need for the V4 states to be independent actors and be less dependent.

Another notable challenge for the V4 states (and all small to medium-sized states more generally) is the idea of the ‘brain drain’, whereby talented individuals are inevitably drawn to larger nations (and

Silicon Valley in particular) due to increased professional opportunities and higher rates of pay. To some degree, this is an inevitable phenomenon as smaller states cannot (and arguably should not) attempt to compete with the salaries of Silicon Valley (echoed by Eeckhout, Hedtrich, & Pinheiro, 2021, who suggest new tech is a key driver of urban inequality). Research participants agreed that rather than attempting to directly resolve the ‘brain drain’ by subsidies, building resilience was instead a more desirable approach. This meant a mixture of being more attentive and accommodating to the tech industry, but also providing an increased talent pool through research funding and encouraging innovation.

Finally, and perhaps most crucially, a key risk to be considered is the erosion of public trust in governance. Public-facing AI services are destined to fail if citizens fundamentally distrust their government. Interview participants felt that trust could be enhanced by ensuring high standards of transparency and legality. Waller & Waller (2020) have also highlighted similar issues within existing research. AI solutions are ‘risky’ by their nature. It is also difficult to ignore the risk of illiberal or untrustworthy governance. As seen in Russia, where little to no trust exists in the authorities, there is limited to no trust in the integrity of state-provisioned digital services (Hardy, 2020). The same logic can be extended to AI-enabled services — the Polish Unemployment Profiling use case highlighted in this paper ultimately failed due to a collapse in public trust in the service and a perception that it was unfair.

Interview participants also highlighted the importance (and risks) of the upcoming EU AI Act, although acknowledged that often it is difficult for small/medium-sized member states such as those of the V4 to shape the outcome. In spite of some deregulationist desires within the research communities and private enterprises, the V4 states will likely have to operate within the EU’s AI framework. It is well recognised that small states on their own can exert less influence. However, if the V4 states were to coordinate their AI approaches they could amplify their voice within European institutions, much as Pastore’s (2013) and Adams’ (2019) research highlighted the value of coordinated cyber strategy approaches among small states.

Conclusions and Policy Recommendations

Artificial intelligence strategy is still in its infancy in the V4, and indeed across Europe, with the majority of European countries adopting strategies in 2019 or later. The upcoming EU AI Act also promises to be transformative in terms of guiding the ethical implementation of AI across the public sectors of Europe. Whilst nation-states will be free to implement services and innovate, there will be

an established ruleset in terms of what is, and is not, permissible. As evidenced in the contributions of some participants in this paper, this is not uncontested. Inevitably, some are likely to feel as though they are being stifled through overregulation. Conversely, it would be naive to expect the market to completely regulate itself. Striving to find a balance between regulation and free reign for innovation is likely to be crucial going forward.

As things stand, it is difficult to follow the development of use cases across the Visegrad states. While this paper has highlighted some use cases, the AI landscape is in constant flux as new services are implemented and others abandoned. It is not always possible to follow exactly which services are and are not available, which are being developed, and which are being abandoned. Improved transparency not only makes the lives of researchers easier but can also be used to build public trust. Existing research has overwhelmingly concluded that trust is crucial to the public using these services and that both trust and service use is likely to develop incrementally over time (Solvak et al, 2019). Trust is drawn from transparency, as well as from the government itself. The more trusted a government is, the more likely citizens are to trust the digital services it provides. Open, democratic governments that focus on accountability and transparency can more easily implement digital public services (Robinson & Hardy, 2021). Conversely, in more autocratic states, it is less likely that digital solutions will be trusted by citizens (Hardy. 2020)

Strictly addressing the Visegrad states, it seems easy to recommend a closer collaborative approach, when much research has already highlighted the benefits of doing so (Such as Pastore, 2013). Yet tempering ideals with reality, this seems unlikely anytime soon. This paper has highlighted both a lack of existing coordination, but also some divergence in priorities. While coordination can build knowledge-sharing and expertise in the region, this study, however preliminary, has indicated that this is not happening. A realistic recommendation would be increased dialogue between the Visegrad countries regarding both AI and cyber security more generally, to develop a unified stance. This might in future lead to the development of collective solutions, as well as speaking with a united voice internationally to expand their influence.

There are a number of opportunities for expanding this research in the near future. This could include further outreach to civil society organisations in the region, as well as increased engagement with research groups and governmental organisations to gather additional primary data to expand this case study. Additionally, future research could be expanded to include the military and private sectors, or might specifically focus on these areas.

To conclude, the implementation of public-facing AI use cases in the V4 ought to be guided by the principles identified by Berryhill et al (2019) — namely — that all should be ethical, trustworthy, and implemented securely. This conclusion applies equally to both the Visegrad states and to the wider European adaption of AI-enabled public services. Below, some key challenges and policy recommendations for the V4 are outlined.

Key challenges include:

- Supply chain security
- Balancing local calls for deregulation with sensible oversight
- Maintaining European commitments while also seeking to extend influence
- Navigating disagreements on AI strategy (such as regulation) between V4 states

Policy Recommendations — What can be done to facilitate AI growth in the region?

- Financial support of PPP's
- Improved governance through closer links with the tech community and more technocratic governance based upon expertise
- Support for the startup industry generally
- Create subsidised spaces for innovation to provide workspace / networking spaces (akin to Garage 48 in Tallinn, these can also support urban regeneration)
- Hosting events (such as 'Hackathons' but with a specific focus on AI service development.)

How can AI growth in the V4 be 'Ethical, Trustworthy, and Secure'?

- Ensuring proper oversight and regulation of development
- Public outreach, education and confidence building
- Public consultation in the implementation of services

Bibliography

Adamson, L., 2019. Let Them Roar: Small States as Cyber Norm Entrepreneurs. *European Foreign Affairs Review*, 24(2).

BBC News, 2021. Huawei Ban: UK to Impose Early End to use of new 5G Kit, BBC News [online], Available at: <<https://www.bbc.com/news/business-55124236>> [Last Accessed 21/10/2021]

Bennetts, M. 2021. Russia Unveils Checkmate Stealth Jet with jibe at Britain, The Times [online], Available at: <<https://www.thetimes.co.uk/article/russia-unveils-checkmate-stealth-jet-with-jibe-at-britain-7bl7hq2mg>> [Last Accessed 4/11/2021]

Berryhill, J., et al. 2019. "Hello, World: Artificial intelligence and its use in the public sector", *OECD Working Papers on Public Governance*, No. 36, OECD Publishing, Paris,

Budapest Business Journal, 2021. Huawei Sign Memorandum of Cooperation, *Budapest Business Journal* [online], Available at: <<https://bbj.hu/business/industry/deals/itm-huawei-sign-mou-on-long-term-cooperation>> [Last accessed 02/11/2021]

Burton, J., 2013. Small states and cyber security: The case of New Zealand. *Political Science*, 65(2), pp.216-238.

Central Register Slovakia, 2021. Memorandum of Agreement - University of Košice and Huawei, CRZ [online], Available at <<https://crz.gov.sk/data/att/2810828.pdf>> [Last accessed 3/11/21]

Cilluffo, F. & Cardash, S. 2019. What's Wrong With Huawei?, *The Conversation* [Online], Available at: <<https://theconversation.com/whats-wrong-with-huawei-and-why-are-countries-banning-the-chinese-telecommunications-firm-109036>> [Last Accessed 02/11/2021]

Csótó, M., Rupp, Z. and Petényi, S., 2021. In the Wake of Algorithmic Decision Making: Mapping AI-related Advancements in the Hungarian Public Sector. In *Central and Eastern European eDem and eGov Days* (pp. 273-284).

Czech Strategy for Artificial Intelligence, 2019. Available at: <https://www.mpo.cz/assets/en/guidepost/for-the-media/press-releases/2019/5/NAIS_eng_web.pdf> [Last accessed 14/10/2021]

Eeckhout, J, Hedtrich, T, & Pinheiro, R. 2021. Inequality is an Urban Affair - and it's due to new tech, Vox EU [online], Available at: <<https://voxeu.org/article/inequality-urban-affair-and-it-s-due-new-tech>> [Last Accessed 01/11/2021]

Hardy, A. 2020. Russia Scales up e-Voting for Key Referendum, *Open Democracy* [online], Available at: <<https://www.opendemocracy.net/en/odr/russia-scales-e-voting-key-referendum-misses-security-issues/>> [Last accessed 25/10/2021]

Heikkilä, M. 2021 What EU Capitals Think of the AI Act, *Politico* [online], Available at: <<https://www.politico.eu/newsletter/ai-decoded/ai-goes-to-school-what-eu-capitals-think-of-the-ai-act-facebooks-content-moderation-headache-2/>> [Accessed 14.11.2021]

Hendrych, L. 2020. Czechia Wants to be AI Leader, Visegrad Info [online], Available at <<https://visegradinfo.eu/index.php/national-policy-reports/596-czechia-wants-to-be-ai-leader-and-rejects-regulation-but-companies-lacks-state-support>> [Last accessed 17/10/2021]

Hungary Artificial Intelligence Strategy, 2020. Available at: <<https://ai-hungary.com/files/e8/dd/e8dd79bd380a40c9890dd2fb01dd771b.pdf>> [Last accessed 14/0/2021]

Kuziemski, M. and Misuraca, G., 2020. AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. *Telecommunications policy*, 44(6), p. 101976.

Markotkin, N. & Chernenko, E. (2020) Developing Artificial Intelligence in Russia: Objectives and Reality. Carnegie Moscow Center. 5 August. Available from: <https://carnegie.ru/commentary/82422> [Accessed 16th November 2020]

Misuraca, G. & Van Noordt, C. 2020. Artificial Intelligence in Public Services, *AI Watch* [online], Available at: <https://knowledge4policy.ec.europa.eu/ai-watch/artificial-intelligence-public-services_en> [Accessed 21.10.2021]

Molinari, F., Van Noordt, C., Vaccari, L., Pignatelli, F. and Tangi, L., 2021. AI Watch. Beyond pilots: sustainable implementation of AI in public services, EUR 30868 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-42587-8 (online)

Monitor Polski Dziennik Urzędowy Rzeczypospolitej Polskiej, 2020. [online] Available at: <<https://monitorpolski.gov.pl/M2021000002301.pdf>> [Last accessed 14/10/2021]

Ovide, S. 2021. The Strange Saga of Huawei, NY Times [online] Available at: <<https://www.nytimes.com/2021/11/02/technology/huawei-us-policy.html>> [Last Accessed 21/10/2021]

Payne, K., 2018. Artificial intelligence: a revolution in strategic affairs?. *Survival*, 60(5), pp.7-32.

Pastore, Gunta. 2013. “Small New Member in the EU Foreign Policy: Toward ‘Small State Smart Strategy’?.” *Baltic Journal of Political Science* 2: 67–84.

Robinson, N, Hardy, A, & Ertan, A. 2022 [forthcoming]. Estonia: A Curious and Cautious Approach to Artificial Intelligence and National Security, In *Routledge Companion to Artificial Intelligence and National Security Policy*, Routledge

Robinson, N & Hardy, A. 2021. Estonia: From the “Bronze Night” to Cyber Security Pioneers, In *Routledge Companion to Global Cyber Security*, (p211-225), Routledge

Šimančík, M. 2021. Slovak Universities have a China Problem and they don’t even know it, *CEIAS* [online], Available at: <<https://ceias.eu/slovak-universities-have-a-china-problemand-they-dont-even-know-it/>> [Accessed 01/11/2021]

Slovak Digitalisation Strategy, 2019. Available at: <<https://www.mirri.gov.sk/wp-content/uploads/2019/10/AP-DT-English-Version-FINAL.pdf>> [Last accessed 14/10/2021]

Solvak, M., Unt, T., Rozgonjuk, D., Vörk, A., Veskimäe, M. and Vassil, K., 2019. E-governance diffusion: Population level e-service adoption rates and usage patterns. *Telematics and Informatics*, 36, pp.39-54.

Stevens, T., 2020. Knowledge in the grey zone: AI and cybersecurity. *Digital War*, 1(1), pp.164-170.

Szicherle, P. 2021. The Laboratory Focusing on Coordinating Research Could Strengthen Hungary's AI Push, *Visegrad Info* [online], Available at: <<https://visegradinfo.eu/index.php/national-policy-reports/612-the-laboratory-focusing-on-coordinating-research-could-strengthen-hungary-s-ai-push>> [Last accessed 13/11/2021]

Waller, Madeleine and Waller, Paul. 2020. Why Predictive Algorithms are So Risky for Public Sector Bodies, *SSRN*, Available at: <https://ssrn.com/abstract=3716166>