A Reference Model to Strengthen Digital Sovereignty in Companies

Martha Klare[1,*], and Ulrike Lechner[1]

[1] *Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, 85577 Neubiberg, Germany*

Abstract

While the European Union is calling for more Digital Sovereignty (DS) in their 2030 agenda, there is no common understanding on what DS actually means or how best to achieve it. Researchers are currently discussing on political, individual and economical levels about DS. The main objective of our research is to contribute to the economic level of the discussion. We offer an understanding based on three case studies, through the lens of IT consultants and professors in Computer Science, Information Systems and Business Administration. Furthermore, we develop recommendations for companies based on two successfully published papers. Three further publications will follow (one have already been submitted). Our key findings are: (1) our definition include many points from publications between 2013 and 2023 in the context of DS but it also provides new insights, (2) key technologies (such as AI, especially federated learning, and blockchain) and the orientation towards affordances can help companies to successfully deal with DS The findings suggest that there is a need for a reference model with regard to DS for companies. Our next research step include the development of such a reference model.

1. Problem Definition

The CrowdStrike incident demonstrates how a software update can affect 8.5 million Windows computers globally, particularly impacting airports, banks, and emergency services in Germany [7]. A dependency is becoming clear. If we look specifically at Germany's imports, we can see that chips, software and hardware are among the top digital imports to Germany and that over 65% of the 604 companies surveyed are concerned about the growing partner China [3]. Another dependency lies in the use of foreign software products. The digital workday for many Germans relies on foreign software products such as Skype, Zoom, and Microsoft Teams, originating in particular from the US [9]. Germany's dependence on digital products is growing [18]. As a result, German and European politicians are calling for more DS in their 2030 agenda [21]. More and more researchers are now questioning how Germany can become more sovereign, which potential innovation fields should be promoted, and how the European Union can contribute to strengthening sovereignty [11, 1, 4].

But what does it actually mean to be "digitally sovereign"? In its most extreme sense, DScould mean self-developed software and domestically produced hardware, thus achieving more autarky [11, 14]. This perspective would lead to disadvantages, as it would limit innovation, quality, and international procurement [8]. A political view of DS, according to Pohle and Thiel [22] could mean collaborating with other nations while having alternatives if, for instance, a politician like Donald Trump imposes tariffs on German goods or blocks deliveries to Germany. A balance act between more autonomy and collaboration. From a technical-economic standpoint, the idea of developing open-source software is increasing discussed [2, 19, 6]. Diversified structures could enable a fast adaptation. However, a major challenge of open source is that security measures must be handled by companies alone, skilled human resources are needed, whereas software companies with proprietary software offer operation, scaling and security updates for companies [4].

These varying interpretations of DS indicate that we still do not have a clear understanding of what DS actually means or how best to achieve it. Pohle and Thiel [22] is the most cited paper in this field, describing that DS is understood differently depending on whether it is required by government institutions, companies, or citizens.

2. Knowledge Gaps

We aim to contribute to the economic dimension.

Thus, we want to answer the following research questions (see figure 1).

RQ1: What does 'digital sovereignty' mean from our perspective?

RQ2: How can German companies achieve digital sovereignty?

RQ3: How can a reference model for strengthening digital sovereignty in companies look like?

	RQ1. WHAT DOES 'DIGITAL SOVEREIGNTY' MEAN FROM OUR PERSPECTIVE?	
	Case study 1: Digital Sovereignty from the Perspective of IT Consultancy in Germany: A Model	
PART I	*RQ1* *Based on best practices from IT consultants, what factors should companies consider when strengthening their Digital Sovereignty?*	*RQ2* *How does a concrete model with weighted factors for Digital Sovereignty look like that represents the best practices from IT consultants?*
PART II	**Case study 2: Digital Sovereignty: Success Factors in a National Defense Scenario from the Standpoint of IT Consultancy**	
	RQ1 *How does the model change in the case of national defense?*	
Part III	**Case study 3: Digital Sovereignty: Factors from the Standpoint of Professors (Computer Science, Information Systems and Business Administration)**	
	RQ1 *How does the model change if we look at the topic of Digital Sovereignty from the perspective of researchers from the fields of Computer Science, Information Systems and Business Administration?*	
	RQ2. HOW CAN GERMAN COMPANIES ACHIEVE DIGITAL SOVEREIGNTY?	
	Deep Dive 1: How Blockchain and Artificial Intelligence influence Digital Sovereignty	
PART IV	*RQ1* *What is the gap between two successfully implemented open source projects (Kubernetes, Matrix) and strategic goals of Digital Sovereignty?*	*RQ2* *What are affordances to strengthen Digital Sovereignty in open-source projects?*
PART V	**Deep Dive 2: Digital Sovereignty: Affordances in Open Source Projects**	
	RQ1 *What is the companies' state of Digital Sovereignty?*	*RQ2* *How do AI and Blockchain support companies' sense of Digital Sovereignty?*
PART VI	**Deep Dive 3: Digital Sovereignty and Digital Transformation Extension for the Software Life Cycle Process in ISO/IEC/IEEE 12207:2017**	
	RQ1 *What are the requirements in the context of Digital Transformation and Digital Sovereignty when introducing software?*	*RQ2* *How does an architectural perspective for integrating the requirements of Digital Sovereignty and Digital Transformation into an existing software introduction framework look?*
	RQ3. HOW CAN A REFERENCE MODEL FOR STRENGTHENING DIGITAL SOVEREIGNTY IN COMPANIES LOOK LIKE?	
	in progress	

Additional RQ3 columns for Part IV and Part V:

	RQ3
PART IV	*How should affordances be designed to strengthen Digital Sovereignty?*
PART V	*How to strengthen Digital Sovereignty?*

Figure 1: Overview of all research questions that will be answered in the thesis

As already described in the introduction, we note that the understanding of the term 'digital sovereignty' differs widely [6, 10, 11]. While we cannot fully solve this problem, we can provide a definition from our perspective, as well as vocabulary and factors that are important for German companies to address DS.

Thus, we will first answer research question RQ1 by presenting an understanding of the term 'digital sovereignty', which is based on the perspectives of IT consultants and professors (in Computer Science, Information Systems, and Business Administration) in Germany. We will answer research question RQ2 by conducting various studies (see section 5.4 To 6.1). We want to show what

opportunities exist for German companies to achieve DS. To this end, we will analyze key factors that emerged from RQ1. It should be emphasized that although the European Union hopes to increase the competitiveness of European companies through economic and industrial policy, researchers are arguing that DS is something software companies lead [22, 12, 16]. How companies successfully master this change is the subject of intense debate [23, 5, 20].

3. Research Method

Methodologically, we initially rely on Yin [25], who provides analytic techniques and discussions on case study designs in his work. The case study, as an empirical research method, helps us achieve progress in knowledge by allowing us to test theories, such as the one on DS. Using three case studies, we offer a definition of DS (see Figure 1).

The second part of the thesis, as shown in Table 1, focuses on so-called deep dives. Here, we analyze several factors of the previously provided definition. Various publications are presented.

For every paper, the publication, the research method is outlined separately.

Table 1: research methods for deep dives 1 to 3

	Name of the paper	Research Method	Source
Deep Dive 1	How Blockchain and Artificial Intelligence Influence Digital Sovereignty	survey	Lehmann et al. (1998)
Deep Dive 2	Digital Sovereignty: Affordances in Open Source Projects	gap analysis	Kim and Ji (2018)
Deep Dive 3	Digital Sovereignty and Digital Transformation Extension for the Software Life Cycle Process in ISO/IEC/IEEE 12207:2017	Soft Design Science Methodology (SDSM)	Venable et al. (2018)

We first decided to conduct a survey to find out what the status of DS is in German companies. We then established that the main driver of DS is open source. Using an affordance analysis, we believe we can show how companies can close gaps in open source projects and drive sovereign software development. Finally, we realize that the purchasing department in companies procures software and hardware in particular. We decided to use the Soft Design Science Methodology (SDSM) to design an artifact that provides companies with procedural guidelines for the purchasing process.

In our research, we ensure a high level of reliability by using similar measurement instruments (interview studies) across the case studies. Additionally, we aim to ensure interpretative objectivity by forming research groups with two or more persons for all papers, in order to achieve similar or identical interpretations of measurement results. Finally, we uncover new factors of DS that had not been previously revealed in this context. With our model, we ensure that all content elements we consider as important for DS are discussed.

4. Timeline
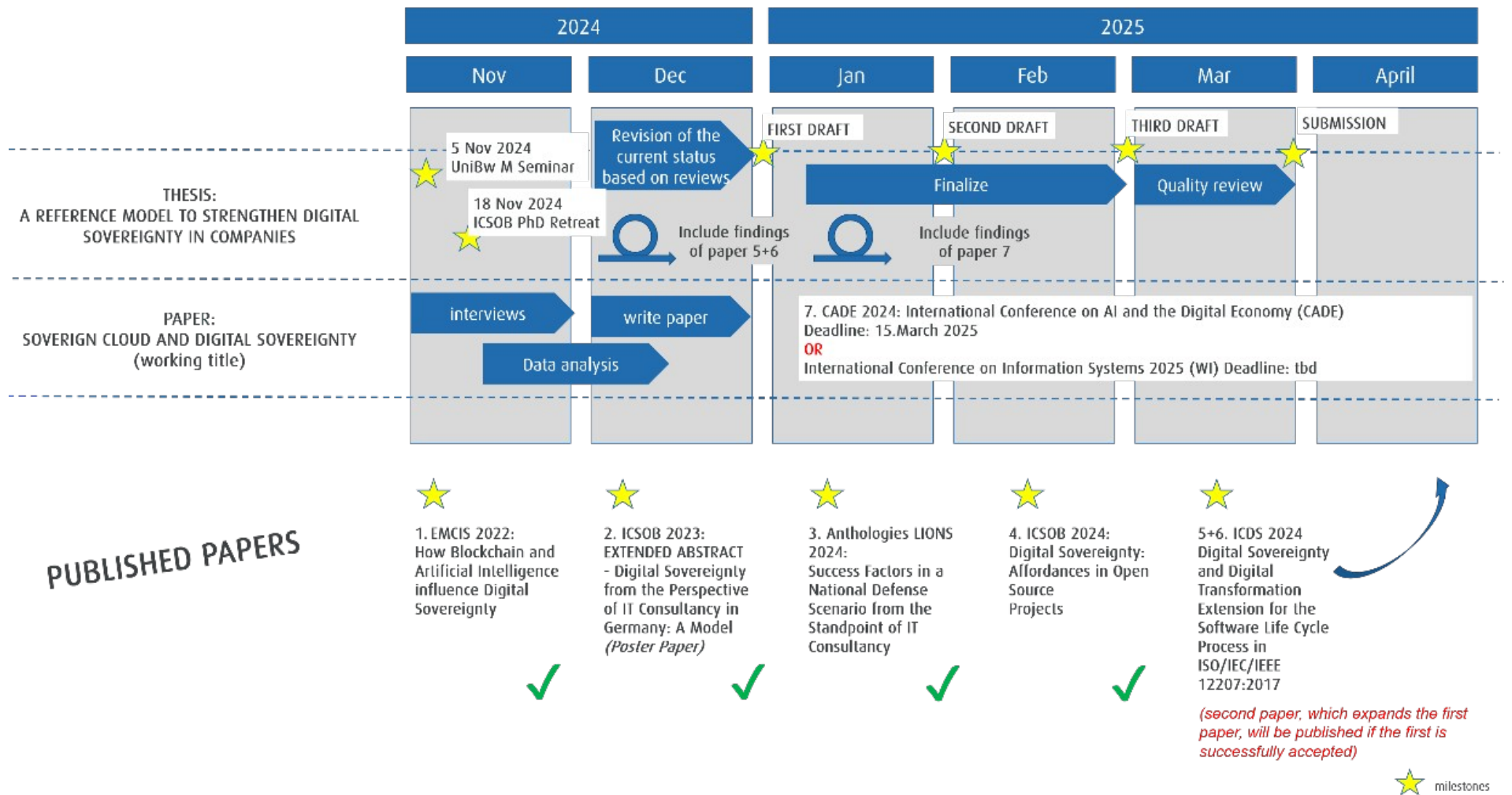
The timeline for the thesis is visualized in Figure 2.

2024

2025

Nov	Dec	Jan	Feb	Mar	April

FIRST DRAFT SECOND DRAFT THIRD DRAFT SUBMISSION

THESIS:
A REFERENCE MODEL TO STRENGTHEN DIGITAL SOVEREIGNTY IN COMPANIES

5 Nov 2024
UniBw M Seminar

18 Nov 2024
ICSOB PhD Retreat

Revision of the current status based on reviews

Include findings of paper 5+6

Include findings of paper 7

Finalize

Quality review

PAPER:
SOVERIGN CLOUD AND DIGITAL SOVEREIGNTY
(working title)

interviews

write paper

Data analysis

7. CADE 2024: International Conference on AI and the Digital Economy (CADE)
Deadline: 15.March 2025
OR
International Conference on Information Systems 2025 (WI) Deadline: tbd

PUBLISHED PAPERS

1. EMCIS 2022:
How Blockchain and Artificial Intelligence influence Digital Sovereignty ✓

2. ICSOB 2023:
EXTENDED ABSTRACT
- Digital Sovereignty from the Perspective of IT Consultancy in Germany: A Model
(Poster Paper) ✓

3. Anthologies LIONS 2024:
Success Factors in a National Defense Scenario from the Standpoint of IT Consultancy ✓

4. ICSOB 2024:
Digital Sovereignty: Affordances in Open Source Projects ✓

5+6. ICDS 2024
Digital Sovereignty and Digital Transformation Extension for the Software Life Cycle Process in ISO/IEC/IEEE 12207:2017

(second paper, which expands the first paper, will be published if the first is successfully accepted)

⭐ milestones

Figure 2: Expected timeline until the thesis is completed (Martha Klare)

5. Preliminary Results

5.1. Digital Sovereignty from the Perspective of IT Consultancy in Germany: A Model (2023)

This work contributes to the resolution of proposing a new model for DS from the perspective of IT consultancy (see Figure 3).
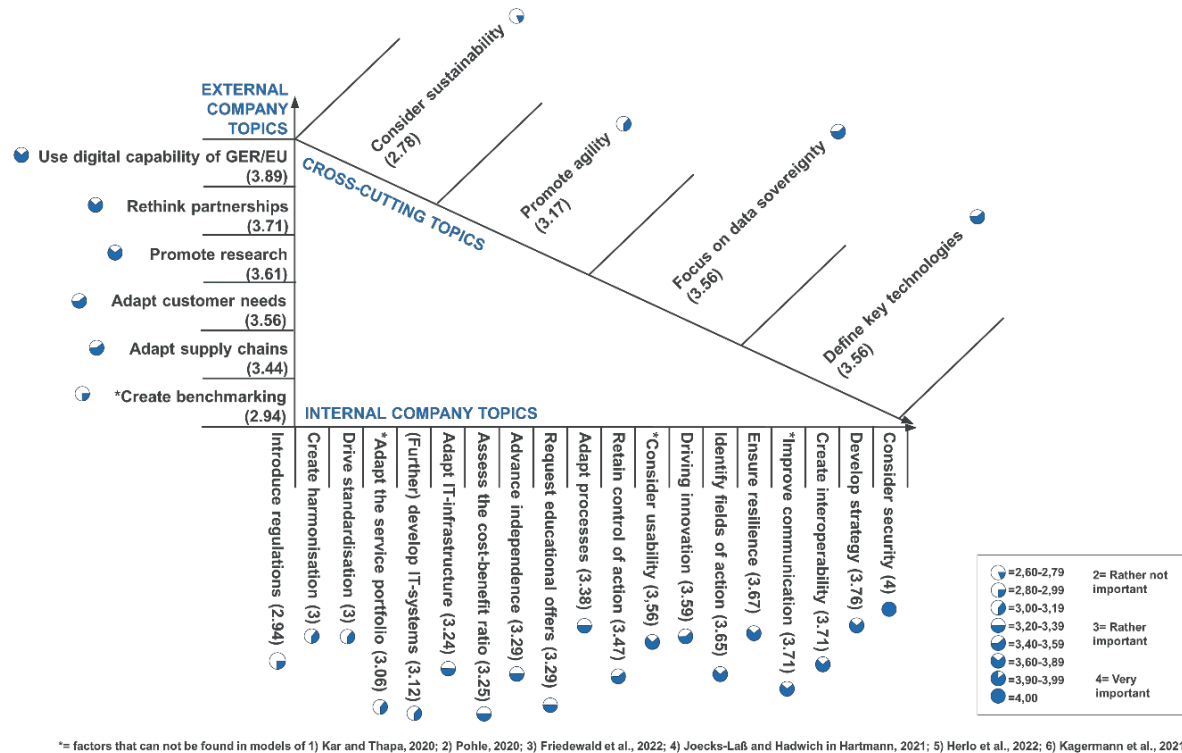

Figure 3: DSMIC (Digital Sovereignty Model from the perspective of IT-Consultancy)

We present the results of expert interviews of IT consultants who have already dealt with the topic of DS. Furthermore, we analyze the current state of the literature regarding DS models. Our key finding is that DS from the perspective of IT consulting is not only a technological problem, but also a strategic one that goes hand in hand with vocabularies like IT security, digital capabilities in Germany and the EU, and suitable key technologies for companies. New factors compared to the literature are (1) communication in companies, (2) adapt service portfolios in companies, (3) usability of IT systems. Companies that want to strengthen their DS can use the advanced model with weighted factors as a strategic instrument [16].

5.2. Digital Sovereignty: Success Factors in a National Defense Scenario from the Standpoint of IT Consultancy (2023)

We compare the findings of case study 1 with findings of case study 2. We analyzed success factors for more DS in a national defense scenario and compared these with the findings from the peace scenario. By doing this, we take the perspective of IT consultancy. Based on our findings, the following three factors are the most important: (1) develop a strategy, (2) consider IT security, (3) rely on European skills, when preparing for DS in a defense scenario in Germany. When comparing success factors for DS in a peace scenario with a national defense scenario in Germany, we see that the adaption of IT infrastructures, the development of IT systems, and the strengthening of data

sovereignty gain significant weight. We transferred these findings into a model as an extension of case study 1 as shown in Figure 4 [15].
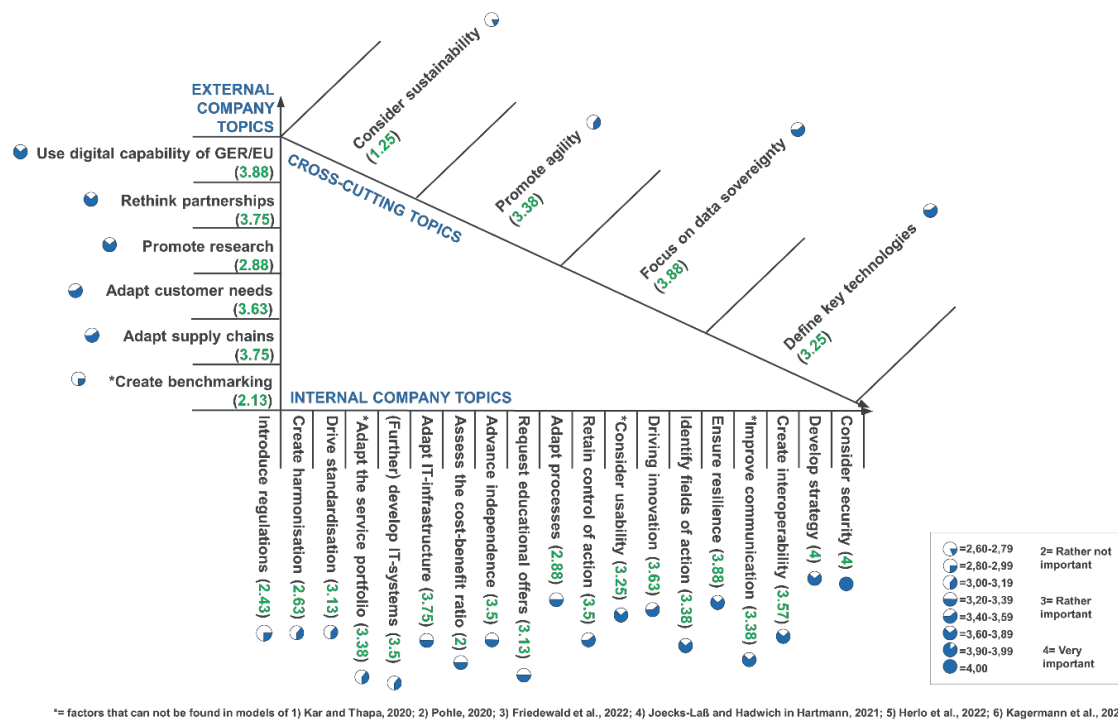

Figure 4: DSMIC in the case of national defense in Germany

5.3. Digital Sovereignty: Factors from the Standpoint of Professors (Computer Science, Information Systems and Business Administration) (2023)

In the third case study, we encounter the issue that the current model focuses exclusively on the perspective of IT consulting. This approach can be problematic, as the factors and their importance may vary depending on the surveyed group. In addition, the opinions of professors from Computer Science, Information Systems and Business Administration can contribute a definition of DS, considering economic and technical considerations.

We find that the professors, in contrast to the IT consultants, consider the following factors to be important to strengthen DS: (1) make investments (in the automotive sector, AI research, 5G, and Big Data), (2) leverage start-ups, (3) promote digitization projects within the EU (validate GAIA-X and CATENA-X), (4) establish alternative production locations (e.g., for chip manufacturing), (5) define open standards, (6) advance open source, and others. We compare the results with those from case studies 1 and 2 and then develop a model that visualizes a common core of all case studies (see Figure 5).
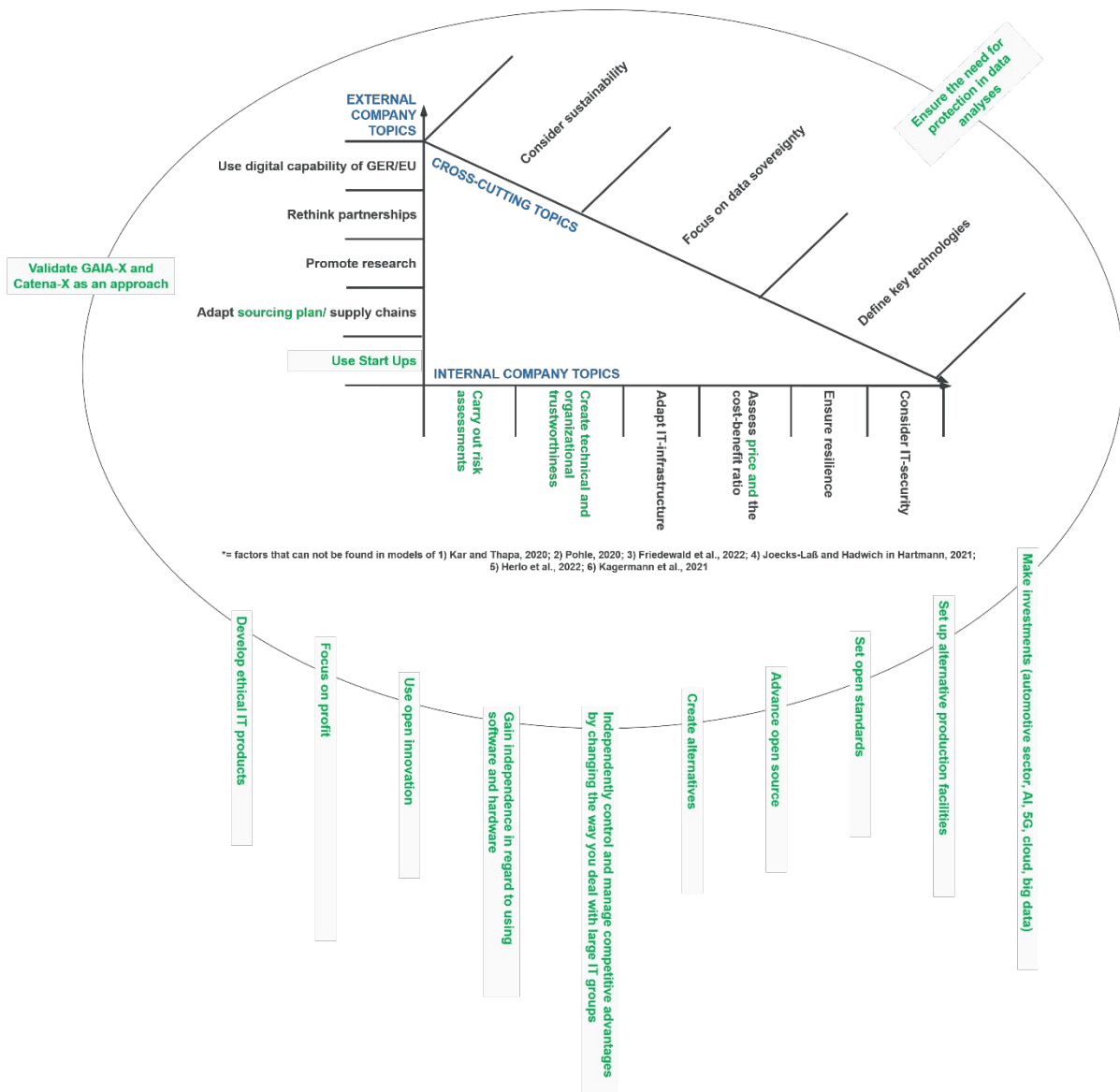
Figure 5: DSMIC expended by the additional perspective of professors (Computer Science, Information Systems and Business Administration)

5.4. How Blockchain and Artificial Intelligence influence Digital Sovereignty (2022)

As Information Systems researchers, we are interested in the state of DS in companies. We want to take a technical perspective on the debate. This paper contains insights on the relationship between DS and the technologies Artificial Intelligence and Blockchain. We look at Artificial Intelligence as it is an emerging, disruptive technology. We hypothesize that Blockchain can contribute to more DS through its cryptographic nature. Our survey consists of 163 respondents. Finally, we note that Artificial Intelligence can contribute to more data sovereignty in connection with the concept of federated learning. Blockchain can also contribute here. With a catalog of measures consisting of seven actions, we share ways in which companies can address issues to strengthen their DS [17].

5.5. Digital Sovereignty: Affordances in Open Source Projects (2024)

To appear

DS is an enabler for more sustainable actions in the digital space. We analyze affordances of DS by presenting two previously conducted open-source projects in Germany. Open source is a central

element of DS because, in contrast to proprietary software, it can reduce vendor lock-in effects. Our primary data sources consist of online interviews with German project teams and literature on DS. By evaluating the project outputs based on affordance theory, we reveal structurally digital offerings. The analysis of the impact of these digital offerings showed that among other things the affordance `AI models' should be elevated to a strategic level. We suggest that companies consider basic, standardizing, controlling, organizational sensemaking, and integrating affordances when introducing DS to open source projects.

5.6. Digital Sovereignty and Digital Transformation Extension for the Software Life Cycle Process in ISO/IEC/IEEE 12207:2017 (2024)

Submitted
The goal of this paper was to generate guidance for public and private organizations along their Software Life Cycle. We investigated challenges and measures regarding Digital Transformation and DS to gain industry practice among the Software Life Cycle Process of organizations. We identified that the choice of options in the procurement of IT systems is limited. This is one of the biggest challenges to consider DS in the Software Life Cycle Process of organizations. To master the collected challenges, we develop recommendation blocks. Finally, we map these recommendation blocks to process groups by following ISO/IEC/IEEE 12207:2017 and thus create an extension for industrial practice-based Software Life Cycle process.

6. Expected Contributions

6.1. Paper: Sovereign Cloud and Digital Sovereignty (working title)

Currently in progress
In this paper, we plan to present the awareness/ attitude towards technologies like sovereign clouds. We address the following research question: Can we achieve more DS through sovereign clouds? Based on our data, we can present three perspectives: 1) an architecture perspective, 2) a management perspective, and 3) a user perspective. Based on our interview study, we can offer these perspectives to describe how they can help to achieve more DS. In addition, we find constraints. Both, opportunities and constraints, can provide an interesting angle to enrich the ongoing debate on this topic.

6.2. Thesis: Suggesting a reference model with assessment guidelines of use at strategic and technological dimensions to strengthen Digital Sovereignty in companies

Still to be completed
As already described in RQ3, my aim is to create a reference model for DS. For this paradigm, I use Design Science Research according to Hevner [13]. The Design Science Research method starts from a problem, which is application-oriented. Just like DS. Based on this problem, an artifact for a problem solution is created. This is then unleashed on the world in order to understand what this solution does. Hevner [13] speaks of design when an artifact is created. And finally 'design science research': the creation of an artifact to solve a problem and the subsequent analysis of this artifact.

References

[1] Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital sovereignty and European security integration: an introduction. European security, 31(3), 337-355.

[2] Biström, D., Adolfsson, K. K., & Stocchetti, M. (2024). Open-Source Software and Digital Sovereignty: A Technical Case Study on Alternatives to Mainstream Tools. In International Conference on Science and Technology Education, 106-113.

[3]   Bitkom,   Deutschlands   Abhängigkeit   von   Digitalimporten   wächst,   2023,   URL: https://www.bitkom.org/Presse/Presseinformation/Souveraenitaet-Abhaengigkeit-Digitalimporten-waechst (Accessed on 24-12-02)

[4]   Butler, S., Gamalielsson, J., Lundell, B., Brax, C., Mattsson, A., Gustavsson, T., ... & Lönroth, E. (2022). Considerations and challenges for the adoption of open source components in software-intensive businesses. Journal of Systems and Software, 186(111152), 1-12.

[5]   Calderao, A., Blumfelde, S. (2022). Artificial intelligence and EU security: the false promise of digital sovereignty? European Security, 31(3), pp. 415-434.

[6]   Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital?. New media & society, 21(10), 2305-2322.

[7]   Delaney, B. (2024). Cybersecurity and all that: reflections on the Crowdstrike outage. British Journal of General Practice, 74(746), 418.

[8]   Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. Research Policy, 52(6), 1-13.

[9]   Engels, B., Mertens, A., & Scheufen, M. (2020). Corona: Neuerungen in der beruflichen Kommunikation (No. 35/2020). IW-Kurzbericht.

[10]   Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philosophy and Technology, 33(3), pp. 369-378.

[11]   Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M. G., Bômont, C., ... & Zanin, C. (2023). Contested spatialities of digital sovereignty. Geopolitics, 28(2), 919-958.

[12]   Goldacker, G. (2017). Digitale Souveränität. Kompetenzzentrum Öffentliche IT, Fraunhofer-Institut für Offene kommunikationssysteme FOKUS.

[13]   Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS quarterly, 75-105.

[14]   Kaloudis, M. (2022). Sovereignty in the Digital Age–How Can We Measure Digital Sovereignty and Support the EU's Action Plan?. New Global Studies, 16(3), 275-299.

[15]   Klare, M. & Lechner, U. (2024): German Digital Sovereignty Success Factors in a National Defense Scenario from the Standpoint of IT Consultancy. In: I.. Fries, M. Grabatin, M. Hofmeier (Hrsg.), Sovereign by Design. The LIONS Approach to Digital Sovereignty (pp.41-55). Logos Verlag Berlin.

[16]   Klare, M., & Lechner, U. (2023). Digital Sovereignty from the Perspective of IT Consultancy in Germany: A Model. In ICSOB Companion.

[17]   Klare, M., Verlande, L., Greiner, M., & Lechner, U. (2022, December). How Blockchain and Artificial Intelligence influence Digital Sovereignty. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 3-16). Cham: Springer Nature Switzerland.

[18]   Lambach, D., & Oppermann, K. (2023). Narratives of digital sovereignty in German political discourse. Governance, 36(3), 693-709.

[19]   March, C., & Schieferdecker, I. (2023). Technological sovereignty as ability, not autarky. International Studies Review, 25(2), 1-12.

[20]   Monsees, L., Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. European Security, 31(3), pp. 377-394.

[21]   Petit, A., Wala, Z., Ciucci, M., Martinello, B., Digital agenda for Europe, 2024, URL: https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europ

[22]   Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4), 2-9 (Accessed on 24-12-02)

[23]   Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., Floridi, L. (2021). Safeguarding european values with digital sovereignty: An analysis of statements and policies. Internet Policy Review, 10(3).

[24]   Wirnsperger, Peter J.; Dinnessen, Felix und Hilberg, Soentje Julia (2021): Mit digitaler Souveränität ins europäische digitale Jahrzehnt, In: Deloitte., 1-7

[25]   Yin, R. K. (2009). Case study research: Design and methods, 4th Edition, 1-219.