

MANAGING DIGITAL SOVEREIGNTY: THE IMPORTANCE OF CONTROL AND OWNERSHIP IN THE DIGITAL AGE USING THE EXAMPLES OF POLAND, THE CZECH REPUBLIC AND GERMANY

Martin Kaloudis

Mendel University, Faculty of Business and Economics

Grzegorz Chmielarz, Robert Kućba

Częstochowa University of Technology

Abstract: The topic of strengthening digital sovereignty and its mechanisms of action, particularly with regards to EU states such as Poland, the Czech Republic and Germany, is largely unexplored. This is an essential element of security management in countries in economically and socially turbulent times. Using a relatively new digital sovereignty index, this article assesses the strengths and weaknesses of digital sovereignty in these countries and identifies potential fields of action for improvement. The shortage of skilled workers with digital expertise in these countries highlights the practical relevance of the recommendations for human resource management (HRM), including improving cooperation between universities and industry.

Key words: digital sovereignty, data security, European Union, security management

Introduction

The concept of digital sovereignty refers to the power and control individuals and nations have over their digital data and infrastructure. As technology advances, the issue of digital sovereignty has become more relevant, with concerns over the centralisation of data leading to the concentration of power in the hands of a few (government-influenced) corporations and the vulnerability of critical systems, cyber-attacks, and loss of privacy. To address these concerns, some countries have taken steps to strengthen their digital sovereignty, such as the EU's GDPR and the development of national digital infrastructure. However, there is a lack of a tested model to measure digital sovereignty on state level, so this paper proposes using a theoretical model to evaluate the states of Poland, the Czech Republic and Germany and provide measures to strengthen their digital sovereignty.

Literature overview

Digital sovereignty refers to a state's ability to control and regulate its digital environment, including its digital infrastructure, data, and cyberspace. It allows nations to control their critical infrastructure (Haché, 2014, pp. 165–173) and it can be used to promote economic development (Maurer, Skierka, Morgus, & Hohmann, 2015) (Haché, 2014, pp. 165–173). It is important for protecting personal and sensitive information, controlling critical infrastructure, and promoting economic development (Deutscher Ethikrat, 2017, pp. 253–261) (Polatin-Reuben & Wright, 2014/2014, p. 6) (Kućba & Chmielarz, 2018, p. 58). In recent years, the increasing importance of digital technologies in everyday life and their impact on society have led to growing concerns about the need to ensure digital sovereignty (Kukkola, Ristolainen, & Nikkarila, 2019). The concept has given rise to a new interdisciplinary field of research called Science and Technology Studies (STS) (DeNardis, Cogburn, Levinson, & Musiani, 2020, pp. 87–92). China and the USA are examples of countries pursuing different models of digital sovereignty, with China pursuing state-institutionalized, autarky-oriented policies and the USA relying on a techno-positivist, capitalist, and libertarian basic model (Creemers, 2020, pp. 107–131) (Hannas & Tatlow, 2021) (Holtmann, 2018, p. 169). Both countries have dominance in the digital economy, but the notion of digital sovereignty is not discussed intensively in either country (Werthner, Prem, Lee, & Ghezzi, 2022, pp. 227–231).



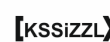
Ministry of Education and Science
Republic of Poland



Częstochowa
University
of Technology



Faculty
of Management



Department of Applied Sociology
and Human Resource Management

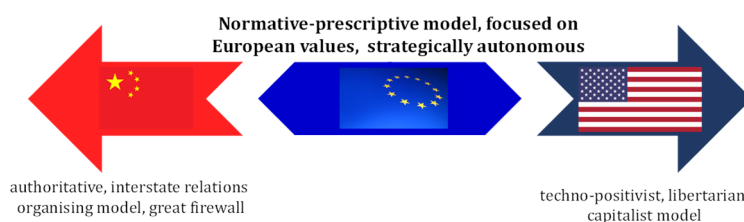


Figure 1. Model of digital sovereignty

Source: based on (Pohle & Thiel, 2021)

Various models exist to evaluate a country's digital and sovereignty status, with different parameters and analysis methods. The comparative index analysis approach compares relevant parameters to determine the strengths and weaknesses of countries' digital sovereignty, using calculated indices to create a composite index and rank countries accordingly. There are many comparative indices for state comparison, and although they are subject to criticism, their use is becoming more prevalent (Bjerre, Römer, & Zobel, 2019, pp. 649–662). Some of them compare the degree of sovereignty of states (Barnett, 2017/2017), others focus on the digital capabilities of states (Yera, Arbelaitz, Jauregui, & Muguerza, 2020) (United Nations, 2022/2022). An index tailored to the self-conception of EU states, the Digital Sovereignty Index (DSI) is based on publicly available secondary data and provides a ranking of UN states (Kaloudis, 2022/2022).

The DSI aggregates additively and multiplicatively over 3 sub-indices $\Delta_{1,2,3}$ and 30 parameters $X_{1,\dots,30}$ an index value for the UN states. Several qualitative studies have been conducted to analyse the digital sovereignty of various countries and regions and identify areas for improvement. However, the only model that integrates both qualitative descriptions and quantitative criteria as a basis for evaluating digital sovereignty is the one mentioned above, which is outlined below in calculating and ranking a DSI (Kaloudis, 2022/2022, p. 184).

Table 1. Parameter overview

X_i	description	X_i	description	X_i	description
1	Sovereignty	11	TOP University	21	Import ICT goods total
2	GDP p.c.	12	Leiden Index	22	Import ICT services
3	FDI in	13	Human capital	23	Digital STRI
4	FDI out	14	OpenData Index	24	EDBI
5	Start-up invest	15	R&D expenditure	25	WDC
6	TIMMS	16	Quantum pub. funding	26	GDPR
7	Assesm. reading, etc.	17	AI Index	27	Internet access
8	Expend. education	18	Blockchain start-ups	28	SIM cards
9	Qualif. ICT employees	19	Exp. ICT services total	29	Governments online
10	Patents	20	Exp. ICT serv./total	30	E-Government rank

Source: based on (Kaloudis, 2022/2022)

Objectives

This article aims to compare the digital sovereignty of UN states, focusing on Poland, the Czech Republic, and Germany, by using a set of relevant parameters to calculate a composite index for each country. The results will be used to group and categorize the countries, identify strengths and weaknesses, and determine areas for improvement. The reliability of the comparative index analysis method will also be evaluated.

Methodology

The comparative index analysis method is a systematic approach to measure countries' digital sovereignty by comparing a set of relevant parameters. The method includes selecting parameters, collecting data, calculating indices, statistical analysis, comparing results to state-specific indices, and visualizing results (OECD, 2008/2020). A set of relevant parameters was chosen to measure digital sovereignty in the author's work, including control over digital data and infrastructure, security and privacy, domestic development of digital technology, and parameters related to state sovereignty (Kaloudis, 2022). Poland, the Czech Republic, and Germany were used as examples to assess their relative strengths and weaknesses in these areas.

Results

With the focus on EU countries it is stated that all are in the top 50 of the UN-ranking, with Germany in 13th rank, the Czech Republic in 29th and Poland in 35th. The selection of Germany, the Czech Republic, and Poland is based on their representation of one of the three groups A, B and C of EU states, based on a comparison of the subindices Δ_1 and $\Delta_2 + \Delta_3$.

Table 2. TOP 50 DSI Ranks

Rank	Country	Rank	Country	Rank	Country
1	USA	18	UK	35	Poland
2	Ireland	19	Austria	36	Latvia
3	Norway	20	Iceland	37	Greece
4	Luxembourg	21	Israel	38	Korea Rep.
5	Switzerland	22	Italy	39	Slovak Rep.
6	Denmark	23	Spain	40	Hungary
7	Netherlands	24	Arab Emirates	41	Chile
8	Sweden	25	Estonia	42	Saudi Arabia
9	Finland	26	Portugal	43	Russia
10	Australia	27	Slovenia	44	Croatia
11	Singapore	28	Qatar	45	Monaco
12	Canada	29	Czech Rep.	46	Malaysia
13	Germany	30	Cyprus	47	Liechtenstein
14	Japan	31	China	48	Kuwait
15	France	32	Malta	49	Romania
16	New Zealand	33	Lithuania	50	Bulgaria
17	Belgium	34	Hong Kong		

Source: based on (Kaloudis, 2021) and (Kaloudis, 2022/2022)

Table 3. Statistical values of Δ_1 and $\Delta_2 + \Delta_3$

	Sovereignty parameters (Δ_1)	Digitalisation parameters ($\Delta_2 + \Delta_3$)
Mean value	23.27	22.21
1 st quartile	10.53	13.03
Median	19.05	16.95
3rd quartile	29.39	29.25

Source: Own study

The countries can be classified by a categorisation cut, which is shown graphically in Figure 4. The 3rd quartile is chosen as the categorisation cut line in each case to identify a group of top performers and to delineate others in this regard.

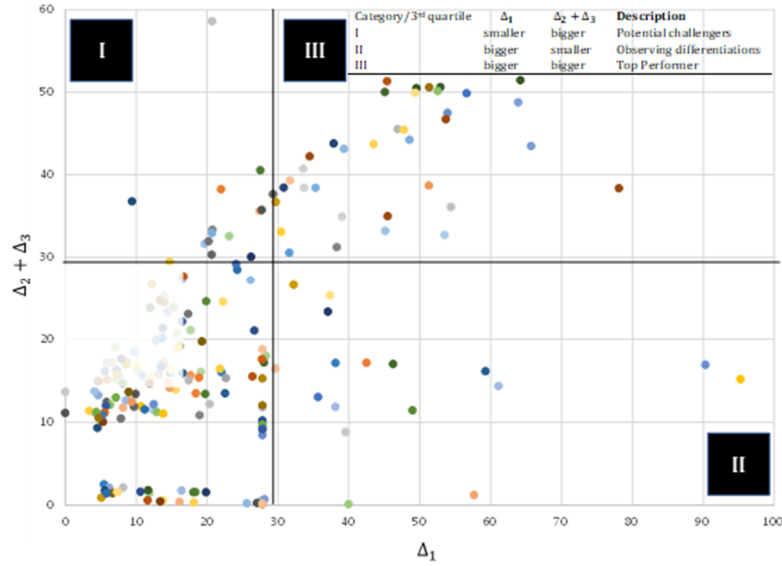


Figure 2 - All states, sub-index points for Δ_1 and $\Delta_2 + \Delta_3$

Source: Own study

No EU countries are included in category II. If the group of EU states in category I is referred to as group C, Poland falls into this group.

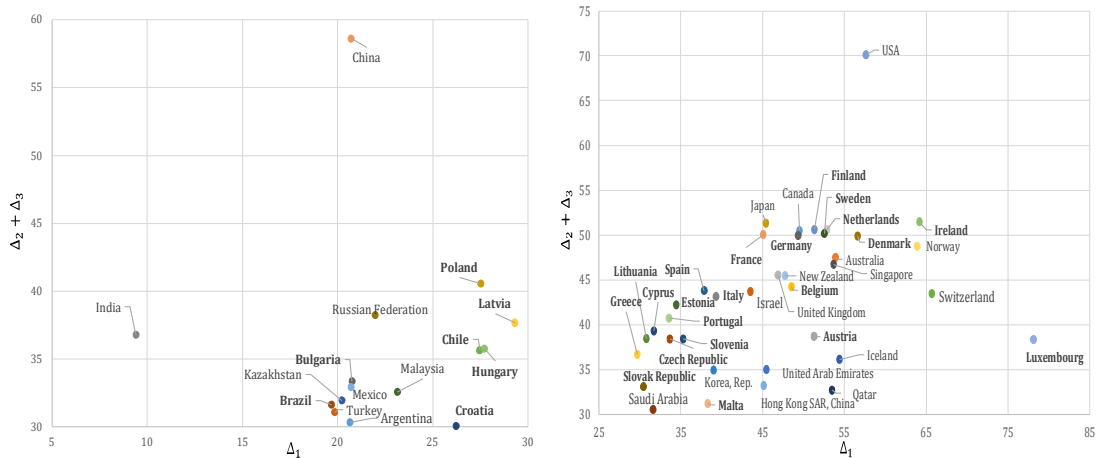


Figure 3 – DSI sub-indices, left: Category I, right: Category III: (EU countries in bold)

Source: Own study

The states of Germany and the Czech Republic can be assigned to category III, but fall into two groups here.

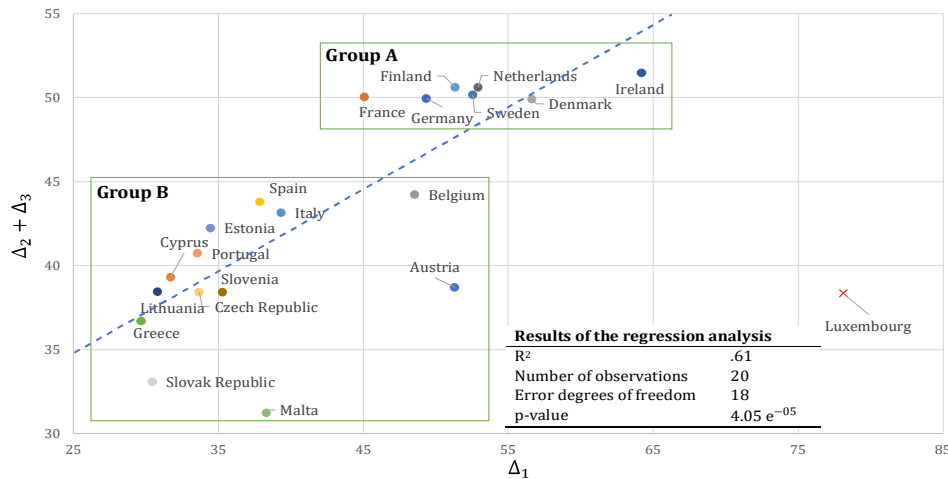


Figure 4 - Analysis of sub-indices for DSI, Category III: $\Delta_1, \Delta_2 + \Delta_3$

Source: Own study

If the EU states in category III are divided into groups A and B, Germany can be placed in group A and the Czech Republic in group B. In order to develop proposals to strengthen the digital sovereignty of states, recommendations can be derived in various ways.

Group recommendations

From the parameter analysis, recommendations for strengthening digital sovereignty can be derived for groups A, B and C and thus also for Poland, the Czech Republic and Germany. This can be done, for example, according to the following pattern.

It is recommended that the countries in Category I, Group C—Poland (and Latvia, Hungary, Croatia, Bulgaria)—strive to reach the top quartile of their comparison group. This can be achieved by focusing on reducing barriers to digital trade, expanding university education, promoting business activity, utilizing open data, and enhancing digitally accessible public authorities. This aligns with the following parameters that need to be strengthened in Group C: TOP University, X_{11} , OpenData Index, X_{14} , digital STRI, X_{23} , EDBI, X_{24} and Governments online, X_{29} . This will help these countries attain a higher ranking among the Category I states.

For the countries in Category III, Group B—Czech Republic (and Austria, Belgium, Italy, Spain, Malta, Estonia, Slovenia, Portugal, Cyprus, Lithuania, Greece, the Slovak Republic)—it is suggested that they aim to reach the intermediate level of Group A. To do this, the following areas of action are crucial: increasing exports of ICT services and imports of ICT goods, putting more emphasis on key technologies such as AI, and enhancing cooperation between universities and industry. This corresponds to the following parameters in Group B: Export ICT services (total), X_{19} , Import ICT goods total, X_{21} , Export ICT services from total, X_{20} , AI Index, X_{17} , and Leiden Index, X_{12} .

For the countries in Category III, Group A—Germany (and Ireland, Denmark, the Netherlands, Sweden, Finland, France)—the following recommendations are made: increase investment in start-ups, enhance the number of qualified individuals in the IT labour market, increase the research and development budget, increase the research and development budget and the number of ICT patents, X_{10} , and lower the barriers to setting up businesses. This is equivalent to the parameters: Start-up investments, X_5 , Qualified ICT employees, X_9 , R&D expenditure, X_{15} , ICT-Patents, X_{10} , and EDBI, X_{24} .

The parameters for the Leiden Index, qualified ICT employees and the TOP University Ranking show a need to catch up in the training of skilled employees in the industry of the states.

Comparison of states with the USA and China

In the following, the 30 parameters of the countries Poland, the Czech Republic and Germany are compared with those of the opposing concept partners USA and China.

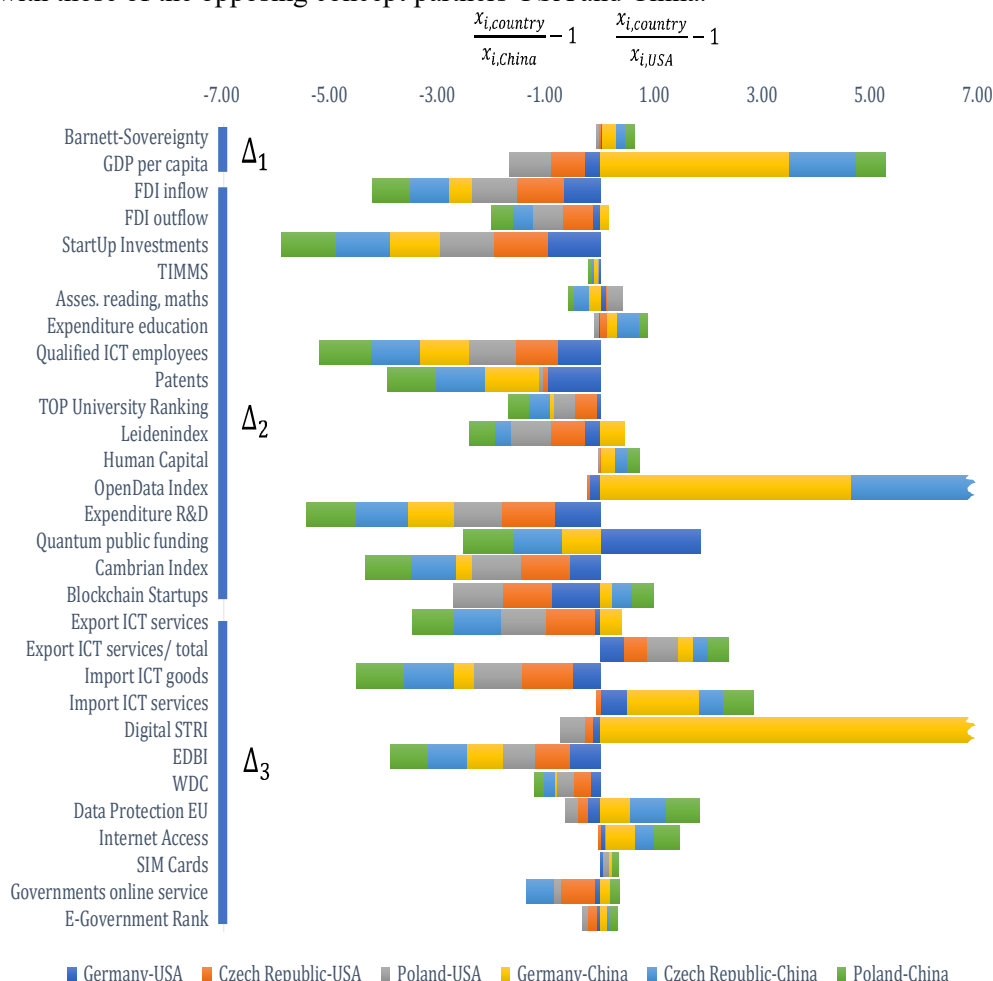


Figure 5 - Deviation Poland, the Czech Republic and Germany to USA and China

Source: Own study

The three sample countries, Poland, the Czech Republic, and Germany, need to catch up with the USA in most parameters related to digital sovereignty, with a few exceptions such as reading and writing assessments and ICT service exports. They also show a need to catch up with China in 17 out of 30 parameters, including FDI, start-up investments, qualified ICT employees, R&D expenditure, ICT patents, and investments in Quantum and AI. Education and training of qualified ICT employees in cooperative approaches between universities and industry is identified as an important area for strengthening digital sovereignty in these countries.

Discussion and conclusions

In this paper, the authors compare the digital sovereignty of different UN states, using the method of comparative index analysis, with a particular focus on: Germany, the Czech Republic and Poland. In the UN's ranking of the sovereignty of its member states, Germany was ranked 13th, the Czech Republic

29th and Poland 35th. The leader in sovereignty is still the USA. The above ranking was carried out on the basis of parameters such as: control over digital data and infrastructure, security of information systems, privacy of digital information, national development of digital technology including: knowledge, skills and competence of human resources in the field of ICT. Therefore, in the course of a discourse based on the UN's ranking of digital sovereignty, it is important to highlight that China, despite its digital dominance, was ranked 31st. This is influenced by limited territorial institutionalism. China, which produces digital technologies largely independently through strong regulation and isolation, still follows the still limited need for cyber sovereignty of the individuals who make up society. Based on its own statistical analyses, a division into quartiles was made according to the level of digital sovereignty of the UN member states, which is the basis for the cross-categorisation. Thus, Germany has been classified at the intermediate level. Recommendations have been proposed for countries representing this level, which include, among others the following: increasing investment in start-ups or creating social intellectual capital. The Czech Republic was ranked in the same quartile as Germany, one level lower. Also in this concluding discourse, it is emphasised that the most relevant recommendations for countries classified in the same category as the Czech Republic are: an increase in exports and imports of ICT services and goods, the diffusion of AI (including machine learning and now multivariate deep learning), as well as an increase in the number of innovative ICT projects carried out through binary cooperation of universities, R&D units with industry and also intermediary organisations.

Poland was classified in the quartile of countries, where work related to the diffusion of new, innovative ICT solutions should be intensified. Key recommendations for countries classified in the same group as Poland are: mitigation of barriers to digital trade, diffusion of electronic document circulation systems and electronic document management systems - especially in public administration. At the same time, it is emphasised that in all the European countries highlighted, despite their classification at different levels, a special role is attributed to human resources, their development and, in particular, the creation of social intellectual capital, which is an accelerator for the intensification of digital sovereignty activities. Detailing the research in this article, in the context of comparing the digital sovereignty of the three highlighted European countries with that of the leading United States, the results are collated for thirty parameters that multidimensionally identify digitisation and digitalisation activities. Although the USA is the leader in all identified areas, it is observed that the differences are beginning to blur. This demonstrates the intensification of multifaceted activities in European countries. This is definitely a move in the right direction, yet, it needs to be stressed that the European struggle to maintain its digital sovereignty is largely dependent on import of IT technologies from the US market where big production companies possess adequate capabilities to satisfy the need for digital products from the European market. Presently, the conducted analysis of the listed thirty parameters of digital sovereignty demonstrates quantitative differences in the dynamics and effectiveness of action. This also applies to Germany, the Czech Republic and Poland, in the areas defined by these parameters. In summary, top-down, society-wide, legislative, legal and administrative actions are important in the context of improving digital sovereignty. These, however, should not follow the Chinese model of confinement within the territory of Europe, as it lacks the capacities of big Chinese high-tech companies and is unable to be digitally self-sufficient. Hence, such activities are being implemented in varying degrees of intensification in all three selected European countries. In Poland, in the context of recommendations introduced for countries classified at the same level, an "open" social coalition for the introduction of the "Polish Charter of Digital Sovereignty" has been established. This coalition was formed by: economists, scientists, experts in new technologies, experts of consumer organisations, with the aim of strengthening lobbying in this area. The main lines of action for digital sovereignty have been identified, which also confirm the relevance of the formulated recommendations proposed in the article. Among these lines of action, the following stand out: the sealing of VAT and better parcel controls in e-commerce, the introduction of a digital tax for digital giants to support the digital sovereignty action of the remaining players in the national economy, the appointment

of a consumer representative and the strengthening of the digital competences of the President of the Office of Consumer and Competition Protection, the obligation of digital platforms to report regularly, and the introduction of an OSA (Algorithm Impact Assessment) mechanism to verify automated systems in terms of their security and impact on competition and consumers.

Further research that will be continued in this area will focus, among others, on evaluating the implementation of the recommended measures in, among others: Germany, the Czech Republic and Poland and measuring their impact on the change of categorisation in the determined quartiles of digital sovereignty of UN member states.

Literature

1. Barnett, M. A. (2017). Quantifying Sovereignty: A New Way to Examine an Essential Concept.
2. Beltrán, N. C. (2016). Technological Sovereignty: What Chances for Alternative Practices to Emerge in Daily IT Use? *Hybrid. Revue des arts et médiations humaines*. (03).
3. Bjerre, L., Römer, F., & Zobel, M. (2019). The Sensitivity of Country Ranks to Index Construction and Aggregation Choice: The Case of Immigration Policy. *Policy Studies Journal*, 47(3), 647–685. doi.org/10.1111/psj.12304
4. Cottey, A., Csernaton, R., Dobber, J., Fiott, D., Ghalehdar, P., Groitl, G., & Martill, B. (2022). *Beyond autonomy: Rethinking Europe as a strategic actor*. London, UK: LSE Ideas.
5. Creemers, R. (2020). *Governing cyberspace: Behavior, power, and diplomacy, China's Conception of Cyber Sovereignty. Digital technologies and global politics*. Lanham: Rowman
6. DeNardis, L., Cogburn, D. L., Levinson, N. S. Musiani, F. (2020). *Researching internet governance: Methods, frameworks, futures*. doi.org/10.7551/mitpress/12400.001.0001
7. Haché, A. (Ed.) (2014). *For Free Information and Open Internet: Technological Sovereignty*. Paris. Retrieved from https://www.coredem.info/IMG/pdf/pass11_an-2.pdf
8. Hannas, W. C., & Tatlow, D. K. (2021). *China's quest for foreign technology: Beyond espionage. Asian security studies*. doi.org/10.4324/9781003035084
9. Holtmann, D. (2018). *Potsdamer Beiträge zur Sozialforschung: Die Performanz von Politik, Wirtschaft und Gesellschaft für 43 Länder und 6 Wohlfahrtsregime*. Potsdam: Wirtschafts- und Sozialwissenschaftliche Fakultät / Sozialwissenschaften.
10. Kaloudis, M. (2021). Sovereignty in the Digital Age – How Can We Measure Digital Sovereignty and Support the EU's Action Plan? *New Global Studies*, doi.org/10.1515/ngs-2021-0015
11. Kaloudis, M. (2022). From Quality to Quantity: How Can Digital Sovereignty be Parsed into Measurable Components? doi.org/10.11118/ejobsat.2022.011
12. Kucęba, R., & Chmielarz, G. (2018). Issues of personal data management in organizations – GDPR compliance level analysis. *Informatyka Ekonomiczna*, 1(47), 58–71. doi.org/10.15611/ie.2018.1.05
13. Kukkola, J., Ristolainen, M., & Nikkarila, J.-P. (2019). GAME PLAYER Facing the structural transformation of cyberspace. *Finnish Defence Research Agency Publications*. (11).
14. Maurer, T., Skierka, I., Morgus, R., & Hohmann, M. (2015). Technological sovereignty: Missing the point? In *Cyber Conflict: Architectures in Cyberspace (CyCon), 2015 7th International Conference on*. Symposium conducted at the meeting of Global Public Policy Institute.
15. OECD (2020). *Handbook on Constructing Composite Indicators*. Retrieved from <https://www.oecd.org>
16. Pohle, J., & Thiel, T. (2021). 2.3.2 Digitale Souveränität. In C. Pfallat (Ed.), *Digitale Gesellschaft: Band 36. Der Wert der Digitalisierung: Gemeinwohl in der digitalen Welt* (Vol. 36, pp. 319–340). Bielefeld: doi.org/10.14361/9783839456590-014
17. Polatin-Reuben, D., & Wright, J. (2014). An Internet with {BRICS} Characteristics: Data Sovereignty and the Balkanisation of the Internet. *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14), 2014*.
18. United Nations (2022). *E-Government Survey 2022: Digital Government in the Decade of Action for Sustainable Development*
19. Werthner, H., Prem, E., Lee, E. A., Ghezzi, C. (Eds.) (2022). *Springer eBook Collection. Perspectives on Digital Humanism* doi.org/10.1007/978-3-030-86144-5
20. Yera, A., Arbelaitz, O., Jauregui, O., & Muguerza, J. (2020). Characterization of e-Government adoption in Europe. *PLOS ONE*, 15(4), 1–22. doi.org/10.1371/journal.pone.0231585

