Referenzmodell zur Stärkung digitaler Souveränität in Unternehmen

Martha Klare, geb. Wermann

Vollständiger Abdruck der von der Fakultät für Informatik der Universität der Bundeswehr München zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften (Dr. rer. nat.)

angenommenen Dissertation.

Gutachter/Gutachterin:

1: Prof. Dr. Ulrike Lechner

2: Prof. Dr. Dr. Albrecht Fritzsche

Die Dissertation wurde am 15.09.2025 bei der Universität der Bundeswehr München eingereicht und durch die Fakultät für Informatik am 02.01.2026 angenommen. Die mündliche Prüfung fand am 11.02.2026 statt.

Urheberrecht ® 2025
Martha Klare
Alle Rechte vorbehalten

Danksagung

Ich danke meinem Ehemann für seine tatkräftige Unterstützung. Ohne seinen Beistand wäre die Fertigstellung dieser Dissertationsschrift nicht möglich gewesen. Gerne wäre ich an der einen oder anderen Stelle noch mehr für meine kleine Familie da gewesen, was im Rahmen meiner Forschungsreise nicht immer so möglich war. Deswegen danke ich insbesondere meinem Mann, der mir Freiheiten eingeräumt hat, um diesen Weg zu gehen, und mich in etlichen Situationen entlastet hat.

Ich danke meiner Familie, darunter auch meinen Eltern, Geschwistern und Schwiegereltern, für die vergangene Betreuung unseres kleinen Sohnes und der allgemeinen Unterstützung bei der Verwirklichung eines großen Traums.

Ich will auch meinen Mentoren danken. Ich habe im Rahmen meiner Promotion viel lernen dürfen, ob es der Anspruch an qualitativ hochwertige Ausfertigungen war, ein Abtauchen in unterschiedlichste Theorien zur Erweiterung meines Horizontes oder die hilfreichen Reviews meiner Papiere. Ich habe diese Zeit sehr genossen und bin dankbar für eine derart engmaschige und hochwertige Betreuung.

Zuletzt danke ich meinem Kooperationspartner, der BWI GmbH, dem Forschungsprojekt LIONS und allen Studienteilnehmern, die an meinen Studien teilgenommen haben. Das Projekt LIONS wird vom dtec.bw – Digitalisierungs- und Technologieforschungszentrum der Bundeswehr finanziert. Auch bei Next-GenerationEU will ich mich herzlich bedanken, denn sie fördern dtec.bw. Die Zusammenarbeit zwischen der UniBw München und der BWI GmbH sieht die Wahrnehmung von Forschungsaufgaben auf der einen Seite und den Einblick bzw. den Zugang in für die Forschung wesentliche, und nicht-kritische unternehmerische Bereiche auf der anderen Seite, vor. So sollen

wissenschaftliche Diskurse auf wirtschaftlich-universitärer Ebene zur Erhöhung digitaler Souveränität angeregt werden. Außerdem stellt LIONS mit seiner Distributed-Ledger-Forschungsplattform eine Laborumgebung für Forschende bereit und bietet damit einen Zugang für technische Auseinandersetzungen und neuartige Forschung.

Kurze Zusammenfassung

Eine souveränere Nutzung von IT, die Sicherstellung von Datenschutz und Privatheit für Nutzer, als auch die Gewährleistung von Sicherheit für Kunden oder den Staat sind nur einige Themen, die mit der Stärkung digitaler Souveränität einhergehen.

Mit dieser Arbeit soll das Verständnis zum Thema digitale Souveränität erweitert werden. Zudem leistet diese Arbeit einen weiteren Beitrag, indem auf Basis eines Referenzmodells ein Weg aufgezeigt wird, wie Unternehmen digitale Souveränität stärken können. Dabei liegt der Fokus bei der Beantwortung der Fragen auf technologischen Aspekten, Prozessen und Aspekten auf Projektebene. In die Debatte rund um digitale Souveränität wird die Perspektive der IT-Beratung stärker eingebracht, die in diesem Zusammenhang noch wenig erforscht ist. Damit leistet diese Arbeit einen wesentlichen Beitrag an der Schnittstelle von Informatik, Betriebswirtschaftslehre, Politik, Wirtschaftsinformatik und Organisationswissenschaft. Das Forschungsdesign besteht aus vier Interviewstudien, einer Umfrage, einer Gap-Analyse und einer Soft Design Science Studie. Darüber hinaus liefern wesentliche Forschungsergebnisse zu dem Thema einen Rahmen zur Gestaltung des Referenzmodells.

Die wichtigsten Ergebnisse sind: (1) Digitale Souveränität ist ein strategisches Konzept, das ein höheres Maß an Unabhängigkeit, Selbstbestimmtheit, Handlungsfähigkeit und Risikoabwägung im digitalen Raum fordert. Damit ist es nicht nur ein technisches Problem, sondern auch ein strategisches. Bei den Forschungsergebnissen sind Zielkonflikte erkennbar, die teilweise nicht auflösbar sind. (2) Schlüsseltechnologien wie Künstliche Intelligenz (KI) und Blockchain können ein wesentlicher Ermöglicher für mehr Datensouveränität sein. Datensouveränität, als wesentlicher Teilbereich digitaler Souveränität,

geht davon aus, dass rechtliche Rahmenbedingungen für eine selbstbestimmtere Kontrolle für die Nutzung, Speicherung und Verarbeitung von Daten nicht ausreichen. In diesem Zusammenhang kann es sinnvoll sein, im Kontext von KI, Federated Learning einzusetzen, um eine Lokalisierung beim Training von Modellen zu erzwingen und so mehr Datenschutz für User zu gewährleisten. (3) Die Affordanztheorie ist hilfreich, um sich souveränerer Softwareentwicklung auf Basis von Open Source zu nähern. Die Affordanztheorie aus Perspektive der Wirtschaftsinformatik ist unter anderem ein Instrument zur Analyse, das die Aufmerksamkeit auf die Bedeutung der Nutzerinteraktion für die Gestaltung von Systemen, Entscheidungen, Prozessen und die Zuweisung von Rollen lenkt. Dabei haben Affordanzen wesentlichen Einfluss auf Handlungsmöglichkeiten und Ergebnisse. Passt man eine Affordanz an, so können sich Rollen, Entscheidungsstrukturen und Prozesse verändern. Eine Analyse von zwei Open Source Projekten (Nutzung von Matrix und Kubernetes) liefert standardisierende, grundlegende, kontrollierende, organisatorische, sensibilisierende und integrierende Affordanzen. Diese Affordanzen müssen jedoch angepasst werden, damit souveränere Softwareentwicklung mit Open Source gelingt. (4) Insbesondere Kosten und Komplexität hindern Unternehmen bei der Gestaltung souveränerer Softwareeinführung. Die in dieser Arbeit vorgeschlagene ISO 12207:2017-Erweiterung kann helfen, sich einer souveräneren Softwareeinführung zu nähern. (4) Souveräne Clouds gelten zwar als Ermöglicher digitaler Souveränität, analysierte Konzepte leisten aber eher einen Beitrag auf der Daten-, Operationalisierungs-, Softwareebene. Es sind die Cloud-Konzepte von Microsoft, Amazon, T-Systems mit Google, Oracle und IBM, GAIA-X als Cloud-Ökosystem, sowie eine Private Cloud aus dem militärischen Bereich analysiert worden. Auf der Grundlage dieser Daten folgt eine Ableitung von 25 Schlüsselfaktoren, die für Manager entscheidend sind, die durch souveräne Clouds digitale Souveränität stärken wollen.

Schließlich münden die vorangegangenen Ergebnisse in dem Design des DISO!-Modells. DISO! als Akronym steht für „**Di**gitale **S**ouveränitätsmodell-**O**ptimierung"). Dieses Referenzmodell trägt zu einem Verständnis für digitale Souveränität bei, da es aufzeigt, welche Faktoren im Rahmen digitaler Souveränität aus der oben beschriebenen Perspektive wichtig sind. Zudem

liefert es einen möglichen Weg, wie man digitale Souveränität steigern kann, indem es verschiedene Handlungsempfehlungen in Hinblick auf Ermöglicher, Prozesse und Risiken aufzeigt. Die Ergebnisse legen nahe, dass Unternehmen in der Praxis einen Bedarf nach einer Referenz für digitale Souveränität haben.

Die vorliegende Dissertationsschrift markiert das Ende eines umfassenden Schreib- und Reflexionsprozesses. Die Ergebnisse wurden im Rahmen eines dreijährigen Promotionsprojekts erzielt und in Forschungsgruppen, auf Tagungen und auf Konferenzen vorgestellt und diskutiert. Dabei gewonnene Erkenntnisse finden sich in dieser Arbeit wieder. Viel Spaß beim Lesen!

Abstract

A more sovereign use of IT, the protection of data privacy and users' personal rights, as well as the guarantee of security for customers and the state, are just some of the issues associated with strengthening digital sovereignty.

This work aims to expand the understanding of digital sovereignty. In addition, it makes a further contribution by presenting a reference model that outlines a path for companies to strengthen digital sovereignty. The focus in answering the research questions is placed on technological aspects, processes, and project-level factors.

This work also brings the perspective of IT consulting into the debate on digital sovereignty—a perspective that has been underexplored in this context. Thus, the dissertation makes an essential contribution at the intersection of computer science, business administration, politics, information systems, and organizational science.

The research design consists of four interview studies, one survey, a gap analysis, and a soft design science study. In addition, key research findings on the topic provide a framework for shaping the reference model.

The main findings are as follows: (1) Digital sovereignty is a strategic concept that demands a higher degree of independence, self-determination, agency, and risk consideration in the digital space. It is therefore not merely a technical problem but also a strategic one. The research results show conflicting goals that are partly irresolvable. (2) Key technologies such as artificial intelligence (AI) and blockchain can be essential enablers of greater data sovereignty. Data sovereignty, as a core component of digital sovereignty, assumes that legal frameworks alone are insufficient to ensure more autonomous control over the use, storage, and processing of data. In this context, using federated learning

in the field of AI may be useful to enforce data localization during model training and thus ensure greater privacy for users. (3) Affordance theory is helpful in approaching sovereign software development based on open source. From the perspective of information systems research, affordance theory describes how the interaction of a user with a system or business service can be understood. Affordances are an integral part of actions. When an affordance is adjusted, roles, decision structures, and processes change. An analysis of two open source projects (use of Matrix and Kubernetes) reveals standardizing, foundational, controlling, organizational, sensitizing, and integrating affordances. However, these affordances must be adapted to enable more sovereign software development with open source. (4) Costs and complexity in particular hinder companies in implementing more sovereign software adoption. The ISO 12207:2017 extension presented in this work can help guide the path to more sovereign software introduction. (5) Sovereign clouds are considered enablers of digital sovereignty, but the analyzed concepts primarily contribute at the levels of data, operationalization, software, and transparency. The cloud concepts of Microsoft, Amazon, T-Systems with Google, Oracle, IBM, GAIA-X as a cloud ecosystem, and a private cloud from the military domain have been analyzed. Based on this data, 25 key factors have been derived that are essential for managers aiming to strengthen digital sovereignty through sovereign clouds.

Finally, these findings lead to the design of the DISO! model (an acronym for "Digital Sovereignty Model Optimization"). This reference model contributes to a better understanding of digital sovereignty by identifying which factors are important in the context of digital sovereignty from the aforementioned perspectives. It also provides a potential pathway for enhancing digital sovereignty by offering various recommendations for action based on enablers, processes, and risks.

The results suggest that companies in practice have a need for a reference model for digital sovereignty. This dissertation thus contributes in two ways: first, to the debate on what digital sovereignty actually means or encompasses; second, to the question of how companies can strengthen their digital sovereignty.

This dissertation marks the conclusion of an extensive process of writing and reflection. The results were obtained over the course of a three-year

doctoral project and have been presented and discussed in research groups, at academic conferences, and professional meetings. The insights from these reflections are included in this work. Enjoy reading!

Inhaltsverzeichnis

Danksagung **iii**

Kurze Zusammenfassung **v**

Short summary **ix**

Inhaltsverzeichnis **xiii**

Abbildungsverzeichnis **xxi**

Tabellenverzeichnis **xxvii**

Akronyme und Abkürzungen **xxix**

1 Einleitung **1**

1.1 Motivation und Problemstellung 1

1.2 Forschungsfragen 4

1.3 Abgrenzung zu anderen Teilgebieten und Kooperationen . . 4

1.4 Publikationen mit Bezug zur Thesis 6

1.5 Struktur der Arbeit 7

2 Stand von Wissenschaft und Praxis **11**

2.1 Digitale Souveränität 11

2.1.1 Digitale Transformation und digitale Souveränität . 12

2.1.2 Perspektive auf digitale Souveränität: IT-Beratung . 13

2.1.3 Ansätze zum Umgang mit digitaler Souveränität . . 14

2.1.3.1 Open Source und digitale Souveränität . . 14

2.1.3.2 Softwarelieferketten, Software-Lebenszyklus und souveräne Softwareeinführung 15
2.1.3.3 Souveräne Clouds und digitale Souveränität 15
2.1.4 Arbeitsdefinition von digitaler Souveränität für diese Arbeit 16

3 Forschungsdesign 17
3.1 Forschungsdesign für diese Arbeit 17
3.1.1 Soft Design Science Methode (SDSM) 17
3.1.2 Design Science Research 19

4 Analysen und Modelliterationen 21
4.1 Erste Fallstudie: Interviewstudie zu Faktoren digitaler Souveränität aus Perspektive der IT-Beratung (Friedensfall) . . 24
4.1.1 Einleitung 24
4.1.2 Forschungsdesign 25
4.1.3 Ergebnisse 27
4.1.3.1 Analyseergebnisse auf Basis einer systematischen Literaturrecherche 27
4.1.3.2 Ergebnisse aus den Experteninterviews mit IT-Beratern (erste Interviewreihe) 30
4.1.3.3 Clustering der Ergebnisse aus Experteninterviews 32
4.1.3.4 Literaturauswahl für die Entwicklung des Modells und Analyse der Literatur auf Basis des Clusterings 38
4.1.3.5 Evaluation der Ergebnisse (zweite Interviewreihe) 43
4.1.3.6 Das DISO-B-Modell (Digitale Souveränitätsmodell-Optimierung durch kompetente Beratung) 46
4.1.4 Zusammenfassung, Limitationen, Ausblick 48
4.2 Zweite Fallstudie: Interviewstudie zu Faktoren digitaler Souveränität aus Perspektive der IT-Beratung (Landesverteidigung) 50
4.2.1 Einleitung 50

4.2.2 Szenare für digitale Souveränität: Friedensfall vs. Landesverteidigung 51
4.2.3 Forschungsdesign 51
4.2.4 Ergebnisse 53
4.2.4.1 Neue Gewichtungen im Landesverteidigungsfall 53
4.2.4.2 Neue Cluster im Landesverteidigungsfall . 58
4.2.4.3 Das DISO-L-Modell (Digitale Souveränitätsmodell-Optimierung im Landesverteidigungsfall) . 59
4.2.5 Zusammenfassung, Limitationen, Ausblick 59
4.3 Dritte Fallstudie: Interviewstudie zu Faktoren digitaler Souveränität aus Perspektive von Professoren aus der Informatik, Wirtschaftsinformatik, und Betriebswirtschaftslehre 61
4.3.1 Einleitung 61
4.3.2 Forschungsdesign 61
4.3.3 Ergebnisse 63
4.3.3.1 Was hat sich verändert? 63
4.3.3.2 Was lässt sich bestätigen? 70
4.3.3.3 Das DISO-A-Modell (Digitale Souveränitätsmodell-Optimierung Academia) 77
4.3.4 Zusammenfassung, Limitationen, Ausblick 77

5 Werkzeuge zur Umsetzung digitaler Souveränität 81
5.1 Werkzeug Schlüsseltechnologien: Umfrage zum aktuellen Stand digitaler Souveränität in Unternehmen und Implikationen sowie Diskussionen über die Schlüsseltechnologien künstliche Intelligenz und Blockchain 81
5.1.1 Einleitung 82
5.1.2 Theoretische Grundlagen 83
5.1.2.1 Schlüsseltechnologien für digitale Souveränität 83
5.1.3 Methodik 85
5.1.4 Ergebnisse 86

5.1.4.1 Gegenwärtiger Stand in deutschen Unternehmen hinsichtlich digitaler Souveränität 86
5.1.4.2 Zwei Gruppen: Unternehmen mit niedriger Souveränität vs. Unternehmen mit hoher Souveränität 87
5.1.4.3 Erkenntnisse aus der Vergangenheit und Empfehlungen für zukünftige Maßnahmen 88
5.1.4.4 Erweiterung des Verständnisses von digitaler Souveränität 90
5.1.4.5 Künstliche Intelligenz und Blockchain: mögliche Schlüsseltechnologien für digitale Souveränität? 91
5.1.5 Zusammenfassung, Limitationen, Ausblick 96
5.2 Werkzeug Open Source: Gap-, und Affordanzanalyse zu Herausforderungen digitaler Souveränität in Open Source Projekten 98
5.2.1 Einleitung 98
5.2.2 Theoretische Grundlagen 99
5.2.2.1 Retrospektive 99
5.2.2.2 Affordanz-Theorie und digitale Souveränität 100
5.2.2.3 Anforderungen, Architekturen, Prozesse und Qualität im Zusammenhang mit digitaler Souveränität 101
5.2.2.4 Anforderungsmodelle 101
5.2.2.5 Architekturmodelle 103
5.2.2.6 Prozessmodelle 103
5.2.2.7 Softwarequalitätsmodelle 104
5.2.3 Forschungsdesign 105
5.2.4 Ist-Analyse Informationssteckbrief (Kubernetes Projekt) 108
5.2.4.1 Darstellung der Ergebnisse aus der Retrospektive 108
5.2.4.2 Darstellung Anforderungsmodelle, Prozessmodell, Architekturmodell und Qualitätsmodell 109

5.2.5 Ist-Analyse Messenger (Matrix Projekt) 122
5.2.5.1 Darstellung der Ergebnisse aus der Retrospektive 122
5.2.5.2 Darstellung Anforderungsmodelle, Prozessmodell, Architekturmodell und Qualitätsmodell 124
5.2.6 Beschreibung des Soll-Zustands: Anforderungen digitaler Souveränität auf Basis der Herausforderungen 138
5.2.7 Gap-Analyse für den Informationssteckbrief 140
5.2.7.1 Gaps in den Anforderungsmodellen des Informationssteckbriefs 140
5.2.7.2 Gaps im Architekturmodell des Informationssteckbriefs 142
5.2.7.3 Gaps im Qualitätsmodell des Informationssteckbriefs 148
5.2.7.4 Gaps im Prozessmodell des Informationssteckbriefs 148
5.2.7.5 Strategische Gaps für den Informationssteckbrief 150
5.2.8 Gap-Analyse für den Messenger 152
5.2.8.1 Gaps in den Anforderungsmodellen des Messengers 152
5.2.8.2 Gaps im Architektur-Modell des Messengers 154
5.2.8.3 Gaps im Prozessmodell des Messengers . . 157
5.2.9 Strategische Gaps für den Messenger 157
5.2.10 Anwendung der Affordanz-Theorie: Ableitung von Affordanzen zur Reduzierung der Gaps 157
5.2.10.1 Ergebnisse aus dem Vergleich zwischen dem Ist-Zustand und dem Soll-Zustand 162
5.2.11 Fazit, Limitationen, Ausblick 167
5.3 Werkzeug Beschaffungsstrategie: Soft Design Science Studie zu Softwareeinführung im Kontext digitaler Souveränität . . 169
5.3.1 Einleitung 169

5.3.2 Forschungsdesign 170
5.3.3 Ergebnisse 172
5.3.3.1 Ergebnisse aus der Online-Umfrage: Zusammenhang zwischen Software-Einführung, digitaler Transformation und digitaler Souveränität in Unternehmen 173
5.3.4 Zusammenfassung, Limitationen und Ausblick . . . 188
5.4 Werkzeug IT-Infrastruktur: Interviewstudie zu souveränen Clouds im Kontext digitaler Souveränität 191
5.4.1 Einleitung 191
5.4.2 Forschungsdesign 192
5.4.3 Ergebnisse aus den Interviews mit den Cloud-Experten 194
5.4.4 Analyse von drei Perspektiven: Management-, Architektur- und Nutzerperspektive 201
5.4.5 Diskussion 205
5.4.5.1 Was sind Anforderungen an digitale Souveränität, die im Rahmen der souveränen Cloud-Konzepte nicht umgesetzt wurden? 205
5.4.5.2 Was hat sich verändert im Vergleich zu den anderen Ergebnissen der Arbeit? 209
5.4.5.3 Wie müssen nun die souveränen Cloud-Konzepte angepasst werden, damit ein höherer Grad digitaler Souveränität erreicht wird? 209
5.4.6 Zusammenfassung, Limitationen und Ausblick . . . 210

6 Referenzmodell für die Stärkung digitaler Souveränität in Unternehmen 213
6.1 Einleitung 213
6.2 Theoretische Grundlagen 214
6.2.1 Referenzmodellierung 214
6.3 Forschungsdesign 215
6.4 Ergebnisse 218

6.4.1 Inhaltliche Analyse der Studienergebnisse aus dieser Arbeit 218
6.4.2 Entwicklung des DISO!-Modells 223
6.5 Diskussion 227
6.6 Zusammenfassung, Limitation und Ausblick 229

7 Fazit, Zusammenfassung, Limitationen, Ausblick 231

Literatur 235

Anhang 259

Abbildungsverzeichnis

1.1 Anzahl der Publikationen unter dem Suchbegriff 'digital sovereignty' von 2013 bis 2025 (abgefragt am 25. Februar 2025) 3
1.2 Aufbau der Dissertationsschrift 5

3.1 Design Science Research Methode nach Hevner et al. (2004) als methodischer Rahmen für das Referenzmodell 19

4.1 Analyseprozess für die ersten drei Fallstudien 23
4.2 Forschungsdesign im Rahmen der ersten Fallstudie 25
4.3 Mittelwerte unternehmensinterne Themen 44
4.4 Mittelwerte unternehmensexterne Themen 45
4.5 Mittelwerte unternehmensübergreifende Themen 46
4.6 DISO-B: Digitale Souveränitätsmodell-Optimierung durch kompetente Beratung (1. Version) 47
4.7 Forschungsdesign für die zweite Fallstudie 52
4.8 DISO-L: Digitale Souveränitätsmodell-Optimierung im Landesverteidigungsfall (2. Version) 60
4.9 Forschungdesign dritte Fallstudie 62
4.10 Neue Faktoren digitaler Souveränität aus Perspektive der Professoren (Bereiche INF, WINF, BWL) 64
4.11 Bestätigte Faktoren digitaler Souveränität aus Perspektive der Professoren (Bereiche INF, WINF, BWL) 70
4.12 DISO-A: Digitale Souveränitätsmodell- Optimierung Academia (3. Version) 78

5.1 Einstufung der Unternehmen hinsichtich digitaler Souveränität 86

5.2 Interesse für digitale Souveränität, Bedeutung des Themas und Abhängigkeiten 87
5.3 Gründe, weswegen sich Unternehmen (nicht) digital souverän einstufen 88
5.4 Maßnahmen, um digitale Souveränität zu stärken 89
5.5 Wahrscheinlichkeit und Gründe, dass eine der Technologien scheitert 92
5.6 Maßnahmen zur Entwicklung einer Vision für digitale Souveränität 93
5.7 Ein Beispiel für eine agile Anforderungsmodellierung (Agile Requirements Modeling) 102
5.8 Ebenen für Qualitätsmodelle (Cavano und McCall, 1978) . 105
5.9 Forschungsdesign für die Gap-Analyse 106
5.10 AA-Modellierung für Anforderung Nr.1 und 2 (Informationssteckbrief) 112
5.11 AA-Modellierung für Anforderung Nr.3 und 4 (Informationssteckbrief) 113
5.12 AA-Modellierung für Anforderung Nr.5 und 6 (Informationssteckbrief) 114
5.13 AA-Modellierung für Anforderung Nr.7 und 8 (Informationssteckbrief) 116
5.14 AA-Modellierung für Anforderung Nr.9 und 10 (Informationssteckbrief) 117
5.15 Projekt-Architektur für den Informationssteckbrief 118
5.16 Qualitätsmodell für den Informationssteckbrief 120
5.17 Prozessmodell für den Informationssteckbrief 121
5.18 AA-Modellierung für Anforderung Nr.1 und 2 126
5.19 AA-Modellierung für Anforderung Nr.3 und 4 127
5.20 AA-Modellierung für Anforderung Nr.5 und 6 129
5.21 AA-Modellierung für Anforderung Nr.7 und 8 130
5.22 AA-Modellierung für Anforderung Nr.9 und 10 131
5.23 Projekt-Architektur für den Messenger 133
5.24 Qualitätsmodell für den Messenger 135

5.25 Prozessmodell für den Messenger 137
5.26 Identifizierte Risiken im AA-Modell für Anforderung 1 und 2 (Informationssteckbrief) 141
5.27 Identifiziertes Risiko im AA-Modell für Anforderung 3 und 4 (Informationssteckbrief) 143
5.28 Identifizierte Risiken im AA-Modell für Anforderung 5 und 6 (Informationssteckbrief) 144
5.29 Identifizierte Risiken im AA-Modell für Anforderung 9 und 10 (Informationssteckbrief) 145
5.30 Identifizierte Risiken in der Projektarchitektur des Informationssteckbriefs 147
5.31 Identifizierte Risiken im Qualitätsmodell des Informationssteckbriefs 149
5.32 Identifizierte Risiken im Prozessmodell des Informationssteckbriefs 151
5.33 Identifizierte Risiken im AA-Modell für Anforderung Nr.2 (Messenger) 153
5.34 Identifizierte Risiken im AA-Modell für Anforderung Nr.6 (Messenger) 155
5.35 Identifizierte Risiken in der Projektarchitektur des Messengers 156
5.36 Identifizierte Risiken im Prozessmodell des Messengers . . . 158
5.37 Übersicht über den Vergleich von Ist- und Soll-Zustand . . 163
5.38 Branchenübersicht 173
5.39 Softwareeinführung im öffentlichen und privaten Sektor . . 174
5.40 Maßnahmen, um digitale Transformation und digitale Souveränität zu meistern 175
5.41 Herausforderungen, digitale Transformation und digitale Souveränität zu meistern 177
5.42 Darstellung des Zusammenhangs zwischen den Clustern digitaler Transformation 179
5.43 Darstellung des Zusammenhangs zwischen den Clustern digitaler Souveränität 181
5.44 Forschungsdesign für die vorliegende Studie 192

5.45 Erfahrung der Experten 194
5.46 Vorteile beim Einsatz von Hyperscalern 196
5.47 Größte Herausforderungen bei der Nutzung souveräner Clouds 197
5.48 Analyseergebnis Architektur-Perspektive 206
5.49 Analyseergebnis Nutzerperspektive 207

6.1 Forschungsdesign für die Entwicklung des Referenzmodells . 215
6.2 Design-Prozess für die Entwicklung des Referenzmodells . . 216
6.3 Design Science Research Methode (Hevner et al., 2004) als methodischer Rahmen für die Entwicklung des Referenzmodells 217
6.4 Ausgangspunkt DISO-A: Digitale Souveränitätsmodell-Optimierung Academia (3. Version) 218
6.5 Zusammenhänge zwischen den Clustern aus dem DISO-A-Modell 220
6.6 Zuordnung der Studienergebnissen zu den Artefakten . . . 222
6.7 DISO!: Digitale Souveränitätsoptimierung - ein Referenzmodell 224

1 Dimensionen digitaler Souveränität nach Pohle (2020) . . . 260
2 Fragebogen erste Fallstudie (1/18) 285
3 Fragebogen erste Fallstudie (2/18) 286
4 Fragebogen erste Fallstudie (3/18) 287
5 Fragebogen erste Fallstudie (4/18) 288
6 Fragebogen erste Fallstudie (5/18) 289
7 Fragebogen erste Fallstudie (6/18) 290
8 Fragebogen erste Fallstudie (7/18) 291
9 Fragebogen erste Fallstudie (8/18) 292
10 Fragebogen erste Fallstudie (9/18) 293
11 Fragebogen erste Fallstudie (10/18) 294
12 Fragebogen erste Fallstudie (11/18) 295
13 Fragebogen erste Fallstudie (12/18) 296
14 Fragebogen erste Fallstudie (13/18) 297
15 Fragebogen erste Fallstudie (14/18) 298
16 Fragebogen erste Fallstudie (15/18) 299
17 Fragebogen erste Fallstudie (16/18) 300
18 Fragebogen erste Fallstudie (17/18) 301

19 Fragebogen erste Fallstudie (18/18) 302
20 Leitfaden zweite Fallstudie (1/3) 303
21 Leitfaden zweite Fallstudie (2/3) 304
22 Leitfaden zweite Fallstudie (3/3) 305
23 Leitfaden zweite Fallstudie (3/3) 306
24 Leitfaden zweite Fallstudie (3/3) 307
25 Leitfaden dritte Fallstudie (1/14) 308
26 Leitfaden dritte Fallstudie (2/14) 309
27 Leitfaden dritte Fallstudie (3/14) 310
28 Leitfaden dritte Fallstudie (4/14) 311
29 Leitfaden dritte Fallstudie (5/14) 312
30 Leitfaden dritte Fallstudie (6/14) 313
31 Leitfaden dritte Fallstudie (7/14) 314
32 Leitfaden dritte Fallstudie (8/14) 315
33 Leitfaden dritte Fallstudie (9/14) 316
34 Leitfaden dritte Fallstudie (10/14) 317
35 Leitfaden dritte Fallstudie (11/14) 318
36 Leitfaden dritte Fallstudie (12/14) 319
37 Leitfaden dritte Fallstudie (13/14) 320
38 Leitfaden dritte Fallstudie (14/14) 321
39 Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (1/13) . 322
40 Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (2/13) . 323
41 Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (3/13) . 324
42 Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (4/13) . 325
43 Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (5/13) . 326
44 Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (6/13) . 327

45 Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (7/13) . 328
46 Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (8/13) . 329
47 Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (9/13) . 330
48 Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (10/13) 331
49 Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (11/13) 332
50 Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (12/13) 333
51 Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (13/13) 334
52 Interviewleitfaden zum Papier »Affordances in Open Source Projects« 335
53 Interviewleitfaden zum Papier »Digital Sovereignty and Digital Transformation Practice Recommendation for the Software Life Cycle Process« (1/4) 336
54 Interviewleitfaden zum Papier »Digital Sovereignty and Digital Transformation Practice Recommendation for the Software Life Cycle Process« (2/4) 337
55 Interviewleitfaden zum Papier »Digital Sovereignty and Digital Transformation Practice Recommendation for the Software Life Cycle Process« (3/4) 338
56 Interviewleitfaden zum Papier »Digital Sovereignty and Digital Transformation Practice Recommendation for the Software Life Cycle Process« (4/4) 339
57 Fragebogen zum Papier »Digital Sovereignty through Sovereign Clouds« (1/2) 340
58 Fragebogen zum Papier »Digital Sovereignty through Sovereign Clouds« (2/2) 341

Tabellenverzeichnis

3.1 Soft Design Science Methodology (SDSM) Aktivitäten nach Pries-Heje et al. (2014) 18

4.1 Übersicht der Befragten in der ersten Fallstudie 28
4.2 Ergebnis des Clustering-Verfahrens nach Mayring und Brunner (2007) (I/II) 33
4.3 Ergebnis des Clustering-Verfahrens nach Mayring und Brunner (2007) (II/II) 34
4.4 Bewertung der Faktoren und Entscheidung für die Zuordnung zu einem Cluster 39
4.5 Ergebnis aus dem Vergleich von entwickelten Themenclustern digitaler Souveränität und denen in den Publikationen . . . 40
4.6 Übersicht der Befragten in der zweiten Fallstudie 52
4.7 Überblick über die Gewichtungen im Friedensfall, im Verteidigungsfall und deren Differenz 54

5.1 Teilnehmer an der Retrospektive (Projekt: Informationssteckbrief) 106
5.2 Teilnehmer an der Retrospektive (Projekt: Messenger) . . . 107
5.3 Anforderungen Informationssteckbrief 110
5.4 Anforderungen Messenger 124
5.5 Zitate aus den Retrospektiven mit den Projektteams 138
5.6 Affordanzanalyse Open Source Projekt Nr.1: Messenger . . 159
5.7 Affordanzanalyse Open Source Projekt Nr.2: Informationsbrief 161
5.8 Soft Design Science Methode (Quelle: Pries-Heje et al. (2014)) 171

5.9 Zuordnung der ermittelten Handlungsempfehlungen zu bestimmten Prozessgruppen und Prozessen (Stelter et al., 2025) 186
5.10 Berufsbezeichnung und Schwerpunkt der Arbeit der befragten Experten 193
5.11 Analyseergebnis Managementperspektive 202

1 Google Scholar Suche »digitale Souveränität« 261
2 Google Scholar Suche »digitale Souveränität« 262
3 Google Scholar Suche »digital sovereignty« 263
4 Google Scholar Suche »digital sovereignty« 264
5 Google Scholar Suche »digital sovereignty« 265
6 Google Scholar Suche »digital sovereignty« 266
7 Google Scholar Suche »digital sovereignty« 267
8 Google Scholar Suche »digital sovereignty« 268
9 Google Scholar Suche »digital sovereignty« 269
10 Google Scholar Suche »digital sovereignty« 270
11 UniBw Suche 271
12 AIS Library Suche 272
13 Suche nach Beratungskonzepten 273
14 Übersicht über die Risiken im Projekt Informationssteckbrief und Empfehlungen zum Umgang mit dem Risiko (1/2) . . 274
15 Übersicht über die Risiken im Projekt Informationssteckbrief und Empfehlungen zum Umgang mit dem Risiko (2/2) . . 275
16 Übersicht über die Risiken im Projekt Messenger und Empfehlungen zum Umgang mit dem Risiko 276
17 Analyseergebnis 1: Referenzmodellierung 277
18 Analyseergebnis 2 (1/3): Referenzmodellierung 278
19 Analyseergebnis 2 (2/3): Referenzmodellierung 279
20 Analyseergebnis 2 (3/3): Referenzmodellierung 280
21 Analyseergebnis 3 (1/2): Referenzmodellierung 281
22 Analyseergebnis 3 (2/2): Referenzmodellierung 282
23 Analyseergebnis 4 (1/2): Referenzmodellierung 283
24 Analyseergebnis 4 (2/2): Referenzmodellierung 284

Liste der Akronyme und Abkürzungen

AA	Agile Anforderungsmodellierung
API	Application Programming Interfaces
AWS	Amazon Web Services
B2B	Business to Business
B2C	Business to Customer
BMDV	Bundesministerium für Digitales und Verkehr
BMI	Bundesministerium des Innern und für Heimat
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BSI	Bundesamt für Sicherheit in der Informationstechnik
Bw	Bundeswehr
BWL	Betriebswirtschaftslehre
CPU	Central Processing Unit
DIN	Deutsches Institut für Normung
DSB	Datenschutzbehörden des Bundes und der Länder
ETL	Extract, Transform, Load
ER	Entity Relationship
EU	Europäische Union
FAU	Friedrich-Alexander-Universität Erlangen-Nürnberg
IEEE	Institute of Electrical and Electronics Engineers
INF	Informatik
IT	Informationstechnologie
KI	Künstliche Intelligenz

LV	Landesverteidigung
NLP	Neuro-Linguistisches Programmieren
Nr	Nummer
OS	Open Source
RAM	Random Access Memory
SDSM	Soft Design Science Methodology
SLA	Service Level Agreements
SSSS	Secondary Security Screening Selection
UniBw	Universität der Bundeswehr
RTC	Web Real-Time Communication
VS-NfD	Verschlusssachen – nur für den Dienstgebrauch
WINF	Wirtschaftsinformatik

1

Einleitung

„Digitale Souveränität ist für mich ein strategisch-technologisches Problem, das sehr weitreichende Herausforderungen angeht. Darunter, wie sich der Staat aufstellen kann, um die Abhängigkeit von bestimmten Ländern bei Softwareeinkäufen und Hardwarelieferungen zu reduzieren. Auf individueller Ebene stellt sich die Frage, wie wir die Daten von Bürgern und Bürgerinnen besser schützen können. Und auf ökonomischer Ebene, wie Unternehmen ihre eigenständige Handlungsfähigkeit bewahren oder erweitern können. Das geht einher mit Themen wie Wettbewerbsfähigkeit, IT-Sicherheit, Innovation, Bildung, politischen Rahmenbedingungen, Schlüsseltechnologien und vielem mehr". (Martha Klare)

1.1 Motivation und Problemstellung

Themen wie die Sicherung digitaler Räume, die Wiedergewinnung von Fairness in digitalen Märkten und nicht zuletzt die Stärkung digitaler Souveränität einzelner europäischer Staaten sind zentral für die europäische Union und die Bundesrepublik Deutschland (Pohle, 2020). Bei der Diskussion über mehr digitale Souveränität gehen politische Vorhaben mit Fragen zu IT-Strategien, Innovationsförderungen, neuen Technologien und - speziell im Kontext kriti-

scher Infrastrukturen - Themen wie staatliche Sicherheit, Verantwortung und Regulierungen, einher (Floridi, 2020; Klare & Lechner, 2024b). Richtungsweisend für diese Entwicklung ist die strategische Agenda der europäischen Union, die vorsieht, dass mit positivem Weitblick eine effektivere Steuerung innerhalb von Europa möglich ist (Petit et al., 2024).

Abhängigkeiten zu Techkonzernen werden deutlich, die sich als Monopolisten für Unternehmen, das deutsche Behörden-Umfeld und für Bürger in Deutschland entwickeln (K. Fritzsche et al., 2022; Klare & Lechner, 2023). Dies führt einerseits für Unternehmen dazu, dass kaum Handlungsspielraum bei Preisverhandlungen besteht und man mit Lock-In-Effekten zu kämpfen hat; andererseits müssen staatliche Institutionen die Datenspeicherung auf amerikanischen Clouds, die Hardwarezulieferung von chinesischen Unternehmen und die zunehmende Software-Abhängigkeit von einigen wenigen Unternehmen für den öffentlichen Sektor grundlegend überdenken (Avila Pinto, 2018; Janßen, 2023; Klare & Lechner, 2024b; Pohle, 2020).

Die Debatte rund um mehr digitale Souveränität ist facettenreich. Sie drängt in staatliche, individuelle und unternehmerische Dimensionen. Auch wenn ihr Ursprung in der Politik liegt, beschäftigen sich heute ganz unterschiedliche Wissenschaften mit dem Thema (Klare & Lechner, 2025; Klare, Lechner & Fritzsche, 2025).

Wie in der folgenden Abbildung 1.1 zu erkennen ist, nimmt die Anzahl der Publikationen zum Thema digitale Souveränität seit 2013 zu. Auch die Bandbreite der Stellungnahmen vergrößert sich. Zum 25.01.2025 liefert eine Google-Scholar-Suche nach Publikationen unter dem Suchbegriff „digital sovereignty“ in Summe mehr als 350.000 Ergebnisse. Zum 28.08.2025 liefert die gleiche Suche ungefähr 554.000 Ergebnisse. So fragen sich beispielsweise Lambach und Oppermann (2023), wie der Staat souveräner werden kann, Bellanova et al. (2022), welche potenziellen Innovationsfelder gefördert werden sollten, oder Reiners (2021), wie die europäische Union zur Stärkung deutscher Souveränität beitragen kann.

Auch Unternehmen fordern die Stärkung digitaler Souveränität; das geht einer Bitkom-Studie aus dem Jahr 2024 hervor (Paulsen, 2024). Besonders aus dieser Studie ist hervorzuheben, dass zwei Drittel der Unternehmen die

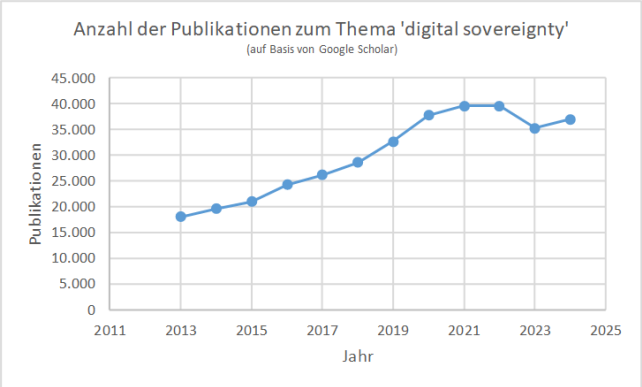


Abbildung 1.1: Anzahl der Publikationen unter dem Suchbegriff 'digital sovereignty' von 2013 bis 2025 (abgefragt am 25. Februar 2025)

große Abhängigkeit von einzelnen Ländern Sorgen bereitet. Als konkretes Beispiel nennen sie China (Paulsen, 2024). Einer der größten Handelsimporteure Deutschlands für Hardware ist China (Paulsen, 2024). Betrachtet man speziell die deutschen Importe, so stellt man fest, dass Chips und Hardware zu den Top-Digitalimporten aus China bzw. Taiwan nach Deutschland gehören (Paulsen, 2024). Im Falle einer Krise sind die Halbleiter-, und Hardwarebeschaffungs-Alternativen für die Bundesrepublik eher rar (Hofmeier et al., 2024; Merkel, 2019).

Meine Motivation ist es, einen Beitrag zum laufenden Diskurs zu leisten, indem ich Firmen eine Orientierungshilfe biete, wie sie digitale Souveränität kurz-, mittel- oder langfristig stärken kann. Zudem führt mich die große Breite der Anwendungen des Begriffs in unterschiedlichsten Kontexten zu der Frage, wie man digitale Souveränität definieren kann. Heißt digitale Souveränität eine Regulierung digitaler Dienste zur Wahrung von Firmengeheimnissen deutscher Unternehmen? Oder bedeutet digitale Souveränität, mit anderen Nationen zusammenzuarbeiten, sodass deutsche Unternehmen Alternativen haben, falls ausländische Politiker Zölle auf digitale Waren erheben oder Lieferungen nach Deutschland blockieren sollte? Oder bedeutet digitale Souveränität die unternehmensinterne Entwicklung von Open-Source-Software, um vielfältige Strukturen zu schaffen, die eine schnelle Anpassung ermöglichen?

Es fehlt ein zusammenhängender Überblick darüber, wie Unternehmen

mit dem Thema digitale Souveränität umgehen können. Dabei zeigen die vorangegangenen Ausführungen, dass eine Auseinandersetzung mit dem Thema an der Schnittstelle zwischen Politik, Informatik und IT-Beratung zur Gestaltung von IT-Strategien fehlt, jedoch besonders bedeutsam ist, um Wege aufzuzeigen, wie digitale Souveränität gestaltet werden kann. In dieser Arbeit werden technologische Aspekte, Prozesse und Aspekte auf Projektebene betrachtet, um Antworten auf verschiedene Fragen zu finden. Darunter zum Beispiel, auf welche Technologien Unternehmen setzen können, um die digitale Souveränität zu stärken. Oder wie man den Softwareeinführungsprozess in Unternehmen souveräner gestalten kann, ob Open Source wirklich der Weg zur Stärkung digitaler Souveränität ist und ob souveräne Clouds Ermöglicher für mehr digitale Souveränität sind.

1.2 Forschungsfragen

Aus dieser Gemengelage ergeben sich folgende Forschungsfragen:

1. Was bedeutet digitale Souveränität?
2. Wie kann man digitale Souveränität erreichen?
3. Wie kann ein Referenzmodell für die Stärkung digitaler Souveränität in Unternehmen aussehen?

Die Abbildung 1.2 auf der nächsten Seite zeigt die Forschungsfragen, die in den jeweiligen Kapiteln dieses Buches adressiert werden. Die Analysen sind für sich alleinstehend. Das heißt, dass jeweils unterschiedliche Perspektiven auf das Thema je nach Kapitel eingenommen werden und damit auch mit unterschiedlichen Ergebnissen geschlussfolgert wird.
Zur Entwicklung des Referenzmodells dienen vor allem die Antworten auf die ersten zwei Forschungsfragen (siehe Kapitel 4 und 5).

1.3 Abgrenzung zu anderen Teilgebieten und Kooperationen

Diese Arbeit grenzt sich wie folgt von anderen Teilbereichen des laufenden Diskurses über digitale Souveränität ab: Erstens wird die Perspektive der IT-Beratung im Themenkomplex digitale Souveränität eingebracht sowie Forschungsergebnisse zu Schlüsseltechnologien, Open Source, souveränen

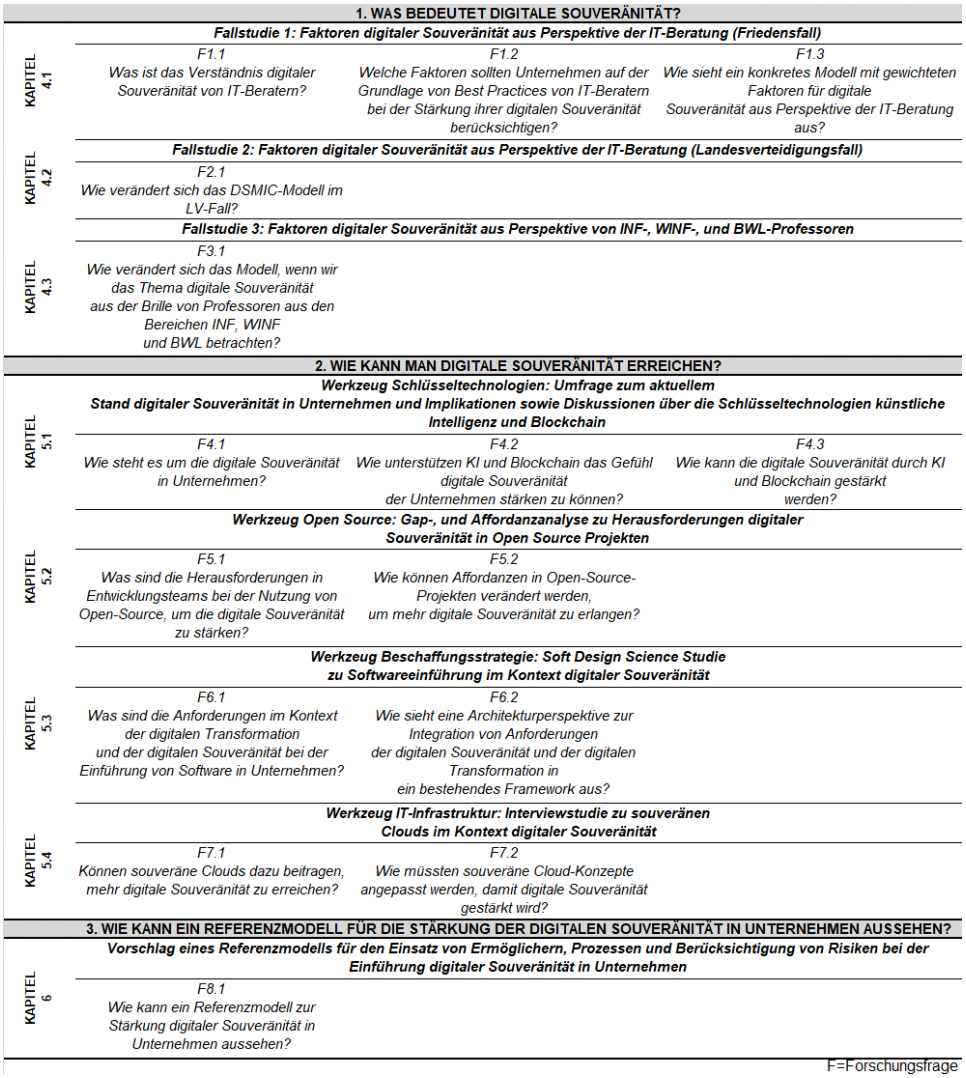


Abbildung 1.2: Aufbau der Dissertationsschrift

Clouds und Referenzmodellierung. Zweitens konzentriert sich die Sichtweise auf Unternehmen, die einer Gesetzgebung unterliegen, die digitale Souveränität fordert. Drittens werden aufgrund der Zuordnung dieser Arbeit zum Lehrstuhl Wirtschaftsinformatik insbesondere Forschungsbeiträge aus der Informatik, Wirtschaftsinformatik und Betriebswirtschaftslehre analysiert. Um der Debatte gerecht zu werden, werden auch die Bereiche Innovationsmanagement, Sozialwissenschaft, Philosophie und Politik angeschnitten.

Mein Promotionsprojekt ist eingebettet in das Forschungsprojekt LIONS

(dtec.bw) und lebt von der Kooperation zwischen der UniBw München und der BWI GmbH. Im Rahmen der Forschungskooperation mit der BWI konnten Inspirationen für diese Forschung gewonnen werden. So beobachtete ich Herausforderungen in der Industrie und erlangte praxisnahe Erkenntnisse für diese Forschung und griff auf eine Vielzahl von Interviewpartnern vieler verschiedener Unternehmen zurück. Die BWI bietete zudem finanzielle Förderung und schaffte Freiräume für diese Forschung. Das Projekt LIONS wird vom dtec.bw (Forschungszentrum Digitalisierung und Technik der Bundeswehr) gefördert und sieht die Erhöhung von digitaler Souveränität und Resilienz mittels Designmöglichkeiten vor. Als Doktorandin an der UniBw München bestand auch die Möglichkeit mit Universitäten und Hochschulen in Austausch zu treten. Zudem sind universitäre und außeruniversitäre Forschungskollaborationen eingegangen worden, um verstärkt Reliabilität, Objektivität und Validität in den Ergebnissen zu gewährleisten. Die Forschungsergebnisse wurden auf Konferenzen veröffentlicht, mehrmals gereviewt, vorgestellt und mit internationalen Forschenden diskutiert. Weitere Diskussionen mit interdisziplinären Forschungsgruppen erfolgten auf dem LIONS Symposium *Ledger Innovation and Operation Network for Sovereignty* oder mit der Fachgruppe *Frauen und Informatik*. Das Gelernte fließt in diese Arbeit ein.
Eine Übersicht aller Publikationen mit Bezug zur Thesis findet sich unter dem nächsten Teilabschnitt.

1.4 Publikationen mit Bezug zur Thesis

1. Klare, M., Verlande, L., Greiner, M. and Lechner, U. (2023). How Blockchain and Artificial Intelligence influence Digital Sovereignty. In: Papadaki, M., Rupino da Cunha, P., Themistocleous, M., Christodoulou, K. (eds) Information Systems. *EMCIS 2022*. Lecture Notes in Business Information Processing, vol 464. Springer, Cham. https://doi.org/10.1007/978-3-031-30694-5_1

2. Klare, M., and Lechner, U. (2023). Digital Sovereignty from the Perspective of IT Consultancy in Germany: A Model. *ICSOB Companion*, 1–14. https://ceur-ws.org/Vol-3621/poster-paper5.pdf -> Award: Best Poster Paper

3. Klare, M., and Lechner, U. (2024). German Digital Sovereignty–Success Factors in a National Defense Scenario from the Standpoint of IT Consultancy. In I. Fries, M. Grabatin and M. Hofmeier (Hrsg.), *LIONS Sovereign by Design* (pp. 41–56). Logos Verlag Berlin. https://doi.org/https://doi.org/10.30819/5834

4. Klare, M., and Lechner, U. (2024). A Reference Model to Strengthen Digital Sovereignty in Companies. *ICSOB Companion*, 1–9. https://ceur-ws.org/Vol-3921/phd-paper3.pdf

5. Hofmeier, M., Klare, M., Fries, I., und Weeber, K. (2024). Digitale Souveränität: Handlungsempfehlungen. *LIONS Bericht*, 1-10. https://www.unibw.de/lions/lions_handlungsempfehlungen_digital.pdf

6. Klare, M., and Lechner, U. (2025). Digital Sovereignty: Affordances in Open Source Projects. In E. Papatheocharous, S. Farshidi, S. Jansen and S. Hyrynsalmi (Hrsg.), *Software Business* (pp. 20–34). https://doi.org/https://doi.org/10.1007/978-3-031-85849-9_2

7. Klare, M., Hrestic, R., Stelter, A., and Lechner, U. (2025). Digital Sovereignty and Digital Transformation Practice Recommendation for the Software Life Cycle Process. *International Conference on Digital Sovereignty, 254*, 221–229. /https://doi.org/10.1016/j.procs.2025.02.081

8. Klare, M., Lechner, U., and Fritzsche, A. (2025). Digital Sovereignty through Sovereign Clouds? *International Conference on AI and the Digital Economy.* -> Award: Highly Commended Paper -> **to appear**

9. Stelter, A., Klare, M., Lechner, U. (2025). Digital Sovereignty and Digital Transformation Extension for the Software Life Cycle Process in ISO/IEC/IEEE 12207:2017. *Artificial Intelligence in Context of Digital Sovereignty.* -> **to appear**

1.5 Struktur der Arbeit

Diese Arbeit folgt folgender Struktur: Einleitung (siehe Kapitel 1), theoretische Grundlagen (siehe Kapitel 2), Forschungsdesign (siehe Kapitel 3), Analysen

und Modelliterationen (siehe Kapitel 4), Werkzeuge zur Umsetzung digitaler Souveränität (siehe Kapitel 5), Referenzmodell für die Stärkung digitaler Souveränität in Unternehmen (siehe Kapitel 6) und Fazit, Zusammenfassung, Limitationen, Ausblick (siehe Kapitel 7).

In der *Einleitung* dieser Dissertationsschrift werden die Motivation der Forschung und die Problemstellung deutlich. Darunter, warum es wichtig ist digitale Souveränität im Unternehmenskontext und aus Sicht der IT-Beratung zu betrachten und welche Forschungslücke adressiert wird. Zudem finden sich die konkreten Forschungsfragen, die im Rahmen des Buches beantwortet werden und eine tabellarische Übersicht über den Aufbau der Arbeit. Wie sich die hier dargestellte Perspektive digitaler Souveränität von anderen Teilgebieten abgrenzt und welche Kooperationen im Rahmen des Promotionsprojekts einen Einfluss auf diese Perspektive hatten, wird ebenfalls dargestellt. Zum Schluss folgt eine Übersicht über die Publikationen, die mit Bezug zur Thesis, bereits veröffentlicht wurden.

Der *theoretische Grundlagenteil* umfasst Forschungsbeiträge, Modelle, Theorien und eine Arbeitsdefinition für digitale Souveränität. In diesem Abschnitt wird das Verständnis digitaler Souveränität aus unterschiedlichen Perspektiven vorgestellt.

Das für diese Arbeit verwendete *Forschungsdesign* lehnt sich an die Soft Design Science Methode (SDSM) nach Pries-Heje et al. (2014) an. Im praktischen „Doing“ ist es notwendig, auf SDSM zurückzugreifen, weil in dieser Arbeit das Verständnis der Konzepte und der Bedarfe eine wesentliche Rolle spielt. So zeigt sich der Mehrwert der Orientierung an Pries-Heje et al. (2014), wenn aus dem allgemeinen Problem digitaler Souveränität, allgemeine Anforderungen extrahiert und allgemeine Lösungen entworfen und bewertet werden.

Der *Ergebnis-Abschnitt* ist anhand der oben genannten drei Forschungsfragen gegliedert. Im ersten werden drei Fallstudien vorgestellt. Die Fallstudien bauen aufeinander auf. Die erste Fallstudie leistet einen Beitrag zu der Erschließung eines neuen Modells für digitale Souveränität aus der Perspektive der IT-Beratung. In der zweiten Fallstudie folgt ein Vergleich der Ergebnisse der ersten Fallstudie mit den Ergebnissen der zweiten Fallstudie. Hier finden sich Ergebnisse zu Erfolgsfaktoren für mehr digitale Souveränität in einem Szenario zur

Landesverteidigung wieder. Sicherheit, Unabhängigkeit und Selbstbestimmtheit sind in einem Fall der Landesverteidigungsfall Deutschlands besonders bedeutsam, was die Notwendigkeit der Analyse dieses besonderen Falls erklärt. Die Ergebnisse werden in das Modell aus der ersten Fallstudie übertragen und ein neues, erweitertes Modell ist das neue Artefakt. Die dritte Fallstudie resultiert aus der Überlegung, dass sich das aktuelle Modell ausschließlich auf die Perspektive der IT-Beratung konzentriert. Dieser Ansatz kann problematisch sein, da die Faktoren und ihre Bedeutung je nach der befragten Gruppe variieren können. Die Meinungen von Professoren aus den Bereichen INF, WINF und BWL tragen zu neuen wirtschaftlichen und technischen Überlegungen bei, die in einer Erweiterung des Modells münden. Dieses Vorgehen führt zum DISO-A-Modell: *Digitale Souveränitätsmodell-Optimierung Academia*. Das Modell inkludiert das Verständnis, das im Rahmen der Arbeit von digitaler Souveränität angenommen wird. Es enthält erhobene Erfolgsfaktoren für mehr digitale Souveränität und eine Gewichtung der Faktoren.

Die darauffolgenden Analysen und Modelliterationen widmen sich der Frage, wie man digitale Souveränität erreichen und modellieren kann. Hier werden die folgenden veröffentlichten Forschungsergebnisse vorgestellt, reflektiert und diskutiert: 1) Stand digitaler Souveränität in Unternehmen und Blockchain sowie künstliche Intelligenz im Kontext von digitaler Souveränität, 2) Affordanzen in Open-Source-Projekten für die Gestaltung digitaler Souveränität in Unternehmen, 3) souveräne Software-Lebenszyklusprozesse und 4) Diskussionen zu souveränen Clouds als Ermöglicher digitaler Souveränität.

Die letzte Forschungsfrage resuliert aus der Überlegung, dass eine Verständniserweitung digitaler Souveränität nicht ausreicht, um zu beantworten, wie man digitale Souveränität durchsetzen kann. Es braucht Design-Empfehlungen. Somit sieht das Kapitel 7 die Darstellung eines Referenzmodells für digitale Souveränität in Unternehmen vor. Ziel ist es mit dem Referenzmodell aufzuzeigen, auf was Unternehmen bei der Transformation hin zu mehr digitaler Souveränität achten sollten. Das Referenzmodell umfasst strategische, technologische, organisationale, als auch operative Leitplanken, wie digitale Souveränität gestärkt werden kann, als auch das Verständnis digitaler Souveränität, das in dieser Arbeit angenommen wird.

In der *Zusammenfassung* sind die wichtigsten Ergebnisse aus der Arbeit zusammengefasst. Außerdem finden sich hier die Diskussion und Limitationen wieder. Zum Schluss folgt ein Ausblick, bei dem konkret aufgezeigt wird, wie weitere Forscher [1] auf den hier vorgestellten Erkenntnissen aufbauen können.

[1] Um den Schreibfluss nicht zu stören, wird in dieser Arbeit nicht durchgängig gegendert. Bei Verwendung der männlichen grammatikalischen Form ist eine Inklusion des weiblichen Pendants gemeint.

2

Stand von Wissenschaft und Praxis

Weil diese Arbeit einen Beitrag zum Verständnis digitaler Souveränität leistet, ist zunächst ein Überblick über den Stand der Diskussion und Begriffsbildung in Wissenschaft und Praxis erforderlich.

2.1 Digitale Souveränität

Es zeigt sich die Notwendigkeit, sich mit der Frage auseinanderzusetzen, was digitale Souveränität insbesondere für Unternehmen bedeutet und welche Strategie sowie welches Vorgehen zu ihrer Stärkung beitragen können. Es scheint wesentlich, digitale Souveränität für diese Arbeit zu definieren. Die Vielfalt an Verständnissen digitaler Souveränität macht eine allgemein zufriedenstellende Definition abstrakt. Um dennoch eine Arbeitsdefinition zu erreichen, nähern sich die folgenden Abschnitte einer Definition an, indem Theorien, Perspektiven, Szenarien, Schlüsseltechnologien und Ansätze festgelegt werden, die im Zusammenhang mit digitaler Souveränität in dieser Arbeit genauer analysiert werden sollen.

Grundsätzlich ist anzumerken, dass man Souveränität einer Person oder Institution nur schwer als feststehendes Attribut zu schreiben kann. Wie Sauer et al. (2022) klarstellen, hat Souveränität eher relationalen Charakter. Sie bezieht sich auf die Möglichkeit, in Situationen als Handlungsträger in Erscheinung zu treten. Dies bedeutet, dass man nicht nur Sachzwängen folgt, die in Situationen auferlegt werden, oder einen fixen Entscheidungsalgorithmus zur Anwendung bringt. Souveränität bezieht sich auf Kategorien von Selbstbestimmtheit, Autorität und Übernahme von Verantwortung (A. Fritzsche, 2022), die im Angesicht gesellschaftlicher Transformationsprozesse immer wieder neu verhandelt werden müssen. Dies ist gerade heute durch die rasante Entwicklung digitaler Technologien der Fall.

2.1.1 Digitale Transformation und digitale Souveränität

Der Zusammenhang zwischen digitaler Transformation und digitaler Souveränität wird ersichtlich, weil digitale Transformation mit einer Veränderung auf wirtschaftlicher, gesellschaftlicher, technologischer und auch kultureller Ebene einhergeht. Digitale Souveränität schneidet ebenfalls diese Bereiche an. Aus dieser Betrachtung heraus, könnte digitale Souveränität somit als Transformationsversuch verstanden werden, was auch bei K. Fritzsche und Spoiala (2022) Andeutung findet. Dies soll im Rahmen der noch folgenden Ergebniskapitel kritisch hinterfragt und auf Basis erhobener Daten bestätigt oder widerlegt werden. Verhoef et al. (2021) definieren Digitalisierung als Informationensumwandlung, die keinen direkten Mehrwert für Aktivitäten schafft. Dieses Verständnis bezieht sich in der Regel auf die Digitalisierung von internen und externen Prozessen und hat eine unternehmerische Ausrichtung (Verhoef et al., 2021). Obwohl es konzeptionelle Unterschiede gibt, werden die Begriffe Digitalisierung und digitale Transformation oft austauschbar verwendet, um sich auf ein umfassendes Konzept zu beziehen, das ein Ökosystem betrifft (Klare, Hrestic et al., 2025; Reis et al., 2018). Digitalisierung ist der Prozess, bei dem Unternehmen digitale Technologien einsetzen, um bestehende Geschäftsprozesse zu optimieren und eine effizientere Koordination zwischen ihnen zu ermöglichen. Sie kann einen Mehrwert schaffen, indem sie die Erfahrungen der Nutzer verbessert (Verhoef et al., 2021) und Wettbewerbsvorteile steigert,

indem sie beispielsweise neue Dienstleistungen über virtuelle Kanäle anbietet oder neue Systeme für das Betriebsmanagement ermöglicht (Reis et al., 2020). Die digitale Transformation ist schließlich die umfassendste Phase des Digitalisierungsprozesses in einem Unternehmen. Sie geht über die Digitalisierung hinaus und verändert das Unternehmen durch die Entwicklung eines neuen Geschäftsmodells (Verhoef et al., 2021). So ist es auch bei digitaler Souveränität.

Gong und Ribiere (2021) führten eine systematische Überprüfung und Analyse von 134 Definitionen der digitalen Transformation durch, um eine einheitliche Definition zu finden. Die Autoren definieren die digitale Transformation als einen Prozess des grundlegenden Wandels, der durch den innovativen Einsatz digitaler Technologien ermöglicht und durch die strategische Nutzung von Schlüsselressourcen und -fähigkeiten begleitet wird. Ziel ist die radikale Veränderung einer Unternehmung und die Neudefinition ihres Wertversprechens für alle Beteiligten. Ein Unternehmen kann sich auf eine Organisation, ein Geschäftsnetzwerk, eine Branche oder eine Gesellschaft beziehen.

2.1.2 Perspektive auf digitale Souveränität: IT-Beratung

Um zu erklären, was digitale Souveränität ist, soll auch der Frage nachgegangen werden, für wen sie zu definieren ist. Eine Perspektive, die diese Arbeit einnimmt, ist die der IT-Beratung.

IT-Beratung ist die Unterstützung eines Kunden, also eines Unternehmens, in den Bereichen IT-Strategien, IT-Prozesse, Organisationsstrukturen und IT-Lösungen, die monetär vergütet wird (Scheer & Köppen, 2013; Zillmann, 2021). IT-Berater entwerfen Sicherheitskonzepte, analysieren IT-Risiken und bieten Lösungen für Kunden unter Berücksichtigung regulatorischer Anforderungen (z.B. des Datenschutzes) (Kumar et al., 2017; Scheer & Köppen, 2013). Den Zusammenhang zwischen IT-Beratung und digitaler Souveränität zu untersuchen, ist relevant in der Praxis, weil im Begriff der Beratung bereits die Vorstellung angelegt ist, den Beratenen handlungsfähig zu machen und Autorität über die eigenen Entscheidungen zu sichern. Dies zeigt sich auch gerade dort, wo ein IT-Berater Kunden bei der Suche nach herstellerunabhängigen IT-Lösungen unterstützt (Deelmann, 2006; Klare & Lechner, 2023). Dies legt die Bedeutung der Betrachtung von IT-Beratungen im Zusammenhang mit digitaler Sou-

veränität nahe. Seyffarth (2023) fordern herstellerunabhängige IT-Lösungen und Andenmatten (2023) die stärkere Berücksichtigung regulatorischer Datenanforderungen. Diese Forderungen werden auch unter dem Deckmantel digitaler Souveränität in der Politik laut (BMI, 2023; IT-Planungsrat, 2013).

2.1.3 Ansätze zum Umgang mit digitaler Souveränität

In dieser Dissertationsschrift werden drei Ansätze einer besonderen Betrachtung unterzogen: Das ist Open Source (Moerel & Timmers, 2021), souveränere Lieferketten (Mörl, 2024) und souveräne Clouds (Rone, 2024) als potenzielle Ermöglicher digitaler Souveränität.

2.1.3.1 Open Source und digitale Souveränität

Open Source als Begriff bezieht sich in dem hier vorliegenden Verständnis auf die Softwareentwicklung (Gacek & Arief, 2004). Entwickler arbeiten über das Internet zusammen und dürfen mit der Verwendung von Open Source Software den Quellcode und die Software kopieren, ohne dafür zu bezahlen (Perens et al., 1999). Außerdem ist eine Modifikation der Software und des Quellcodes erlaubt. In welcher Art und Weise dies der Fall ist, muss immer den jeweiligen Lizenzbestimmungen der Software entnommen werden. Open Source sieht also neben der freien Zugänglichkeit des Quellcodes eines Systems die Zulässigkeit zur Verwendung einer Softwarelizenz vor (Laurent, 2004).

Es ist wichtig, den Zusammenhang von Open Source und digitaler Souveränität tiefgehender zu analysieren, da es verschiedene Publikationen gibt, die darauf hinweisen, dass Open Source der Weg zu mehr digitaler Souveränität sein könnte (Bechara & Lechner, 2024; Biström et al., 2024; Hofmeier et al., 2024; Moerel & Timmers, 2021). Beim Verständnis digitaler Souveränität in diesem Zusammenhang ist insbesondere der folgende Balance-Akt wesentlich: eine stärkere Unabhängigkeit von IT-Monopolisten vs. Verfügbarkeit, Skalierbarkeit und Leistungsfähigkeit durch moderne Open-Source-Komponenten (Fries et al., 2022; Wallenhorst, 2023). Das heißt, in dieser Arbeit soll ein Beitrag zum Verständnis darüber erlangt werden, wie man mit Open Source die genannten Vorteile nutzen kann und gleichzeitig eine gewisse Unabhängigkeit von großen IT-Monopolisten schaffen kann. Zudem ist darauf einzugehen, welche Herausforderungen sich durch Open Source im Kontext digitaler

Souveränität ergeben und wie man diese Herausforderungen angehen kann.

2.1.3.2 Softwarelieferketten, Software-Lebenszyklus und souveräne Softwareeinführung

Diese Dissertationsschrift begrenzt den Begriff der Softwarelieferkette auf die Einführung von Software in ein Unternehmen. Dies kann, wie es bereits im Namen steckt, über die Lieferkette eines Unternehmens abgebildet werden (Verwijmeren, 2004). Um Software als Ressource in der Gesamtarchitektur eines Unternehmens berücksichtigen zu können, wurde eine internationale Norm geschaffen: die *ISO/IEC/IEEE 12207 Systems and software engineering - Software life cycle processes*, die seit ihrer Einführung im Jahr 1995 mehrfach aktualisiert wurde. Sie bietet einen prozessualen Leitfaden für die Einführung von Software in Unternehmen mit Prozessgruppen und Serviceleistungen. Dabei unterstreicht die Norm, dass Software nicht nur entwickelt, sondern auch genutzt, beschafft, entworfen, betrieben und ausgemustert werden kann. Die ISO/IEC/IEEE 12207 verfolgt das Ziel, den gesamten Lebenszyklus einer Software im Rahmen ihrer Einführung abzubilden. Damit umfasst es wesentliche Prozesse für den Softwarelebenszyklus, von der Idee bis zur Stilllegung.

In der Disziplin des Enterprise Architecture Managements werden andere Lebenszyklusphasen vorgeschlagen (Hanschke, 2022). TOGAF hat zum Beispiel Phasen von der Vision und der Geschäftsarchitektur bis hin zur Governance und dem Management von Architekturänderungen (Harrison, 2016). Das Wasserfall-Modell ist auf die Arbeit von W. Royce aus dem Jahr 1970 zurückzuführen (Royce, 1970) und das Spiralmodell der schnellen Anwendungsentwicklung auf B. W. Boehm (1988).

Diese Ansätze konzentrierten sich jedoch eher auf den Entwicklungsprozess und dessen Abwicklung in einem Projekt als auf den Lebenszyklus. Im Kontext digitaler Souveränität ist es notwendig, auch Phasen wie die Einführung von Software einzuschließen, was die Entscheidung zur ISO/IEC/IEEE 12207 erklärt.

2.1.3.3 Souveräne Clouds und digitale Souveränität

In diesem Ansatz wird eine souveräne Cloud als eine technische Lösung mit einem rechtlichen Rahmen für mehr Datensicherheit und die Gewährleistung

einer größeren Wahlfreiheit unter den gegebenen Marktbedingungen definiert (Rath et al., 2023; Urban & Garloff, 2022). Zum einen hat eine souveräne Cloud zum Ziel, operative Souveränität zu erreichen (Holfelder et al., 2022). Dies bedeutet mehr Kontrolle und Transparenz im Betrieb, die Gewährleistung eines effektiven Betriebs und gleichzeitig die Überwachung des Betriebs, um die Einhaltung von Vorschriften zu sichern. Zum anderen soll Software-Souveränität gewährleistet sein. Unter Software-Souveränität versteht man Transparenz darüber, welche Software wo eingesetzt wird und die Möglichkeit, diese möglichst schnell und einfach auszutauschen (Bratton, 2016). Und schließlich versprechen souveräne Clouds mehr Datensouveränität, als Public Cloud Konzepte, indem sie der Idee folgen, dass Daten auf der Grundlage von GDPR, Gesetzen und Regeln der EU gesammelt werden, dass Daten in einem bestimmten Land in der EU gespeichert werden und dass die EU die Autorität hat, Datenflüsse innerhalb Europas zu regeln (Rone, 2024). Dieses Verständnis souveräner Clouds, das angenommen wird, macht den Zusammenhang mit digitaler Souveränität deutlich: das Konzept verfolgt ähnliche Ziele wie die digitale Souveränität. Zur Differenzierung sind in Abschnitt 5.4 zusätzliche Definitionen von souveränen Clouds auf der Grundlage von Experten aus der Industrie zu finden.

2.1.4 Arbeitsdefinition von digitaler Souveränität für diese Arbeit

Digitale Souveränität meint in dieser Arbeit ein strategisches Konzept, das ein höheres Maß an Unabhängigkeit, Selbstbestimmtheit, Handlungsfähigkeit und Risikoabwägung im digitalen Raum fordert und mit der Frage einhergeht, welche technologischen und prozessualen Ermöglicher einen Beitrag für Unternehmen leisten können. Diese Arbeitsdefinition unterliegt der Erforschung verschiedener Anwendungsdomänen, konkret: Digitale Souveränität und die Schlüsseltechnologien KI und Blockchain, der Einsatz von Open Source, die Gestaltung souveräner Softwareeinführung und die Herausforderungen souveräner Clouds.

3

Forschungsdesign

3.1 Forschungsdesign für diese Arbeit

Da in dieser Arbeit Konzepte und Bedarfe eine wesentliche Rolle spielen, wird zunächst auf die Soft Design Science Methode zurückgegriffen. Zudem ist es das Ziel, ein Referenzmodell zu entwickeln. Hierfür wird auf das Forschungsparadigma Design Science Research zurückgegriffen.

3.1.1 Soft Design Science Methode (SDSM)

Als Orientierung dient Pries-Heje et al. (2014). Auf Basis von Pries-Heje et al. (2014) sind die folgenden acht Forschungsaktivitäten durchzuführen: (1) Das spezifische Problem verstehen: im vorliegenden Fall handelt es sich um digitale Souveränität. (2) Das allgemeine Problem extrahieren: das wird für jede einzelne Studie dieser Arbeit getan. Hier werden verschiedene Problemstellungen für digitale Souveränität abstrahiert, zum Beispiel Schlüsseltechnologien für digitale Souveränität oder souveräne Softwareeinführungen. (3) Die allgemeine Lösung einführen und ableiten: Die Ableitung ist zunächst ein Modell, das ein besseres Verständnis der digitalen Souveränität ermöglicht. (4) Ex-

Ante-Bewertung: meint die Befragung von IT-Beratern, ob dieses Modell hilfreich für sie ist. (5) Entwurf einer spezifischen Lösung für ein spezifisches Problem: das wird in dieser Arbeit durch Handlungsempfehlungen für digitale Souveränität auf Basis der Studien dargestellt. (6) Ex-Ante-Bewertung, dieses Mal spezifisch: die Handlungsempfehlungen der Studien werden mit dem Ziel einer Abstraktion der Ergebnisse für ein Referenzmodell bewertet. (7) Spezifische Lösung konstruieren: das Referenzmodell. Und schließlich (8) Ex-Post-Bewertung: die Prüfung, ob das Referenzmodell den ursprünglichen Zweck erfüllt: Leitlinien für Unternehmen zu bieten, um die digitale Souveränität zu stärken (vgl. Tabelle 3.1).

Forschungsaktivitäten	**Reale Welt oder Design-Thinking-Welt?**
1. Das spezifische Problem verstehen	Real
2. Generelles Problem und generelle Anforderungen kreieren	Design Thinking
3. Generelle Lösung intuitiv erfassen und ableiten	Design Thinking
4. Ex Ante Evaluation (generell)	Design Thinking
5. Spezifische Lösung für das spezifische Probelm entwickeln	Design Thinking
6. Ex Ante Evaluation (spezifisch)	Real
7. Spezifische Lösung konstruieren	Real
8. Ex Post Evaluation	Real

Tabelle 3.1: Soft Design Science Methodology (SDSM) Aktivitäten nach Pries-Heje et al. (2014)

SDSM eignet sich besonders gut für die Entwicklung von Referenzmodellen in der Wirtschaftsinformatik, wenn es um komplexe sozio-technische Systeme geht, also um Systeme, bei denen Menschen, Organisationen und Technologien gleichermaßen berücksichtigt werden müssen (Baskerville et al., 2009). Da es sich in dieser Arbeit um eine komplexe Problemstellung handelt, die in vielen Bereichen Anwendung findet, lässt sich dieses Problem allein technisch nicht lösen. Es bedarf einer Integration von sozialen, organisatorischen sowie technischen Aspekten. SDSM ermöglicht die Inklusion von Stakeholdern, die Berücksichtigung von Kontexten sowie eine interpretationsabhängige Artefaktentwicklung (Baskerville et al., 2018). Mit SDSM ist es zudem möglich, ein Referenzmodell partizipativ schrittweise mit Experten zu verfeinern und es frühzeitig in der Praxis zu evaluieren.

In dieser Dissertationsschrift wird ein Referenzmodell für digitale Souverä-

nität in Unternehmen entwickelt. Es werden Experten eingebunden, Projekte analysiert und Artefaktversionen iterativ weiterentwickelt sowie die Ergebnisse theoretisch eingebettet. SDSM wird demnach gebraucht, weil in dieser Arbeit die Vereinbarkeit von Praxisnähe und Wissenschaftlichkeit eine große Rolle spielt, die Methode sich für konzeptionelle Referenzmodelle besonders gut eignet und sie offene, komplexe Forschungsfelder strukturiert bearbeitbar macht.

3.1.2 Design Science Research

Design Science Research ist ein Forschungsparadigma, mit dessen Hilfe Artefakte entwickelt und evaluiert werden können (Gregor & Hevner, 2013). Der Ansatz geht davon aus, dass mit der Gestaltung eines Artefakts ein praktisches Problem gelöst und gleichzeitig ein Beitrag zur Wissenschaft geleistet werden kann. Hevner et al. (2004) etablierte und systematisierte die Design Science Research Methode (vgl. Abbildung 3.1).

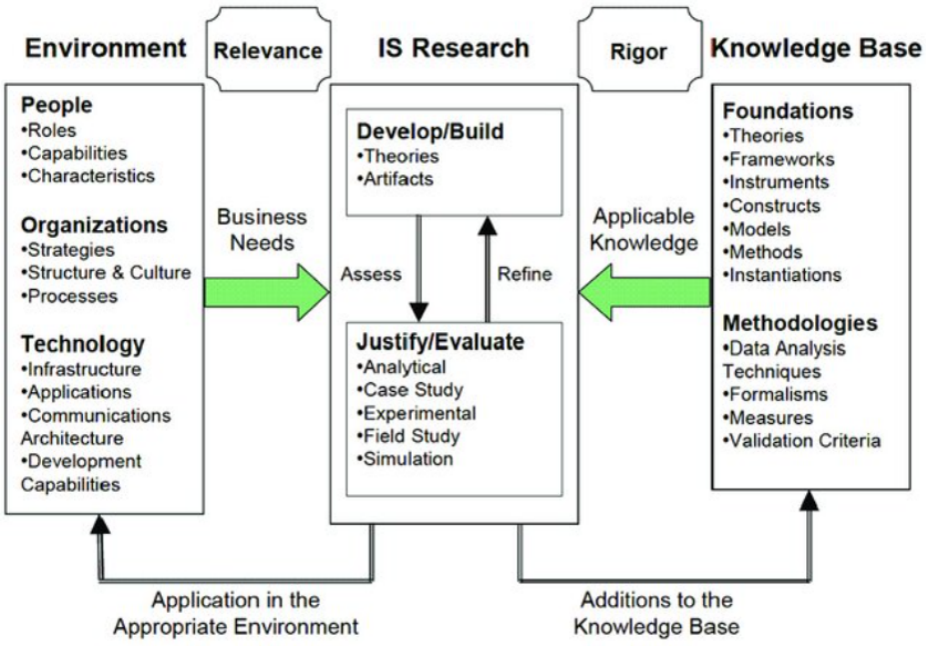


Abbildung 3.1: Design Science Research Methode nach Hevner et al. (2004) als methodischer Rahmen für das Referenzmodell

Hevner et al. (2004) unterscheidet zwischen gestaltender und erklärender Forschung. Im Mittelpunkt steht die Entwicklung von Artefakten (z.B. Mo-

delle, Konstrukte, Methoden), die eine gestaltungsorientierte Lösung für ein reales Problem darstellen. Die Anwendbarkeit und der Nutzen des Artefakts wird vor dem Hintergrund wissenschaftlicher Ansätze (z.B. Fallstudien, Feldstudien, Experimenten) evaluiert und angepasst. Ein zentrales Kennzeichen der Design Science Research sind *Relevanz* und *Rigor* (vgl. Abbildung 3.1). Relevanz beschreibt, dass die Forschungsergebnisse eine Lösung anbieten, die für die Umwelt (z.B. Menschen, Organisationen, Technologien) wertvoll ist. Rigor bedeutet, dass eine wissenschaftliche Strenge bei der Entwicklung von Artefakten einzuhalten ist (z.B. theoretische und methodische Fundiertheit).

Design Science Research ist besonders geeignet, um Referenzmodelle zu entwickeln, da es nicht nur theoretisches Wissen, sondern auch praktische Erkenntnisse einbindet. Dadurch leistet der Ansatz einen Brückenschlag zwischen Wissenschaft und Praxis, was ihn für anwendungsorientierte Forschungsfragen, wie hier im Kontext digitaler Souveränität, besonders relevant macht.

4

Analysen und Modelliterationen

Nach Design Science Research kann es verschiedene Modellversionen als Stufen der Entwicklung eines Artefakts geben (Hevner et al., 2004). So liefert jede Studie in diesem Kapitel (vgl. Kapitel 4) eine Modelliteration als Beitrag zum Gestaltungsprozess des Referenzmodells in Kapitel 6. Erweiternd zu Kapitel 4 werden in Kapitel 5 zusätzliche Einzelstudien vorgestellt, die einen empirischen Beitrag liefern, um digitale Souveränität konkreter erfassen zu können. Durch die Einbindung der Ergebnisse aus Kapitel 5 in einen größeren Designprozess können die Ergebnisse aus Kapitel 4 analysiert, evaluiert und anschließend die Aussagekraft des Referenzmodells gefestigt werden. So entsteht Schritt für Schritt ein Raster der empirischen Wirklichkeit von digitaler Souveränität.

In der ersten Studie wurde zunächst ein Modell für digitale Souveränität entwickelt, das Aufschluss über das Verständnis in Forschung und Praxis über digitale Souveränität gibt. In der zweiten Studie wird dieses erste Modell als Ausgangspunkt verwendet, um es auf Basis eines anderen Szenarios weiterzuentwickeln. In der dritten Studie wird schließlich das zweite Modell weiterentwickelt, indem auch andere Anwendungsdomänen in den Gestaltungs-

prozess einfließen. Das heißt, in diesem Kapitel finden sich Analyseergebnisse auf Basis von drei Fallstudien wieder. Es werden drei Modelliterationen vorgestellt: die erste Version ist DISO-B, ein Modell für digitale Souveränität aus Perspektive der IT-Beratung (B=Beratung), die zweite Version ist DISO-L, hier wird der Fall der Landesverteidigung (L=Landesverteidigung) angenommen. Und schließlich die dritte Modellversion: diese ist DISO-A (A=Academia), hier wurden Professoren zu digitaler Souveränität befragt. Das Akronym DISO ergibt sich aus „**Di**gitale **S**ouveränitätsmodell-**O**ptimierung".

Die drei Fallstudien mit den drei Modellversionen (DISO-B, DISO-L, DISO-A) verfolgen alle dasselbe Ziel: ein besseres Verständnis darüber zu erlangen, was digitale Souveränität aus Unternehmensperspektive bedeutet (siehe Forschungsfrage 1) und zu verstehen, wie man diese erreichen kann (siehe Forschungsfrage 2).

Wie auch bei anderen iterativen Vorgehensweisen (z.B. agile Entwicklung (Abrahamsson et al., 2017) oder der Delphi-Methode (Häder & Häder, 2000)) besteht die Grundidee der vorliegenden Studien darin, die Modellentwicklung durch Rückmeldung aus der Praxis abzusichern. Zu diesem Zweck erfolgt in jeder Iteration ein Austausch mit Experten, um ihre Erfahrung in den Entwicklungsprozess einzubringen. Durch die Rückmeldung der Experten und den Fortschritt der Modellentwicklung verschieben sich dabei die Inhalte des Austauschs. Darüber hinaus ergeben sich auch Schwerpunktsetzungen, die ab Kapitel 5 als „Werkzeuge digitaler Souveränität“ besprochen werden. Generell erfolgt die Einbindung der Experten nach dem Schema problemzentrierter Interviews von Witzel und Reiter (2022). Dabei ist zu beachten, dass der Standardisierungsgrad im Verlauf der Entwicklung abnimmt. So ist zum Anfang noch die Verwendung von Fragebögen möglich. Im späteren Verlauf werden hingegen semistrukturierte Interviewleitfäden und Whiteboards auf Online-Kollaborationsplattformen verwendet, um visuelle Zusammenarbeit mit den Experten zu ermöglichen. Die befragten Experten, die Art der Rekrutierung und die gestellten Fragen in den Interviewreihen werden in den folgenden Kapiteln vorgestellt. Die genauen Interviewten, die Art der Rekrutierung und die gestellten Fragen können ebenfalls den folgenden Kapiteln entnommen werden. Das gesammelte Datenmaterial umfasst Fragebögen, Leitfäden und

Vorlagen. 136 Seiten Text ergeben sich nach Transkription.

Abbildung 4.1 zeigt den Analyseprozess für die folgenden drei Interviewstudien. Die einzelnen Fallstudieninterviewergebnisse werden zunächst in die Software-Anwendung MAXQDA überführt, um sie im Anschluss einer Kodierung zu unterziehen. Ähnliche Aussagen werden in offenen Codes zusammengefasst. Ein offener Code kann demnach eben ein Zitat eines Interviewten sein, oder eine Aggregation verschiedenster Aussagen. Darüber hinaus werden ähnliche Antworten in einem Cluster zusammengefasst. Unter einem Clustering ist in dieser Arbeit eine Zusammenführung ähnlicher Themen aus den Interviews zu einem Themenblock gemeint. So konnten N=29 Themencluster, n=3 Oberthemen zugeordnet werden (siehe Fallstudie 1, Abbildung 4.1). In der darauffolgenden Fallstudie sind die Oberthemen, Themencluster und Gewichtungen aus dem DISO-A-Modell überprüft worden, und in der dritten Fallstudie wurden erneut die Themencluster auf Basis einer anderen Befragungsgruppe geprüft.

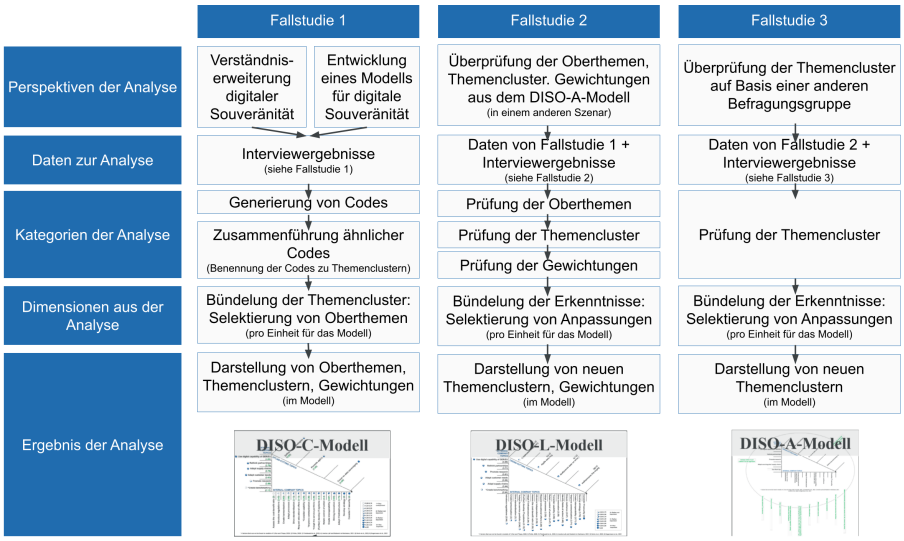


Abbildung 4.1: Analyseprozess für die ersten drei Fallstudien

Somit werden in den folgenden Kapiteln neue Perspektiven aus der Praxis fortlaufend vorgestellt und mit dem aktuellen Stand der Forschung zur digitalen Souveränität abgeglichen, um ein theoriegeleitetes Verständnis digitaler Souveränität erweitern zu können und eine realitätsnahe Entwicklung eines Modells zu ermöglichen.

4.1 Erste Fallstudie: Interviewstudie zu Faktoren digitaler Souveränität aus Perspektive der IT-Beratung (Friedensfall)

Teile dieses Kapitels wurden in einer ersten Version hier publiziert: *Klare, M., and Lechner, U. (2023). Digital Sovereignty from the Perspective of IT Consultancy in Germany: A Model. ICSOB Companion, 1–14. https://ceur-ws.org/Vol-3621/poster-paper5.pdf*

4.1.1 Einleitung

Deutsche Beratungsunternehmen beraten Unternehmen zunehmend in Sachen digitaler Souveränität (Scholze et al., 2023; Wirnsperger et al., 2021). Rothmann (2016) hat festgestellt, dass Beratungsunternehmen sich in der Verantwortung sehen, kritische Informationen von Unternehmen zu schützen. Wirnsperger et al. (2021) sieht die Verantwortung der Beratung in der Unterstützung einer schnelleren Digitalisierung im deutschen öffentlichen Sektor und Scholze et al. (2023) beobachtet, dass die IT-Beratung einen Beitrag leisten kann, um Unternehmen vor zu starken Abhängigkeiten von Techgiganten zu schützen. Es stellt sich die Frage, was digitale Souveränität eigentlich aus Sicht der IT-Beratung bedeutet, was sie alles umfasst und welche Bereiche digitaler Souveränität für IT-Beratungsunternehmen besonders wichtig sind. Es zeigt sich, dass sich IT-Berater bereits mit dem Konzept der digitalen Souveränität auseinandersetzen (Rothmann, 2016). Die IT-Beratung kann einen wesentlichen Beitrag leisten, weil sie Unternehmen bei der Einführung und Umsetzung von IT-Strategien beraten und so Einblicke in Herausforderungen bei der Umsetzung digitaler Souveränität liefern können (Zillmann, 2021).

Es werden die folgenden Forschungsfragen adressiert:

- Was ist das Verständnis digitaler Souveränität der IT-Beratung?
- Welche Faktoren sollten Unternehmen auf der Grundlage von Best Practices von IT-Beratern bei der Stärkung ihrer digitalen Souveränität berücksichtigen?
- Wie sieht ein konkretes Modell mit gewichteten Faktoren für digitale Souveränität aus Perspektive der IT-Beratung aus?

Ziel der ersten Fallstudie ist es demnach ein Modell für die Stärkung digitaler Souveränität aus der Perspektive der IT-Beratung vorzuschlagen, das als Vokabular für Unternehmen dienen kann, die sich mit diesem Thema auseinandersetzen. Das Modell enthält Faktoren, die aus Sicht der IT-Beratung wichtig sind, um digitale Souveränität zu stärken.

Die Ergebnisse aus Experteninterviews (N=22) mit IT-Beratern und eine systematische Literaturrercherche zu digitaler Souveränität mit einer detaillierten Analyse von N=78 Publikationen fließen in ein Modell ein. Die Faktoren im Rahmen des Modells ergeben sich aus Clustern, die auf Basis einer qualitativen Inhaltsanalyse aus den Experteninterviews extrahiert werden. Das Modell wird zudem kritisch vor dem Hintergrund der Literatur zum Thema digitale Souveränität (Jahre: 2014 bis 2022) reflektiert.

Die erste Fallstudie ist unterteilt in folgende Unterkapitel: 1) Einleitung, 2) Vorstellung des Forschungsdesigns, 3) Ergebnisse aus der erste Fallstudie, 4) Zusammenfassung, Limitationen, Ausblick.

4.1.2 Forschungsdesign

Das Forschungsdesign für dieses Kapitel ist der folgenden Abbildung 4.2 zu entnehmen.

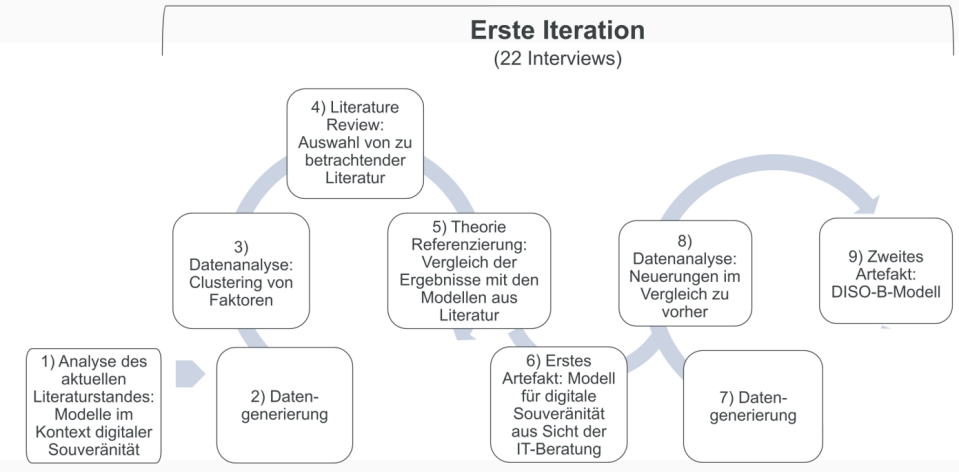


Abbildung 4.2: Forschungsdesign im Rahmen der ersten Fallstudie

Zunächst wurde eine systematische Literaturrecherche nach Brocke et al. (2009) durchgeführt. Diese unterliegt dem Ziel, einen Überblick darüber zu

erhalten, welche Modelle es im Kontext des Themenkomplexes digitaler Souveränität bereits gibt und zu entschlüsselt, mit welcher Zielsetzung diese Modelle erstellt wurden. Verschiedene Datenbanken wie Google Scholar, UniBw, AIS eLibrary, die Homepages der Big Fours und der BWI werden durchsucht. Durch diese Auswahl der Datenbanken soll gewährleistet werden, dass ein breites Bild über digitale Souveränität entsteht. Die Bereiche Wirtschaftsinformatik, Informatik, Innovationsmanagement, Rechtswissenschaft, Sozialwissenschaft, Politik und Philosophie werden in die Literaturübersicht aufgenommen und im Anschluss analysiert. Im ersten Schritt wird die Suche auf die Jahre 2014 bis 2022 begrenzt. Die Auswahl des Betrachtungsrahmens scheint schlüssig, da sie Aktualität bei der Debatte sicherstellt, gleichzeitig aber die Entwicklungen bei der Entstehung des Konzepts digitaler Souveränität nicht außen vor lässt. Dann folgt eine elektronische Volltextsuche nach den Stichwörtern *Digital Sovereignty* und *Digitale Souveränität*. Im Anschluss sind nur diejenigen Publikationen aufgenommen worden, die auch die Begriffe *Digital Sovereignty* oder *Digitale Souveränität* im Titel tragen. Im nächsten Schritt wird als Ausschlusskriterium festgelegt, dass nur diejenigen Publikationen aufgenommen werden, die 1) bei digitaler Souveränität von einem europäischen Konzept ausgehen und 2) Handlungsempfehlungen für das Konzept digitaler Souveränität liefern. Analysegegenstand sind Veröffentlichungen, wobei insbesondere die Anteile theoretisches Verständnis, Definitionen, Grundlagen und der Abschnitt Ergebnisse analysiert werden. Das führt zu 78 identifizierten Artikeln. Im letzten Schritt erfolgt die Eingrenzung der Literaturauswahl auf diejenigen Publikationen, die ausschließlich Modelle digitaler Souveränität liefern. Das führt zu N=6 Artikeln.

Um Einblick in die Erfahrungen der IT-Berater zu erhalten, wird auf eine Interviewstudie zurückgegriffen. Ein Fragebogen dient als Leitfaden für die Interviews (siehe Anhang). Die IT-Berater werden aus dem Netzwerk der BWI akquiriert und halbstrukturierte Interviews werden durchgeführt. Nach der Datengenerierung folgt die Analyse der Daten, die sich an die qualitative Inhaltsanalyse nach Mayring und Brunner (2007) anlehnt. Ähnliche Antworten der Interviewten können in Clustern zusammengefasst und so in dieser Arbeit kommuniziert werden.

Die Ergebnisse werden vor dem Hintergrund der Literatur kritisch reflek-

tiert und mit der gewonnenen Übersicht an Modellen digitaler Souveränität verglichen. Aus diesem Reflexionsprozess geht die Entscheidung, sich an das Modell von Pohle (2020) anzulehnen, hervor. Eine ihrer Dimensionen aus dem Modell wurde um die hier vorliegenden Ergebnisse erweitert: die wirtschaftliche Dimension. Andere Modelle, wie die von Friedewald et al. (2022) oder Kar und Thapa (2020), wurden nicht ausgewählt, da sie eine weniger starke Ausrichtung auf Unternehmen haben.

Schließlich wird ein neues Modell vorgeschlagen, das neue Erkenntnisse aus Experteninterviews mit IT-Beratern in die Debatte rund um digitale Souveränität für Unternehmen inkludiert: das DISO-Modell (digitale Souveränitätsmodell-Optimierung).

Zur Evaluation der Ergebnisse dient eine zweite Interviewstudie mit IT-Beratern. Hierbei konfrontiert man die Interviewten mit dem neuen DISO-Modell. Sie hatten die Möglichkeit, die Sinnhaftigkeit der Cluster in Frage zu stellen, Anpassungswünsche zu äußern und die Cluster zu gewichten, um diese in eine sinnvolle Reihenfolge zu bringen.

Die Erkenntnisse aus der Evaluation werden in einer erneuten Modelliteration eingearbeitet und schließlich wird das DISO-C-Modell vorgestellt: digitale Souveränitätsmodell-Optimierung durch kompetente Beratung. Die Entwicklung dieses Modells erfolgte somit durch ein systematisches Literatur-Review und empirische Validierung (zwei Interviewstudien). Insgesamt wurden 22 IT-Berater befragt (siehe Tabelle 4.1).

4.1.3 Ergebnisse

4.1.3.1 Analyseergebnisse auf Basis einer systematischen Literaturrecherche

Die detaillierte Übersicht über die Literatur, die aus der systematischen Literaturrecherche hervorgeht, kann dem Anhang entnommen werden (vgl. Tabelle 1 bis 13). Die Tabellen zeigen neben Jahr, Autor und Titel der Publikation auch eine Zuordnung zur staatlichen, unternehmerischen oder individuellen Dimension digitaler Souveränität. Außerdem liefert eine Kurzzusammenfassung einen Einblick über den Inhalt der Publikation. Aus der systematischen Literaturrecherche wird eine Forschungslücke deutlich: es geht hervor, dass

Interviewte	Expertise	Länge des Interviews (Stunden:Minuten:Sekunden)
IT-Berater 1	Innovation Management	Pre-Test ohne Aufnahme
IT-Berater 2	Digital Battle Management	00:27:55
IT-Berater 3	Cyber Information Security	00:39:39
IT-Berater 4	Data & Digital Intelligence	00:34:58
IT-Berater 5	Digital Strategy	00:46:01
IT-Berater 6	IT-Architecture & Design	01:01:27
IT-Berater 7	Strategic Process Advisory	01:02:53
IT-Berater 8	Automation Engineering	00:57:48
IT-Berater 9	Change Management	01:31:03
IT-Berater 10	Communication & Marketing	00:47:25
IT-Berater 11	Public Sector Consulting	01:34:36
IT-Berater 12	IT Project Management	01:00:40
IT-Berater 13	Organisational Development	00:57:53
IT-Berater 14	Project Management Office	00:56:38
IT-Berater 15	Geo IT-Consulting	01:03:55
IT-Berater 16	Enterprise Service Management Processes	00:54:20
IT-Berater 17	Data Analytics & Data Science	01:04:46
IT-Berater 18	Product Owning in Software Engineering Projects	01:12:00
IT-Berater 19	Cyber Defense & Data Protection	01:35:09
IT-Berater 20	Strategic Digital Transformation	01:05:16
IT-Berater 21	Defense & Digital Battlefield	00:52:04
IT-Berater 22	Solution Delivery Management	01:15:38
		17:53:50

Tabelle 4.1: Übersicht der Befragten in der ersten Fallstudie

Forschung aus der Perspektive der IT-Beratung zur digitalen Souveränität unterrepräsentiert ist. Die IT-Beratung kann jedoch einen wesentlichen Beitrag zur Debatte leisten, da sich IT-Berater bereits mit dem Konzept der digitalen Souveränität auseinandersetzen (Scholze et al., 2023; Wirnsperger et al., 2021). Sie können Einblick zu Möglichkeiten der Umsetzung, aber auch Herausforderungen von Unternehmen geben.

Unterschiedliche Verständnisse digitaler Souveränität

Es ist ersichtlich, dass die Empfehlungen, wie man digitale Souveränität erreichen sollte, sehr unterschiedlich sind (vgl. Tabelle 1 bis 13). Während Pohle und Thiel (2021) sehr stark politisch ausgerichtete Empfehlungen geben (z.B. Wirtschaftsförderung oder verbraucherpolitischer Schutz), setzt Dreo et al. (2020) eher auf die Stärkung der europäischen Resilienz durch Schlüs-

seltechnologien (z.B. Quantum Computing). Dies scheint auf die teilweise sehr unterschiedlichen Verständnisse digitaler Souveränität zurückzuführen zu sein. Einerseits sieht es die Fokusgruppe (2019) für digitale Souveränität als notwendig an, digitale Souveränitätsforderungen stärker in die Politik, Verwaltung, Wirtschaft, Wissenschaft und Forschung einzuführen. Andererseits bringt Fox (2018) das Kompetenzverständnis über digitale Medien als Teilbereich digitaler Souveränität ein. Schauf et al. (2019) verknüpfen digitale Souveränität mit einem Wettbewerbsverständnis und fordern einen neuen Marktrahmen für Technologien. Das Analyseergebnis wird bestätigt durch Couture und Toupin (2019), die ebenfalls divergente Konzeptualisierungen digitaler Souveränität in ihrem Beitrag deutlich macht.

Die Publikationen, die aus der Datenbank der UniBw München resultieren, zeigen wie breit digitale Souveränität verstanden werden kann. Glasze et al. (2022) diskutieren das Konzept auf rechtlicher, politischer, wirtschaftlicher, technischer sowie auf ethischer Ebene. Peuker (2020) will digitale Souveränität eher als verfassungsrechtliches Leitbild verstehen, das staatliche Infrastrukturverantwortung beinhält. Für Piétron (2019) handelt es sich um ein technisches Problem, das durch Interoperabilität gelöst werden kann.

Bei genauerer Betrachtung von Forschungsbeiträgen aus Tabelle 12 stellt man fest, dass ein großer Anteil der Beiträge aus der Wirtschaftsinformatik einen starken Fokus auf das Thema Datensouveränität haben. Datensouvueränität ist ein wesentlicher Teilbereich digitaler Souveränität. Bei der Gewinnung von mehr Datensouveränität geht es um die Annahme, dass rechtliche Regelungen aktuell nicht ausreichen, um eine selbstbestimmte Kontrolle über die Verarbeitung, Speicherung und Nutzung von Daten zu erreichen (Hummel et al., 2021).

Aus Tabelle 13 geht hervor, dass deloitte als Beratungshaus Beratungskonzepte mit konkreten Digitalisierungsinitiativen für die EU empfiehlt (Wirnsperger et al., 2021). Wirnsperger et al. (2021) entgegnet der Perspektive von Hummel et al. (2021) mit der Notwendigkeit, die EU für das nächste digitale Zeitalter bereit machen zu müssen (vgl. Tabelle 13).

4.1.3.2 Ergebnisse aus den Experteninterviews mit IT-Beratern (erste Interviewreihe)

Digitale Souveränität auch für die IT-Beratung eine Worthülse

Die IT-Berater sollten als erstes äußern, was sie unter digitaler Souveränität verstehen. Ein Zitat: „Durch die Ausweitung des Leistungsportfolios und der Erweiterung des Spektrums erzeugt man [für mich] eine Steigerung der digitalen Souveränität". Ein anderer IT-Berater teilt: „Grundsätzlich ist digitale Souveränität für mich stark damit verbunden, wie ich möglichst sinnvoll, effektiv und effizient mit Abhängigkeiten umgehen kann", und: „Ich verstehe unter digitaler Souveränität Möglichkeiten oder Fähigkeiten, selbstständig und resilient auf aktuelle Gegebenheiten in der IT-Welt einzugehen". An dieser Stelle wird genau wie in der systematischen Literaturrecherche deutlich, dass das Verständnis des Begriffs digitale Souveränität sich unterscheidet. Während ein Großteil der IT-Berater der Meinung sind, dass Unternehmen versuchen sollten, mehr Kontrolle über ihre Handlungen zu erlangen, um digitale Souveränität zu erreichen, ist die Hälfte der IT-Berater überzeugt, dass eher das Thema Unabhängigkeit wesentlich ist. Eine zu starke Form der Unabhängigkeit kann jedoch zu weniger Handlungskontrolle führen und das würde zu einem Spannungsverhältnis dieser beiden Konzepte (Handlungskontrolle vs. digitale Souveränität) führen.

Erfahrungen aus der Vergangenheit: Was kann man tun, um digitale Souveränität zu erreichen?

Dann wurden die IT-Berater gefragt, was sie in der Vergangenheit getan haben, um Unternehmen bei der Stärkung von digitaler Souveränität zu unterstützen.

Die IT-Berater bezeichnen die Entwicklung einer Strategie als entscheidend, um Abhängigkeiten im digitalen Raum zu reduzieren. Außerdem wird die Definition von Handlungsfeldern, in denen eine stärkere Form der Unabhängigkeit gewünscht ist, als hilfreich erachtet, um das Thema digitale Souveränität greifbarer zu machen. Es wird deutlich, dass bei den Handlungsempfehlungen der Fokus der IT-Berater stark auf dem Thema Unabhängigkeit liegt, auch wenn mehr IT-Berater das Konzept der Kontrolle in ihrem Verständnis in den Vordergrund gerückt haben. Die IT-Berater berichten, dass einige Unternehmen bereits ihre Eigenentwicklungen vorangetrieben haben, ihre IT-Infrastruktur und

ihr Service-Portfolio angepasst haben, um sich digital souveräner aufzustellen.

Im Rahmen der Experteninterviews wurde zudem deutlich, dass digitale Souveränität vor dem Hintergrund von Funktionsfähigkeit diskutiert werden muss. Interoperabilität zwischen den IT-Systemen ist wichtig, um ein nahtloses Zusammenspiel zwischen unterschiedlichen Systemen zu gewährleisten. Zudem ist die Harmonisierung von IT-Landschaften bei Kunden ein aktuell wesentliches Thema, um Tools zu vereinheitlichen oder auch die Daten- und Prozessharmonisierung voranzutreiben, um Effizienzen zu heben.

Die IT-Berater sagen zudem, dass die Verbesserung von unternehmensinterner Kommunikation und die Schaffung von Bildungsangeboten wesentlich ist, um Souveränität in Unternehmen voranzutreiben. Sie teilen mit, dass sie bereit wären, Kooperationen mit anderen Unternehmen für entsprechende Bildungsangebote einzugehen. Ebenso äußern sich alle IT-Berater zum Thema Kosten-Nutzen-Verhältnis. Hier sind die Meinungen kontrovers. Während einige der IT-Berater sagen, dass es notwendig ist, Kosten gegenüber Nutzen abzuwägen, verweisen andere IT-Berater darauf, dass mehr Sicherheit zwangsläufig mit höheren Kosten einhergeht. Das primäre Ziel scheint nach Meinung aller IT-Berater jedoch die Gewährleistung von mehr Sicherheit zu sein.

Darüber hinaus weisen die IT-Berater darauf hin, dass Unternehmen nicht vergessen sollten, Innovationen voranzutreiben, um nicht vom Markt zu verschwinden. Sie fordern die Schaffung innovationsfreudiger Rahmenbedingungen (z.B. Förderung potenzieller Innovationsfelder). Aus den Interviews ergibt sich weiter, dass alle IT-Berater die Anpassung der Lieferketten und das Überdenken von Partnerschaften innerhalb der Lieferkette für wichtig halten.

Empfehlungen für die Zukunft: was tun, um digitale Souveränität in Unternehmen voranzutreiben?

Die IT-Berater wurden als nächstes gefragt, was sich verändern muss, um digitale Souveränität stärker treiben zu können.

Sie schätzen, dass eine stärkere Fokussierung auf Schulungen und den Kunden bei dem Thema notwendig ist. Schaffung regulierender Rahmenbedingungen (z.B. festgelegte Standortmöglichkeiten für unternehmensinterne Rechenzentren) und mehr Regulierungen innerhalb der Unternehmen (z.B. stärkere Regeln zur Wahrung der Privatsphäre im Cyberspace) sind zwei

konkrete Maßnahmen. Weitere Faktoren, die zur Stärkung der digitalen Souveränität genannt wurden, sind die Schaffung von Benchmarking, die Förderung von Forschung und die Stärkung der digitalen Fähigkeiten in Deutschland und der EU. Schließlich wurden noch einige übergreifende Themen genannt: Dazu gehören Resilienz, Nachhaltigkeit, Schlüsseltechnologien und Datensouveränität. Zwei weitere Faktoren, die aber am seltensten genannt wurden, sind einerseits die Berücksichtigung von Benutzerfreundlichkeit bei den Systemen und die Förderung von Agilität in Projekten.

4.1.3.3 Clustering der Ergebnisse aus Experteninterviews

Ähnliche Antworten werden nun in einem Cluster zusammengefasst.

Die folgenden Ausführungen gehen näher darauf ein, welche Themen in einem Themencluster zusammengeführt wurden (siehe 1. Clustering).

Im Anschluss folgt eine Referenzierung zur Forschungsfrage. Ziel ist es, ein Modell für digitale Souveränität für Unternehmen zu entwickeln. Demnach wird reflektiert, welche der ermittelten Themencluster Unternehmen beeinflussen können. In diesem Zuge werden die Oberthemen selektiert. Ein Oberthema ist *unternehmensinterne Themen*, eines *unternehmensexterne Themen*.

1. Clustering

Die Tabellen 4.2 und 4.3 zeigen, welche Fragen konkret im Fragebogen aufgeführt waren. Dabei stellen die Tabellen exemplarisch die Antworten eines IT-Beraters dar. Die Art der Zuordnung ist bei allen anderen IT-Beratern (N=21) genau in der gleichen Form durchgeführt worden. Nach Mayring und Brunner (2007) wurden die Antworten aller IT-Berater hinsichtlich der Frage analysiert, was die IT-Berater unter digitaler Souveränität verstehen. Ziel ist es also, Faktoren digitaler Souveränität aus Sicht der IT-Beratung aus den Interviewergebnissen zu extrahieren. Hierzu wurden die Antworten codiert, wenn nötig paraphrasiert und Kategorien gebildet. Die Paraphrasen und Kategorien sind dann auf eine höhere Abstraktionsebene zusammengefasst worden, indem spezifische Aussagen oder Paraphrasen verdichtet und interpretiert wurde, welche Clusterbezeichnung die Verdichtung am ehesten umschreibt.

Diese Art des Clusterings liefert folgende 29 Cluster.

Themencluster 1: Lieferketten. Um mehr digitale Souveränität zu erreichen,

ID	Experte	Auseinandersetzung mit dem Thema	Themenbereich	Frage	Filterfragen	Themenblock 1: Lieferketten	Themenblock 2: Schlüsseltechnologien	Themenblock 3: IT-Sicherheit	Themenblock 4: IT-Infrastruktur	Themenblock 5: IT-Systeme	Themenblock 6: Innovation	Themenblock 7: Partnerschaft	Themenblock 8: Regularien	Themenblock 9: Forschung	Themenblock 10: Harmonisierung	Themenblock 11: Datensouveränität	Themenblock 12: Strategie	Themenblock 13: Kunden	Themenblock 14: Resilienz	Themenblock 15: Nachhaltigkeit	Themenblock 16: Prozesse	Themenblock 17: Bildung	Themenblock 18: Kommunikation	Themenblock 19: Interoperabilität	Themenblock 20: Handlungskontrolle	Themenblock 21: Kostennutzen
1	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Wie verstehen Sie den Terminus „digitale Souveränität" aus der Eigentümerstrategie der BWI?		x	xx	x	x	x		x														
2	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Was hat ihr Unternehmen in der Vergangenheit bereits getan, um digital souveräner zu werden?				x		x	x			x										x		
3	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Was wird ihr Unternehmen in Zukunft noch tun, um sich digital souveräner aufzustellen?				x	x	x	x		x	x										x		x
4	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Wie gut sind ihre Mandanten derzeit im Eigenbetrieb in folgenden Themen aufgestellt?			x	x		x						x										
5	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Welche der in Punkt 5 genannten Punkte empfinden Sie am wichtigsten zur Stärkung der digitalen Souveränität?			x		x																	
6	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Gibt es noch weitere als die in Frage 6 genannten Punkte, die Sie als wichtig für die Stärkung digitaler Souveränität der BWI erachten?			x		x			x														
7	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Was muss sich verändern, um digitale Souveränität stärker treiben zu können?			x		x			x														
8	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Inwieweit glauben Sie, dass ihr Unternehmen die eigenen Angebote digital souveräner gestalten sollte?																						
9	1	Regelmäßig	Digitale Souveränität aus Sicht des	Wie könnte man ihrer Meinung nach die Souveränität von Angeboten (z.B. Software) stärken?				xx	x						x		x									
10	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Inwieweit glauben Sie, dass die Effizienz (Kosten-Nutzen-Verhältnis) der BWI durch die Auseinandersetzung mit dem Thema digitale Souveränität leiden könnte?	Sehr																						
11	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Welche Schwerpunkte muss man in der IT-Beratung legen, um digital souverän zu sein?														x								
12	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Welche (Beratungs-)Unternehmen würden sie einem hohen Grad an digitaler Souveränität zuschreiben und warum?	Kein anderes Unternehmen.																					
13	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Welche (Beratungs-)Unternehmen beraten Ihrer Meinung nach digital souverän?	/																					
14	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	In welchen Fällen würden Sie Kooperationen mit anderen Unternehmen in Erwägung ziehen, um ihre digitale Souveränität zu erhöhen?			x			x		x				x						x			x	
15	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	In welchen der folgenden Fälle könnte Ihrer Meinung nach die IT-Beratung besonders gut unterstützen?		sehr		sehr									x		sehr	sehr						
16	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Inwieweit glauben Sie, dass die Einführung von Open-Source-Software bei der Stärkung digitaler Souveränität helfen könnte?			schon eher																			
17	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Wenn Schieberegler auf "ein wenig oder sehr" gesetzt wurde: Glauben Sie, dass die IT-Beratung bei der Einführung von Open-Source-Software unterstützen kann?																						
18	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Würde die IT-Beratung bei der Anpassung folgender Punkte unterstützen?			x	x									x	x			x					
19	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Wie kann das Bewusstsein der Mitarbeiter für das Thema digitale Souveränität in der BWI gestärkt werden?																		xxxx	x			

Tabelle 4.2: Ergebnis des Clustering-Verfahrens nach Mayring und Brunner (2007) (I/II)

ID	Experte	Auseinandersetzung mit dem Thema	Themenbereich	Frage	Filterfragen	Themenblock 22: Benutzerfreundlichkeit	Themenblock 23: Standardisierung	Themenblock 24: Service-Portfolio	Themenblock 25: Handlungsfelder	Themenblock 26: Fähigkeiten EU/ Deutschlands	Themenblock 27: Benchmarking	Themenblock 28: Unabhängigkeit	Themenblock 29: Agilität
1	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Wie verstehen Sie den Terminus „digitale Souveränität" aus der Eigentümerstrategie der BWI?					x	x			
2	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Was hat ihr Unternehmen in der Vergangenheit bereits getan, um digital souveräner zu werden?				x		x			
3	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Was wird ihr Unternehmen in Zukunft noch tun, um sich digital souveräner aufzustellen?			x	x	x				
4	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Wie gut sind ihre Mandanten derzeit im Eigenbetrieb in folgenden Themen aufgestellt?									
5	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Welche der in Punkt 5 genannten Punkte empfinden Sie am wichtigsten zur Stärkung der digitalen Souveränität?									
6	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Gibt es noch weitere als die in Frage 6 genannten Punkte, die Sie als wichtig für die Stärkung digitaler Souveränität der BWI erachten?		x				x	x	x	x
7	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Was muss sich verändern, um digitale Souveränität stärker treiben zu können?		x			x	x			
8	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Inwieweit glauben Sie, dass ihr Unternehmen die eigenen Angebote digital souveräner gestalten sollte?									
9	1	Regelmäßig	Digitale Souveränität aus Sicht des	Wie könnte man Ihrer Meinung nach die Souveränität von Angeboten (z.B. Software) stärken?		x							
10	1	Regelmäßig	Digitale Souveränität aus Sicht des Interviewten	Inwieweit glauben Sie, dass die Effizienz (Kosten-Nutzen-Verhältnis) der BWI durch die Auseinandersetzung mit dem Thema digitale Souveränität leiden könnte?	Sehr				x				
11	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Welche Schwerpunkte muss man in der IT-Beratung legen, um digital souverän zu sein?					x				
12	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Welche (Beratungs-)Unternehmen würden sie einem hohen Grad an digitaler Souveränität zuschreiben und warum?	Kein anderes Unternehmen.								
13	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Welche (Beratungs-)Unternehmen beraten Ihrer Meinung nach digital souverän?	/								
14	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	In welchen Fällen würden Sie Kooperationen mit anderen Unternehmen in Erwägung ziehen, um ihre digitale Souveränität zu erhöhen?									
15	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	In welchen der folgenden Fälle könnte Ihrer Meinung nach die IT-Beratung besonders gut unterstützen?									
16	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Inwieweit glauben Sie, dass die Einführung von Open-Source-Software bei der Stärkung digitaler Souveränität helfen könnte?									
17	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Wenn Schieberegler auf "ein wenig oder sehr" gesetzt wurde: Glauben Sie, dass die IT-Beratung bei der Einführung von Open-Source-Software unterstützen kann?									
18	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Würde die IT-Beratung bei der Anpassung folgender Punkte unterstützen?									
19	1	Regelmäßig	Digitale Souveränität aus Sicht der IT-Beratung	Wie kann das Bewusstsein der Mitarbeiter für das Thema digitale Souveränität in der BWI gestärkt werden?					x				

Tabelle 4.3: Ergebnis des Clustering-Verfahrens nach Mayring und Brunner (2007) (II/II)

ist es den Daten nach sinnvoll, Lieferkettenmodelle konkret zu analysieren und zu entscheiden, wo man Open-Source einsetzen will, welche Akteure innerhalb der Lieferkette ein potenzielles Risiko darstellen und welche Komponenten und Waren auf anderem Wege (z.B. national) beschafft werden sollten.
Themencluster 2: Schlüsseltechnologien. Für Unternehmen ist es den IT-Beratern nach ratsam, potenzielle neue Technologien (z.B. KI), auf die man setzen will, festzulegen.
Themencluster 3: IT-Sicherheit. Die Gewährleistung von mehr IT-Sicherheit ist nach Meinung der IT-Berater einer der wichtigsten Beweggründe für digitale Souveränität. Unternehmen sollten kritisch reflektieren, wie sie einen besseren Schutz von Informationen sicherstellen können.
Themencluster 4: IT-Infrastruktur. Die IT-Berater fordern eine stärkere Auseinandersetzung mit souveränen IT-Infrastrukturen (Cloud oder Rechenzentrum).
Themencluster 5: IT-Systeme. Das Thema IT-Systeme sollte vor dem Hintergrund der unternehmerischen Beschaffungsstrategie reflektiert werden. Sprich: sind die Komponenten, die Unternehmen benötigen, um die Systeme zu bauen und zu nutzen, souverän genug beschafft? Auch die Entwicklungsstrategie sollte den IT-Beratern nach kritisch reflektiert werden. Also die Frage, ob souverän genug entwickelt wird. Und letztlich die Anpassungsstrategie. Sprich, ist das Unternehmen im Falle einer Krise in der Lage, möglichst souverän Anpassungen vorzunehmen.
Themencluster 6: Innovation. Aus den Experteninterviews geht auch hervor, dass Unternehmen bei der Stärkung digitaler Souveränität nicht vergessen sollten, zu innovieren. Unternehmen sollten ihre Innovationsstrategie vor dem Hintergrund digitaler Souveränität überdenken und prüfen, ob die Ausrichtung der Innovationskampagnen mit den Zielen digitaler Souveränität einhergehen.
Themencluster 7: Partnerschaften. Um den Balance-Akt zwischen weniger Abhängigkeit und gleichzeitig guten, zielführenden Kooperationen zu meistern, sollten Unternehmen den IT-Beratern nach, ausgewählte Partnerschaften eingehen. Unternehmen sollten demnach ausgewählte Kooperationen vor dem Hintergrund von Sicherheit, Resilienz und Zuverlässigkeit kritisch prüfen.
Themencluster 8: Regularien. Die IT-Berater empfehlen die Einführung

unternehmensinterner Regeln für den Umgang mit digitaler Souveränität.
Themencluster 9: Forschung. Zudem wurde deutlich, dass IT-Berater Unternehmen empfehlen, systematische externe Untersuchungen zur Erforschung der digitalen Souveränität durchzuführen.
Themencluster 10: Harmonisierung. Um Funktionsfähigkeit zu gewährleisten, sind den IT-Beratern nach, Prozesse und Anwendungen in Einklang zu bringen.
Themencluster 11: Datensouveränität. Nicht nur in der systematischen Literaturrecherche wird deutlich, dass das Thema Datensouveränität eine zentrale Rolle einnimmt, sondern auch in den Interviews. IT-Berater sprechen sich demnach dafür aus, Vorschriften für den Umgang mit Daten innerhalb von Unternehmen einzuführen, die die Speicherung und Analyse umfassen.
Themencluster 12: Strategie. Als wesentlich aus den Interviews geht die Entwicklung eines Plans für die Ausrichtung der digitalen Souveränität in Unternehmen hervor.
Themencluster 13: Kunden. Es wurde zudem deutlich, dass auch die externe Einflussnahme durch Kunden auf die digitale Souveränität der Unternehmen nicht untergraben werden darf.
Themencluster 14: Resilienz. Unternehmen sollten zusätzlich auch die Fähigkeit, sich schnell von Störungen oder ungeplanten Ereignissen zu erholen, ausbauen.
Themencluster 15: Nachhaltigkeit. Ein weiterer Themenblock ist die nachhaltige Entwicklung. Hier äußern IT-Berater die Nutzung strategischer Instrumente zur Gestaltung eben dieser Entwicklung.
Themencluster 16: Prozesse. Es wird deutlich, dass Handlungsmaßnahmen zur Stärkung der digitalen Souveränität in Unternehmen zu prozessualen Anpassungen führen.
Themencluster 17: Bildung. Eine stärkere Fokussierung auf Schulungen zum Thema digitale Souveränität (z.B. IT-Systeme und Entscheidungsfindung) scheint den IT-Beratern nach entscheidend, um in Zukunft Unternehmen dabei zu unterstützen, dass das Thema nicht nur auf Management-Ebene bleibt, sondern auch zu den Mitarbeitern durchdringt.
Themencluster 18: Kommunikation. Zudem wurde klar, dass ein stärkerer Austausch von Informationen zum Thema digitale Souveränität an Mitarbeiter

und Entscheidungsträger notwendig ist.

Themencluster 19: Interoperabilität. Ein weiteres Thema, das Kunden der IT-Berater aktuell stark beschäftigt und deswegen auch in den Interviews genannt wurde, ist Interoperabilität: hier zu verstehen als die Möglichkeit einer Kommunikation zwischen zwei oder mehreren IT-Systemen.

Themencluster 20: Handlungskontrolle. Die Ergebnisse zeigen, dass digitale Souveränität für die Befragten mit einer stärkeren Kontrolle über Handlungen einhergeht, die es mit der Gestaltung neuer Handlungsmöglichkeiten zu formen gilt.

Themencluster 21: Kosten-Nutzen-Verhältnis. Einige IT-Berater verweisen darauf, dass Unternehmen das Thema digitale Souveränität erst vor dem Hintergrund von Kosten und Nutzen reflektieren sollten.

Themencluster 22: Benutzerfreundlichkeit. Souveräne Anwendungen werden nur genutzt, wenn diese auch einfach in ihrer Anwendung sind. Dies sollte den IT-Beratern nach bei der Ausgestaltung digitaler Souveränität berücksichtigt werden.

Themencluster 23: Standardisierung. Souveräne IT-Systeme erfordern den IT-Beratern nach standardbasierte und kompatible Technologien.

Themencluster 24: Service-Portfolio. Unternehmen sollten dafür sorgen, dass eine vollständige Liste der vorhandenen Anwendungen (IT-Produkte und Dienstleistungen) im Unternehmen existiert und im Sinne digitaler Souveränität prüfen, welche Anwendungen ausgetauscht, angepasst oder beibehalten werden.

Themencluster 25: Handlungsfelder. Identifizierung konkreter Handlungsfelder für digitale Souveränität kann den IT-Beratern zur Folge, Unternehmen dabei helfen, das Thema griffiger zu machen.

Themencluster 26: Fähigkeit Deutschlands und Europas. Die Möglichkeiten der Unternehmen sind abhängig vom Markt und demnach den digitialen Fähigkeiten in Deutschland und Europa. Unternehmen sollten vor diesem Hintergrund kritisch hinterfragen, auf welche nationalen oder europäischen Alternativen sie zurückgreifen können.

Themencluster 27: Benchmarking. Ebenfalls einigen IT-Beratern nach kann es Unternehmen den Einstieg und den Umgang mit dem Thema digitale

Souveränität erleichtern, wenn sie benchmarken, also Einblicke erlangen, wie andere Unternehmen ein höheres Maß an digitaler Souveränität erreicht haben.
Themencluster 28: Unabhängigkeit. Schließlich sollte es das Ziel von Unternehmen sein, mehr Autarkie in ihrem Unternehmen zu erreichen, ohne zu große Abhängigkeiten von Externen.
Themencluster 29: Agilität. Es ist auch im Sinne der IT-Berater, die Fähigkeit von Unternehmen auszubauen, schnell und vorteilhaft auf derartige Veränderungen zu reagieren.

2. Zuordnung der Themencluster zu Oberthemen

In diesem Forschungsschritt wird der Frage nachgegangen, welche der ermittelten Themencluster Unternehmen beeinflussen können.

Der Tabelle 4.4 ist die Bewertung der Themen zu entnehmen. Die Datenanalyse führt zu dem Ergebnis, dass es Themen gibt, die sich eindeutig Unternehmen zuordnen lassen, sprich: Themen, die Unternehmer intern angehen können, so zum Beispiel die Ausrichtung von Prozessen auf digitale Souveränität, die Einführung von Regulierungen im Hinblick auf digitale Souveränität oder die Entwicklung einer Strategie. Diese Cluster sind dem Oberthema *unternehmensinterne Themen* zugeordnet. Darüber hinaus wurden auch unternehmensexterne Themencluster gebildet, unter anderem die digitalen Fähigkeiten in Deutschland und Europa. Sie werden zusammen mit den Themen Partnerschaften, Forschung, Kunden, Lieferketten und Benchmarking dem Oberthema *externe Unternehmensthemen* zugeordnet. Sie können einen direkten oder indirekten Einfluss auf die Ausgestaltung der digitalen Souveränität von Unternehmen haben. Alle anderen Themencluster sind dem Oberthema *Querschnittsthemen* zu entnehmen, zum Beispiel Nachhaltigkeit, Agilität oder Datensouveränität.

4.1.3.4 Literaturauswahl für die Entwicklung des Modells und Analyse der Literatur auf Basis des Clusterings

Wie bereits im Forschungsdesign beschrieben, wird im nächsten Schritt nun die Literaturauswahl aus 4.1.3.1 auf diejenigen Publikationen eingegrenzt, die ausschließlich Modelle digitaler Souveränität liefern. Das führt zu N=6 Modellen aus ebenso vielen Publikationen, die der nachfolgenden Tabelle 4.5 entnommen werden können.

Datenset	Beeinflussbar durch Unternehmen	Indirekte Auswirkungen auf das Handeln von Unternehmen	Starke Leitlinien für Unternehmen	Erklärung	Entscheidung
Strategie	++	+	- -	1. Ein Plan für die Ausrichtung der digitalen Souveränität im Unternehmen	Intern
Handlungsfelder	++	+	- -	1.1 Identifizierung konkreter Maßnahmen zur digitalen Souveränität	Intern
IT-Systeme	++	+	-	2. Entscheidung über eine souveräne IT-Infrastruktur (Cloud oder Rechenzentrum)	Intern
IT-Infrastruktur	++	+	-	3. Beschaffungs-, Entwicklungs- und Anpassungsstrategie für Anwendungen	Intern
Harmonisierung	++	+	+	3.1. Standardbasierte und kompatible Technologien und Anwendungen	Intern
Standardisierung	++	+	+	3.2 Kommunikation zwischen zwei oder mehreren IT-Systemen ist möglich	Intern
Interoperabilität	++	+	+	3.3. Einfache Bedienung einer Anwendung	Intern
Bildung	++		-	4. Austausch von Informationen zum Thema Digitale Souveränität an Mitarbeiter und Entscheidungsträger	Intern
Kosten-Nutzen-Verhältnis	++	+	- -	5. Schulungen zum Thema Digitale Souveränität (z.B. IT-Systeme und Entscheidungsfindung)	Intern
Prozesse	++	+	+	6. Index für das Kosten-Nutzen-Verhältnis eines Projekts im Rahmen einer Kosten-Nutzen-Analyse	Intern
Regulierungen	++	+	+	7. Handlungsmaßnahmen zur Stärkung digitaler Souveränität führen zu prozessualen Anpassungen	Intern
IT-Sicherheit	++	+	+	7.1. Prozesse und Anwendungen in Einklang bringen	Intern
Unabhängigkeit	++	+	- -	8. Einführung interner Regeln für den Umgang mit digitaler Souveränität	Intern
Handlungskontrolle	++	+	- -	9. Informationsschutz vor dem Hintergrund digitaler Souveränitätsanforderungen	Intern
Innovationen	++	+	-	10. Mehr Autarkie im Unternehmen ohne zu große Abhängigkeit von Externen	Intern
Forschung	+	++	+	10.1 Kontrolle der Maßnahmen innerhalb des Unternehmens	Extern
Digitale Fähigkeiten in Deutschland/ EU	+	++	- -	11. Prüfen, ob Innovationsstrategie und Innovationskampagnen mit den Zielen digitaler Souveränität einhergehen	Extern
Partnerschaften	+	++	- -	12. Möglichkeiten systematische externe Untersuchungen zur Erforschung der digitalen Souveränität	Extern
Kunden	+	++	- -	13. Möglichkeiten für Unternehmens, digitale Fähigkeiten aus Deutschland und Europa zu beziehen	Extern
Lieferketten	+	++	+	14. Kooperationen zur Gestaltung der digitalen Souveränität in Unternehmen überdenken	Extern
Resilienz	++	+	+	15. Externe Einflussnahme durch Kunden auf die digitale Souveränität von Unternehmen	Intern
Nachhaltigkeit	+	+	++	16. Lieferkettenmodelle analysieren, und entscheiden, wo Technologien wie Open Source eingesetzt werden, welche Akteure innerhalb der Lieferkette ein potenzielles Risiko darstellen und welche Komponenten und Waren auf anderem Wege (z.B. national) beschafft werden sollten	Querschnitt
Datensouveränität	+	+	++	17. Die Fähigkeit von Unternehmen, sich schnell von Störungen oder ungeplanten Ereignissen zu erholen	Querschnitt
Schlüsseltechnologien	+	+	++	18. Nutzung strategischer Instrumente zur Gestaltung nachhaltiger Entwicklung	Querschnitt
Agilität	+	+	++	19. Vorschriften für Daten, die von Unternehmen gespeichert oder analysiert werden (z. B. GDPR)	Querschnitt
Kommunikation	++	+	- -	20. Festlegung von Schlüsseltechnologien (key enabling technologies = KETs)	Intern
Service Portfolio	++	+	- -	21. Die Fähigkeit von Unternehmens, schnell und vorteilhaft auf Veränderungen zu reagieren	Intern
Benutzerfreundlichkeit	++	+	+	22. Liste der vorhandenen Anwendungen (IT-Produkte und -Dienstleistungen) im Unternehmen vor dem Hintergrund digitaler Souveränitätsbestrebungen anpassen	Intern
Benchmarking	+	++	-	23. Einblicke, wie andere Unternehmen ein höheres Maß an digitaler Souveränität erreicht haben.	Extern

Tabelle 4.4: Bewertung der Faktoren und Entscheidung für die Zuordnung zu einem Cluster

Diese 6 Publikationen werden einem Vergleich unterzogen, mit dem Ziel zu verstehen, welche Faktoren digitaler Souveränität in den Publikationen genannt werden. Zudem wird die Clusterstruktur kritisch überprüft. Von Interesse sind neue Cluster oder die Bestätigung der bereits erarbeiteten Cluster.

Bei der Betrachtung der Publikationen aus Tabelle 4.5 zeigt sich, dass alle Autoren das Thema Strategie aufgreifen (Friedewald et al., 2022; Hartmann, 2021; Herlo et al., 2022; Kagermann, 2021; Kar & Thapa, 2020; Pohle, 2020). Strategie war ein Cluster, das im Rahmen der Analysephase ebenfalls erarbeitet wurde.

Datenset	Kar and Thapa (2020)	Pohle (2020)	Friedewald et al. (2022)	Joecks-Laß and Hadwich in Hartmann (2021)	Herlo et al. (2022)	Kagermann et al. (2021)
Strategie	✓	✓	✓	✓	✓	
Handlungsfelder	✓		✓	✓	✓	✓
IT-Systeme	✓		✓			
IT-Infrastruktur	✓	✓	✓		✓	✓
Harmonisierung			✓			✓
Standardisierung			✓			✓
Interoperabilität	✓	✓	✓		✓	✓
Bildung	✓	✓	✓	✓	✓	✓
Kosten-Nutzen-Verhältnis	✓					
Prozesse	✓	✓	✓		✓	✓
Regulierungen	✓	✓	✓	✓	✓	✓
IT-Sicherheit		✓				
Unabhängigkeit		✓	✓	✓		✓
Handlungskontrolle				✓		
Innovationen	✓	✓	✓		✓	✓
Forschung	✓	✓	✓	✓	✓	✓
Digitale Fähigkeiten in Deutschland/ EU		✓				✓
Partnerschaften		✓		✓	✓	
Kunden		✓		✓		✓
Lieferketten				✓		✓
Resilienz	✓	✓		✓	✓	✓
Nachhaltigkeit		✓	✓	✓	✓	✓
Datensouveränität		✓	✓	✓	✓	✓
Schlüsseltechnologien	✓	✓			✓	✓
Agilität				✓		✓
Kommunikation						
Service Portfolio						
Benutzerfreundlichkeit						
Benchmarking						

Tabelle 4.5: Ergebnis aus dem Vergleich von entwickelten Themenclustern digitaler Souveränität und denen in den Publikationen

5 von 6 Autoren nennen konkrete Handlungsfelder wie Open Data, ML2KMU, strategische Allianzen oder digitale Intelligenz (Friedewald et al., 2022; Hartmann, 2021; Herlo et al., 2022; Kagermann, 2021; Kar & Thapa, 2020).

Darüber hinaus integriert Friedewald et al. (2022) die Entwicklung von IT-Systemen als einen Faktor der digitalen Souveränität in ihr Modell. Kar und Thapa (2020) nehmen die Entwicklung von IT-Systemen nicht in ihr Modell auf, aber sie beziehen sie in ihre weiteren Ausführungen ein. Die Experteninterviews ergaben, dass alle IT-Berater die Anpassung der IT-Infrastrukturen für Unternehmen als wesentlich ansehen. Vergleicht man diese Ergebnisse mit denen aus der Literatur, so zeigt sich, dass hier 5 von 6 Autoren die Anpassung von Infrastrukturen, z.B. kritischen Infrastrukturen, als essentiell einstufen (Friedewald et al., 2022; Herlo et al., 2022; Kagermann, 2021; Kar & Thapa, 2020; Pohle, 2020). Die Befragten führten Harmonisierung, Standardisierung und Interoperabilität als Faktoren ein. 5 von 6 der Autoren nannten ebenfalls Interoperabilität (Friedewald et al., 2022; Herlo et al., 2022; Kagermann, 2021; Kar & Thapa, 2020; Pohle, 2020), aber nur 2 von 6 Harmonisierung und die gleiche Anzahl an Autoren Standardisierung (Friedewald et al., 2022; Kagermann, 2021). Die Ergebnisse zeigen, dass insbesondere die Berücksichtigung von Interoperabiltität bedeutsam im Kontext digitaler Souveränität zu sein scheint. Auch wenn Interoperabilität in der systematischen Literaturrecherche zunächst ein Randthema zu sein schien. In Bezug auf die Bildung sind sich alle Befragten einig: dass es wichtig ist, diese Themen zu behandeln. Dies deckt sich mit der Literatur. Hier betonen alle Autoren den Faktor Bildung (Friedewald et al., 2022; Herlo et al., 2022; Joecks-Laß & Hadwich, 2021; Kagermann, 2021; Kar & Thapa, 2020; Pohle, 2020). Einer von 6 der Autoren erwähnt das Kosten-Nutzen-Verhältnis (Kar & Thapa, 2020) und alle außer Joecks-Laß und Hadwich (2021) das Thema Prozessanpassung. Es fällt jedoch auf, dass keiner der Autoren diese beiden Faktoren in seine Modelle übernommen hat (Friedewald et al., 2022; Herlo et al., 2022; Joecks-Laß & Hadwich, 2021; Kagermann, 2021; Kar & Thapa, 2020; Pohle, 2020). Während nur einige wenige der IT-Berater Regelungen in Unternehmen als Faktor nennen, sind alle 6 Autoren davon überzeugt, dass strengere Regelungen elementar sind (Friedewald et al., 2022; Herlo et al., 2022; Joecks-Laß & Hadwich, 2021; Kagermann, 2021; Kar & Thapa, 2020; Pohle, 2020). Kar und Thapa (2020) modellieren genau diesen Faktor in einer zusätzlichen Grafik, da sie die Abhängigkeit der Regelungen von der Leistungstiefe beschreiben wollen. Die Modellierung

des Sicherheitsaspekts wird von Pohle (2020) ausschließlich auf die staatliche Dimension beschränkt. Einerseits sehen 2 von 6 der Autoren aus der Literatur die Unabhängigkeit nicht als Schwerpunkt für digitale Souveränität (Herlo et al., 2022; Kar & Thapa, 2020). Andererseits weisen Joecks-Laß und Hadwich (2021) auf den Faktor Handlungskontrolle hin, um mehr digitale Souveränität zu erreichen. Das unterscheidet sich von den Interviewergebnissen. Obwohl 5 von 6 der Autoren aus der Literatur erwähnen, dass Unternehmen nicht vergessen sollten, Innovationen voranzutreiben, um die Wettbewerbsfähigkeit zu sichern, wird der Faktor Innovation bisher von keinem Autor modelliert.

Die Literatur in diesem Bereich kommt einheitlich zu dem Schluss, dass die deutsche digitale Souveränität mit Hilfe der europäischen Ebene gestärkt werden sollte (Friedewald et al., 2022; Hartmann, 2021; Herlo et al., 2022; Kagermann, 2021; Kar & Thapa, 2020; Pohle, 2020). Diese Abhängigkeit von Forschung und Entwicklung findet sich sowohl in dem Modell von Kar und Thapa (2020) als auch in dem Modell von Herlo et al. (2022) wieder. Die Abhängigkeit von den jeweiligen Möglichkeiten des Bundes zeigt sich in den Modellen von Kagermann (2021) und Pohle (2020). 3 der 6 Autoren sind auch der Meinung, dass Partnerschaften (Hartmann, 2021; Herlo et al., 2022; Pohle, 2020) und Kunden (Hartmann, 2021; Kagermann, 2021; Pohle, 2020) genauer untersucht werden müssen. Kagermann (2021) weisen darauf hin, dass es möglich ist, Kundenbereiche zur Stärkung der digitalen Souveränität zu finden (Kagermann, 2021). 2 von 6 Autoren in der Literatur erwähnen auch die Anpassung von Lieferketten als Folge der digitalen Souveränitätstransformation (Hartmann, 2021; Kagermann, 2021). 5 von 6 Autoren erwähnen Resilienz (Herlo et al., 2022; Joecks-Laß & Hadwich, 2021; Kagermann, 2021; Kar & Thapa, 2020; Pohle, 2020), Nachhaltigkeit (Friedewald et al., 2022; Herlo et al., 2022; Joecks-Laß & Hadwich, 2021; Kagermann, 2021; Pohle, 2020) und Datenhoheit (Friedewald et al., 2022; Herlo et al., 2022; Joecks-Laß & Hadwich, 2021; Kagermann, 2021; Pohle, 2020). Die Berücksichtigung von Schlüsseltechnologien wird von 4 von 6 Autoren (Herlo et al., 2022; Kagermann, 2021; Kar & Thapa, 2020; Pohle, 2020) und Agilität von 2 von 6 (Joecks-Laß & Hadwich, 2021; Kagermann, 2021) erwähnt. Nachhaltige digitale Souveränität und ihre Interdependenzen auf individueller

Ebene werden in diesem Zusammenhang in Herlo et al. (2022) diskutiert.

Neue Faktoren

Die Faktoren Benchmarking, Serviceportfolio und Benutzerfreundlichkeit waren Teil der Experteninterviewergebnisse, sind aber nicht Teil der analysierten Modelle (vgl. Tabelle 4.5). Keiner der Autoren erwähnt die Kommunikation innerhalb von Unternehmen, obwohl sie von allen IT-Beratern in der Interviewreihe genannt wurde. Pohle (2020) und Friedewald et al. (2022) schlagen zum Beispiel vor, mehr Telekommunikation zu fördern. Kagermann (2021) beschreiben die Verbesserung der Kommunikationsinfrastruktur und Herlo et al. (2022) nennen die Bedeutung einer Analyse von Kommunikationstechnologie. Kar und Thapa (2020) konzentrieren sich auf die Kommunikation zwischen Netzwerken. Darüber hinaus sehen Joecks-Laß und Hadwich (2021) die Kommunikation als wesentlich an, um mehr Verantwortung zu erlangen. Diese Arbeit unterstreicht, dass IT-Berater die Kommunikation innerhalb von Unternehmen eher als ein wesentliches Instrument betrachten.

4.1.3.5 Evaluation der Ergebnisse (zweite Interviewreihe)

Ziel dieses Abschnitts ist es, die vorangegangenen Ergebnisse zu evaluieren und herausfinden, ob das Modell für IT-Berater hilfreich ist und wie man es optimieren kann.

Das Modell hilft Beratern besser digitale Souveränität zu verstehen 94% der Befragten sehen die gegebenen Cluster als hilfreich an, um Unternehmen zu beraten, auf welche Faktoren sie sich bei der Stärkung der digitalen Souveränität konzentrieren sollten. Aus diesem Grund werden die vorgegebenen Cluster für das Modell beibehalten.

IT-Berater empfehlen, dass die neu identifizierten Themencluster hervorgehoben werden sollten. Sie werden daher im Modell mit einem Stern gekennzeichnet. Darüber hinaus kann man im Rahmen der Evaluation detaillierteren Einblick gewinnen, welche Themencluster den IT-Beratern besonders wichtig sind. Die Befragten wurden demnach gebeten, die Themen mit Hilfe einer Skala von 0=überhaupt nicht wichtig bis 4=sehr wichtig zu gewichten. Daraus konnten Mittelwerte (M) ermittelt werden. Im folgenden Abschnitt werden die errechneten Werte vorgestellt.

Mittelwerte unternehmensinterner Themencluster

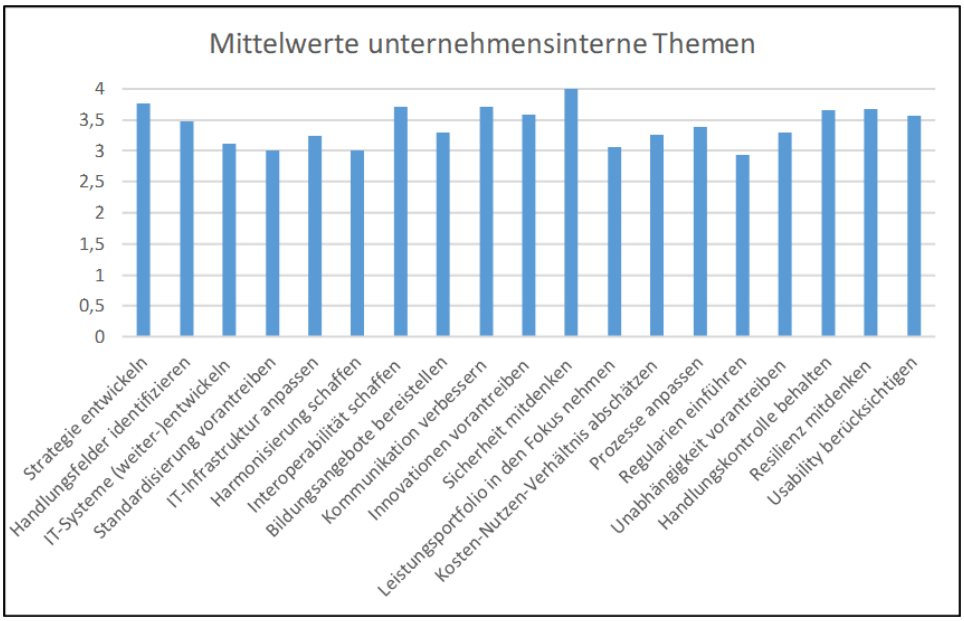


Abbildung 4.3: Mittelwerte unternehmensinterne Themen

Aus den berechneten Mittelwerten geht hervor, dass das wichtigste Thema für die IT-Berater die Gewährleistung von mehr IT-Sicherheit (M=4) im Kontext digitaler Souveränität ist (vgl. Abbildung 4.3). Auf das Thema IT-Sicherheit folgt für die Berater von der Bedeutung her die Entwicklung einer Strategie (M=3,76), gefolgt von der Gewährleistung von Interoperabilität (M=3,71), der Verbesserung der Kommunikation in Unternehmen (M=3,71) und schließlich der Gewährleistung von Resilienz (M=3,67). IT-Berater nennen als nächstes das Vorantreiben von Innovation und als etwas weniger wichtigen Faktor die Berücksichtigung von Benutzerfreundlichkeit (M=3,47). Den zuvor genannten Faktoren folgen das Zurückgewinnen bzw. Behalten von Handlungskontrolle (M=3,47), die Anpassung von Prozessen (M=3,38) und die Bereitstellung von Bildungsangeboten (M=3,29). Als nächstes ordnen die Interviewten die Schaffung von mehr Unabhängigkeit (M=3,29) ein, noch vor der Analyse des Kosten-Nutzen-Verhältnisses (M=3,25) und der Anpassung der IT-Infrastruktur (M=3,24). Die (Weiter-)entwicklung von IT-Systemen (M=3,12) und die Neuausrichtung des Leistungsportfolios (M=3,06) bilden gemeinsam mit den Themen Standardisierung (M=3), Harmonisierung (M=3)

und Regularien (M=2,94) das Schlusslicht.

Mittelwerte unternehmensexterner Themencluster

Der Abbildung 4.4 sind sechs externe Faktoren zu entnehmen.

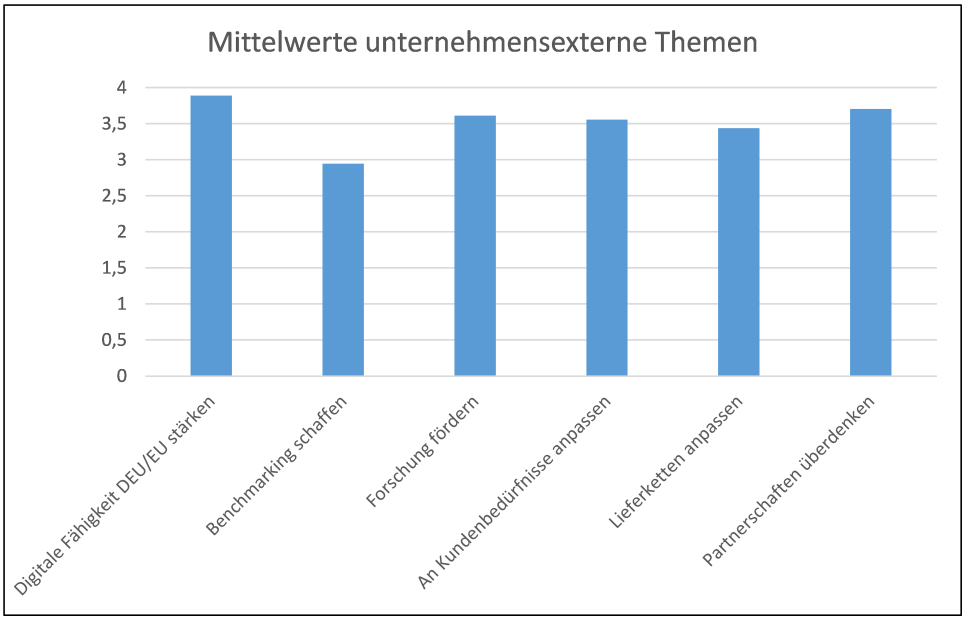


Abbildung 4.4: Mittelwerte unternehmensexterne Themen

Bei den unternehmensexternen Themen nimmt zunächst das Nutzen digitaler Fähigkeiten aus Deutschland und der EU die höchste Gewichtung ein (M=3,89), gefolgt vom Überdenken von Partnerschaften (M=3,71) und der Förderung von Forschung (M=3,61). Etwas unwichtiger als die anderen Faktoren ist den IT-Beratern nach die Anpassung an Kundenbedürfnisse (M=3,56) und die Anpassung von Lieferketten (M=3,44). Benchmarking ist von allen unternehmensexternen Clustern am unwichtigsten (M=2,94).

Mittelwerte übergreifender Themencluster

Abbildung 4.5 zeigt, wie die übergreifenden Themen gewichtet wurden.

Bei den unternehmensübergreifenden Themen wird deutlich, dass zwei Themen als gleich wichtig erachtet werden: Die Fossierung von Schlüsseltechnologien (M=3,56) und die Fokussierung auf das Thema Datensouveränität (M=3,56). Danach folgt erst die Förderung von Agilität in Projekten (M=3,17), während die Berücksichtigung des Themas Nachhaltigkeit eher unwichtig ist (M=2,78).

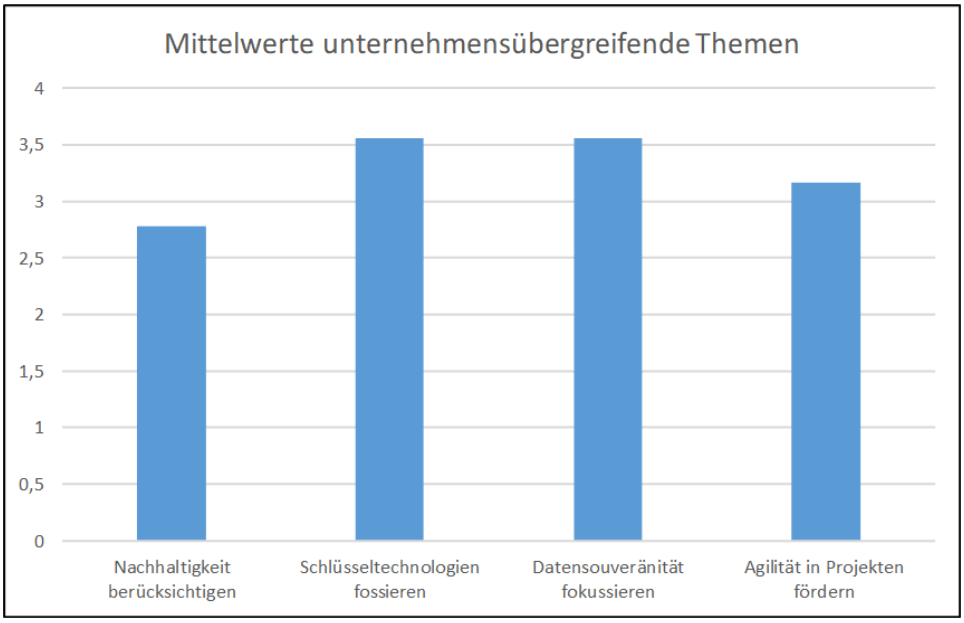


Abbildung 4.5: Mittelwerte unternehmensübergreifende Themen

4.1.3.6 Das DISO-B-Modell (Digitale Souveränitätsmodell-Optimierung durch kompetente Beratung)

Wie im Methodenanteil beschrieben, resultiert das finale Modell aus einem Prozess mehrerer Iterationen.

Das DISO-B-Modell umfasst die Ergebnisse aus den vorangegangenen Abschnitten 4.1.3.1 bis 4.1.3.5 (vgl. Abbildung 4.6). Es visualisiert die aus den Experteninterviews mit den IT-Beratern extrahierten Faktoren, markiert alle Faktoren, die in den oben genannten Modellen nicht in der ausgewählten und unter dem Modell genannten Literatur gefunden werden konnten, mit einem Stern, liefert ein Clustering und enthält Gewichtungen.

Das Modell digitaler Souveränität von Pohle (2020) dient als Orientierung für das Design, da es (1) Anwendbarkeit auf unternehmerische Fragestellungen, (2) Erweiterbarkeit um praxisnahe Ergebnisse und (3) Nutzbarkeit im Austausch mit genannten Experten bietet. Dieses Modell von Pohle (2020) kann dem Anhang entnommen werden (vgl. Abbildung 1, Anhang).

Schließlich ist dem DISO-B-Modell zu entnehmen, dass Zielkonflikte zwischen den Faktoren entstehen können, die nicht immer auflösbar sind. Ein Bei-

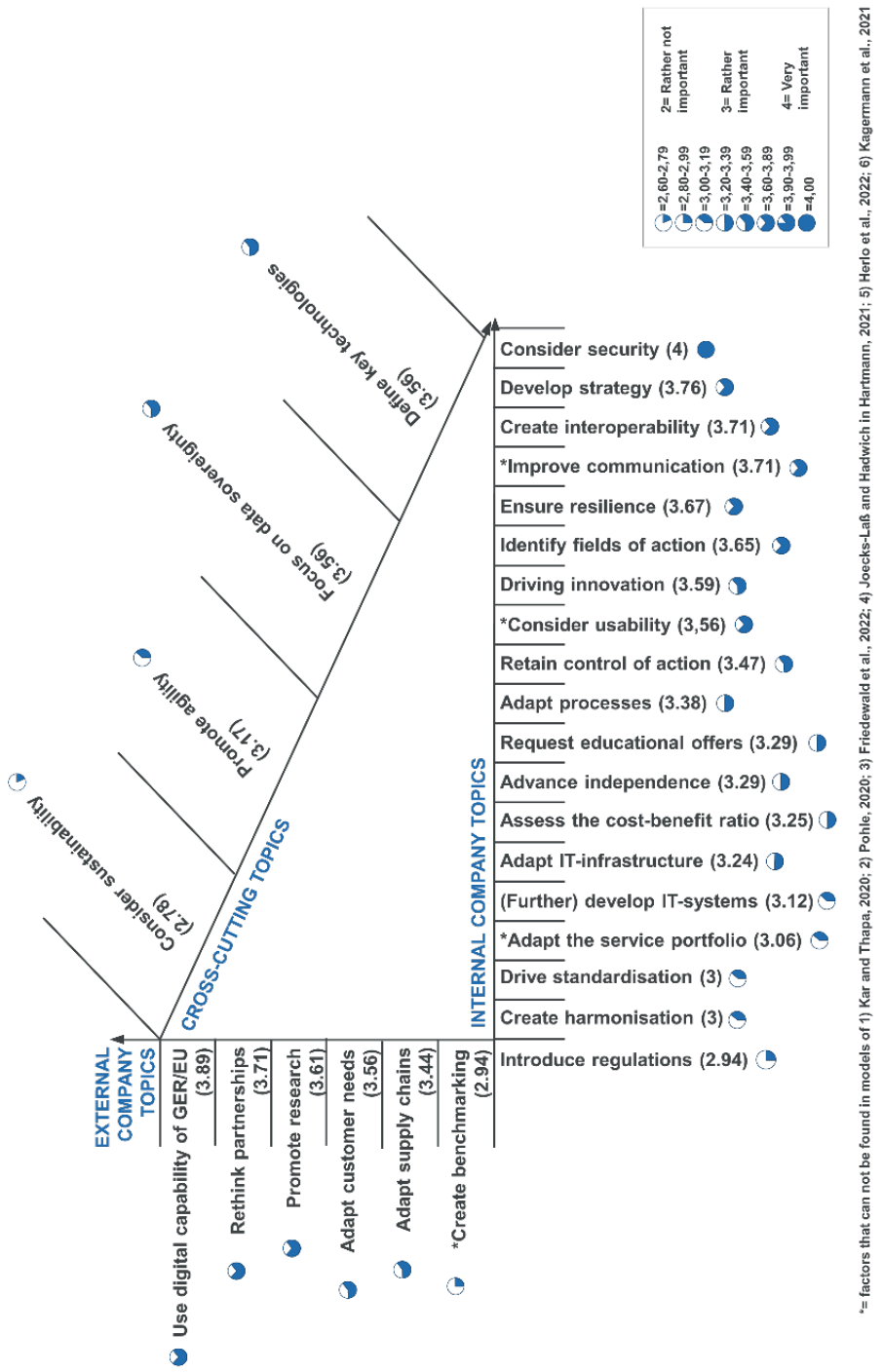


Abbildung 4.6: DISO-B: Digitale Souveränitätsmodell-Optimierung durch kompetente Beratung (1. Version)

spiel ist: Entscheidet sich ein Unterenhmen für die Entwicklung von souveränen IT-Systemen in-house, kann das im Konflikt stehen mit der Nutzung europäischer oder strategischer Partner zur Bereitstellung souveräner IT-Systeme.

4.1.4 Zusammenfassung, Limitationen, Ausblick

Die Ergebnisse weisen darauf hin, dass es eine Kombination strategisch-technischer Herausforderungen zu bewerkstelligen gilt, um digitale Souveränität zu erreichen. Zum Beispiel, wie man als Unternehmen sein Service-Portfolio aufsetzen will, das ist eine sowohl strategische als auch technische Entscheidung. Digitale Souveränität ist damit aus Perspektive der IT-Beratung nicht durch rein technische Maßnahmen zu lösen.

Zusammenfassend lässt sich festhalten, dass das Modell mit Faktoren digitaler Souveränität aus Sicht der IT-Beratung Orientierung bieten kann, welche Faktoren IT-Berater berücksichtigen können, wenn sie sich dem Thema digitale Souveränität im Unternehmenskontext nähern. Das Modell zeigt auf, welche Faktoren andere Unternehmen in Zusammenarbeit mit IT-Beratern angegangen sind, um ihre digitale Souveränität zu stärken. Zudem hat der Vergleich mit bereits existierenden Modellen in der Literatur gezeigt, dass neue Faktoren gefunden werden konnten. Darunter: 1) Verbesserung der Kommunikation in Unternehmen, 2) die Anpassung des Service-Portfolios und 3) die Berücksichtigung der Bedienbarkeit von Anwendungen, wenn digitale Souveränität gestärkt werden soll.

Es können jedoch Zielkonflikte zwischen den Faktoren entstehen, die nicht immer auflösbar sind.

Die systematische Literaturrecherche umfasst Literatur von 2014 bis 2022. Ein anderer Betrachtungshorizont würde zu anderen Ergebnissen führen.

Auf der International Conference on Software Business, wo das Modell vorgestellt wurde, diskutierten wir zwei Punkte: 1) Digitale Souveränität ist wohlmöglich szenar-abhängig. Die Faktoren könnten sich in einem anderen Szenar verändern. 2) Es kann problematisch sein, digitale Souveränität ausschließlich aus der Perspektive der IT-Beratung zu betrachten. Diese beiden Hypothesen werden im Rahmen dieser Dissertationsschrift überprüft.

Als nächsten Forschungsschritt ist das Modell kritisch vor dem Hintergrund

eines anderen Szenars zu reflektieren: die Landesverteidigung Deutschlands.

4.2 Zweite Fallstudie: Interviewstudie zu Faktoren digitaler Souveränität aus Perspektive der IT-Beratung (Landesverteidigung)

Eine erste Version des nachfolgenden Kapitels wurde hier veröffentlicht: *Klare, M., and Lechner, U. (2024). German Digital Sovereignty–Success Factors in a National Defense Scenario from the Standpoint of IT Consultancy. In I. Fries, M. Grabatin and M. Hofmeier (Hrsg.), LIONS Sovereign by Design (pp. 41–56). Logos Verlag Berlin. https://doi.org/https://doi.org/10.30819/5834*

4.2.1 Einleitung

Das Modell aus dem vergangenen Kapitel wurde für ein Friedensszenar entwickelt. Sollte es zu einem Landesverteidigungsfall kommen, so kann davon ausgegangen werden, dass sich das Modell verändert. Es stellt sich die Frage, wie digitale Souveränität für den Fall, Deutschland stünde im Kriegsgeschehen, aussehen würde (Klare & Lechner, 2024a). Ziel ist es somit, ein neues Modell explizit für den Fall Landesverteidigung (LV) zu entwickeln und Unterschiede zu den Auswertungen im Friedensfall aufzuzeigen. Der Fokus der Erhebung liegt weiterhin auf der IT-Beratung in Deutschland.

Es ist interessant digitale Souveränität vor dem Hintergrund eines derartig eskalativen Konflikts zu untersuchen, weil weil in solchen Szenarien die Abhängigkeit von ausländischen IT-Dienstleistern, Cloud-Infrastrukturen oder Softwarelösungen ein erhebliches Sicherheitsrisiko darstellen würde (Moerel & Timmers, 2021). In Krisen- oder Kriegszeiten müssen Staaten in der Lage sein, ihre digitalen Infrastrukturen unabhängig, sicher und selbstbestimmt zu betreiben (Pohle, 2020). Digitale Souveränität im Kontext der Landesverteidigung verdeutlicht, wie eng digitale Infrastruktur mit nationaler Sicherheit verbunden ist – und wie wichtig es ist, rechtzeitig strategische, technologische und organisatorische Vorkehrungen zu treffen. Ziel dieses Kapitels, ist es - durch eine Erweiterung des DISO-C-Modells - einen für Unternehmen Leitfaden zu entwickeln, digitale Souveränität im Falle der Landesverteidigung zu berücksichtigen. Die Analyse in diesem Kapitel fokussiert sich damit darauf, auf welche Faktoren es in diesem Szenar ankommt und auf welche nicht.

Folgende Forschungsfrage soll beantwortet werden:

- Wie verändert sich das DISO-B-Modell im LV-Fall?

In Kapitel 4.2.2 wird das Szenar festgelegt und dann das Forschungsdesign vorgestellt (Kapitel 4.2.3). Die Analyseergebnisse finden sich im Anschluss im Kapitel 4.2.4 wieder, gefolgt von dem Schluss (Kapitel 4.2.5).

4.2.2 Szenare für digitale Souveränität: Friedensfall vs. Landesverteidigung

Um sich einer Definition von digitaler Souveränität weiter anzunähern, scheint es wichtig, sich darüber im Klaren zu werden, aus welchem Szenar heraus, digitale Souveränität erzielt werden soll: aus einem Friedens- oder einem Landesverteidigungsszenario.

Unter Landesverteidigung versteht man ein Szenar, in dem die Verteidigung Deutschlands durch die Bundeswehr eingeleitet wird (Fuhr, 1977). Es handelt sich hierbei um eine Krisensituation, in dem eine Abwehr gegenüber eines Agressors erfolgt (Unger, 2014). Die Landesverteidigung wird definitorisch von der Bündnisverteidigung abgegrenzt. Bei der Bündnisverteidigung handelt es sich um eine kollektive militärische Anstrengung durch mehrere Staaten (Möllers, 2022). Die Friedenstheorie, die hier angenommen wird, grenzt sich von der Landesverteidigung wie folgt ab: Es geht von einer friedlichen Tranformation aus, die keine Ausklammerung von Konlikten meint, sondern vielmehr den Zustand eines Nicht-Kriegs-Zustandes (Brock, 1990; Klare & Lechner, 2024a).

4.2.3 Forschungsdesign

Das Forschungsdesign in der zweiten Fallstudie ist in Abbildung 4.7 dargestellt.
Bestimmung des Analyseumfangs: Diese Analyse begrenzt sich auf den Fall der LV.
Datengenerierung: Methodisch wird eine Interviewstudie durchgeführt. Die Ergebnisse aus der ersten Fallstudie sollen um neue Ergebnisse in einem anderen Szenar erweitert werden. Als Leitfaden für die Interviews dienen die Fragen, die dem Anhang entnommen werden können (vgl. Abbildung 20-24, Anhang). Als Interviewte dienen, wie auch schon in der ersten Fallstudie, IT-Berater aus Deutschland (vgl. Tabelle 4.6).
Sie wurden in der Zeit von Oktober 2022 bis Januar 2023 befragt. Dabei sind die IT-Berater mit dem Szenar der LV in Deutschland konfrontiert worden,

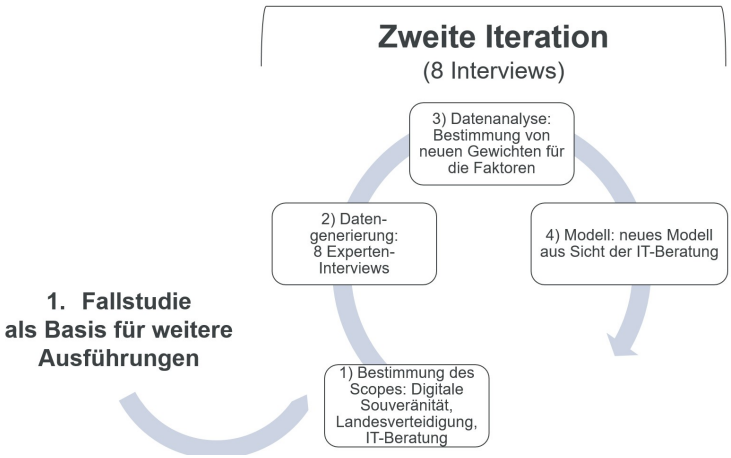


Abbildung 4.7: Forschungsdesign für die zweite Fallstudie

Interviewte	**Expertise**	**Länge des Interviews** (Stunden:Minuten:Sekunden)
IT-Berater 1	Innovation Management im militärischen Sektor	01:05:52
IT-Berater 2	Prozessberatung im öffentlichen Sektor	00:49:33
IT-Berater 3	Strategieberatung für den militärischen Sektor	00:54:28
IT-Berater 4	Projektmanagement im Cyber- und Informationsraum	00:54:10
IT-Berater 5	Planung und Beschaffung von Hardware und Software	01:28:03
IT-Berater 6	Enterprise Service Management im öffentlichen Sektor	00:52:34
IT-Berater 7	IT-Sicherheit im militärischen Sektor	00:52:35
IT-Berater 8	Organisationsanpassungen im öffentlichen Sektor	00:49:59
		07:75:23

Tabelle 4.6: Übersicht der Befragten in der zweiten Fallstudie

indem dieses Szenar als Ausgangslage des Interviews diente. Zudem wurde ihnen eine Definition digitaler Souveränität geliefert sowie das DISO-C-Modell aus der ersten Fallstudie. Sie konnten die einzelnen Faktoren neu gewichten oder unwichtige Faktoren herausstreichen.

Datenanalyse: Ziel der Datenanalyse ist es, die Veränderungen der Gewichtungen zwischen dem Friedensfall und dem LV darzustellen, neue Cluster zu bilden sowie ein neues Modell für den Fall der LV zu liefern.

Modell: Der letzte Abschnitt liefert ein neues Modell für digitale Souveränität aus Sicht der IT-Beratung. Dieses Mal, für das Szenar der LV.

4.2.4 Ergebnisse

4.2.4.1 Neue Gewichtungen im Landesverteidigungsfall

Tabelle 4.7 stellt dar, wie sich die Gewichte der Faktoren digitaler Souveränität im Szenar Landesverteidigung verändern.

Eine Strategie für digitale Souveränität als wichtigster Faktor Die Daten verdeutlichen, dass vor Eintritt des LV-Falls die Entwicklung einer Strategie für das Thema digitale Souveränität notwendig ist. Die IT-Berater schätzen es demnach, ähnlich wie im Friedensfall, auch in einem Krisenszenario als sehr wichtig ein, einen Plan in Form einer Strategie zu entwickeln (M=4). Die Gewichtung steigt leicht in der Krisensituation im Vergleich zur Friedenssituation (δ=0,24). Es fällt auf, dass die IT-Berater im Friedensfall die Schaffung von IT-Sicherheit durch technologische Maßnahmen als am wichtigsten erachteten. Im LV-Fall reiht sich neben dieser Dimension nun auch die Strategie als Top-Thema ein.

Weiterhin hoher Stellenwert des Themas IT-Sicherheit Unternehmen müssen sich weiterhin die Frage stellen, wie sie sich sicher im Cyberraum bewegen können, aber auch sichere Hard- und Software beschaffen können, oder sicherheitsbewusste Partner bei Krisensituationen in ihr digitales Ökosystem einbetten können. Die IT-Berater finden das Thema IT-Sicherheit sehr wichtig (M=4). Im Vergleich zur Friedenssituation hat sich die Gewichtung nicht verändert (δ=0).

Zurückgreifen auf digitale Fähigkeiten in Deutschland bzw. Europa auch im Krisenszenar notwendig Den Daten nach sollten Unternehmen, auch im Krisenszenar, wenn möglich, auf europäische Fähigkeiten zurückgreifen. Es ist aus Sicht der IT-Beratung wichtig (M=3,88) zu prüfen, welche europäische Software oder Hardware man beschaffen kann. Die Gewichtung dieser Facette verändert sich im Vergleich zum Friedenfall kaum (δ=-0,01).

Die Sicherstellung von Datensouveränität ist bedeutsam für die Handlungsfähigkeit Datensouveränität nimmt im Szenar eine noch etwas höhere Bedeutung ein, jedoch mit anderer Ausrichtung (M=3,88, δ=0,32). Es wird argumentiert, dass nur mit Hilfe des Zugangs zu Daten das Handeln des Akteurs in der Krise gut unterstützt werden kann und nur dann eine

Faktor	Alte Gewichtung (Friedensfall)	Neue Gewichtung (Landesverteidigung)	Differenz
Strategie berücksichtigen	3,76	4	+0,24
Aktionsfelder identifizieren	3,38	3,38	0
IT-Systeme (weiter-)entwickeln	3,12	3,5	+0,38
IT-Infrastruktur anpassen	3,24	3,75	+0,51
Harmonisierung schaffen	3	2,63	-0,37
Standardisierung vorantreiben	3	3,13	+0,13
Interoperabilität schaffen	3,71	3,57	-0,14
Bildungsangebote anfordern	3,29	3,13	-0,16
Kosten-Nutzen-Verhältnis bewerten	3,25	2	-1,25
Prozesse anpassen	3,38	2,88	-1,10
Regulierungen einführen	2,94	2,43	-0,49
IT-Security berücksichtigen	4	4	0
Handlungskontrolle gewährleisten	3,71	3,57	-0,14
Innovationen vorantreiben	3,47	3,5	+0,03
Forschung fördern	3,59	3,63	+0,04
Digitale Fähigkeit DEU/EU nutzen	3,89	3,88	-0,01
An Kundenbedürfnisse anpassen	3,56	3,63	+0,07
Lieferkette anpassen	3,71	3,75	+0,04
Resilienz sicherstellen	3,56	3,63	+0,07
Nachhaltigkeit berücksichtigen	3,44	1,25	2,19
Auf Datensouveränität fokussieren	3,67	3,88	-0,21
Schlüsseltechnologien definieren	2,78	3,75	-0,97
Agilität fördern	3,17	3,38	+0,21
Kommunikation verbessern	3,71	3,38	-0,33
Service Portfolio anpassen	3,06	3,38	+0,32
Nutzerfreundlichkeit berücksichtigen	3,56	3,25	-0,31
Benchmarking durchführen	2,94	2,13	-0,81

Tabelle 4.7: Überblick über die Gewichtungen im Friedensfall, im Verteidigungsfall und deren Differenz

fundierte Ableitung von Entscheidungen möglich ist.

Gewährleistung von Resilienz Resilienz ist im Szenar Verteidigung noch bedeutender als zuvor (M=3,63, δ=0,07). Gerade im Krisenszenario ist die Möglichkeit, Funktionalitäten in gewissem Maße aufrechtzuerhalten und Widerstandsfähigkeit gegen Cyberangriffe durch Prozesse, IT-Systeme und Infrastruktur zu gewährleisten, wichtig.

Gewährleistung von sicherer, resilienter IT-Infrastruktur Die IT-Infrastruktur, auf die das Unternehmen zurückgreift, muss sicher und resilient gegenüber Angriffen sein. Das ist im Szenar Landesverteidigung noch wichtiger (δ=0.31). IT-Berater sehen es als wichtig an (M=3,75), die Anzahl an Ausfällen möglichst zu reduzieren, schnelle Reaktionszeiten mit Krisenplänen aufzuweisen und unbefugtes Eindringen so gut es geht zu verhindern.

Eingehen sicherer, strategischer Partnerschaften Ebenso wichtig wie eine sichere IT-Infrastruktur schätzen die IT-Berater sichere, strategische Partnerschaften ein (M=3,75). Die Gewichtung im Vergleich zum Friedensfall ist deutlich höher (δ=0,51).

Management von Software- und Hardwarekomponenten in Lieferketten Es ist davon auszugehen, dass sich die Lieferketten im Verteidigungsfall verschieben. Unternehmen werden auf andere Software- und Hardware-Komponenten zurückgreifen müssen, als das im Friedensfall der Fall ist. Dies spiegelt sich in der Gewichtung der IT-Berater wider (δ=0,04). Sie schätzen ein souveränes Management von Software- und Hardware-Lieferketten als wichtig ein (M=3,75).

Förderung von Innovationen im Krisenszenar noch wichtiger Die IT-Berater sehen schnelle Innovationen in einem Krisenszenar als notwendigen Treiber und im Kontext digitaler Souveränität als zwingend an. Die Gewichtung ist leicht aufsteigend im Vergleich zum Friedensfall (M=3,5, δ=0,03).

Berücksichtigung von Kundenbedürfnissen Geht man davon aus, dass Unternehmen im Kriegsfall dazu gezwungen werden, im Sinne der Verteidigungsstrategie zu leisten, so schlussfolgern die IT-Berater, dass eine Ausrichtung auf eben diese Kunden durchaus wichtig ist. Die IT-Berater gehen jedoch davon aus, dass sich die Kunden im Krisenszenar verändern. Gesetzt diesen Falles sollten die Unternehmen ihre Kunden kennen und sich auf ihre Bedürf-

nisse ausrichten. Das ist jedoch auch im Friedensszenar so. Deswegen verändert sich die Gewichtung der IT-Berater im Mittel kaum (M=3,63, δ=-0,07).

Sicherstellung von Interoperabilität zwischen den IT-Systemen als Zusatzthema Interoperabilität, also die Vereinbarkeit von Systemen, ist ein sehr bedeutsames Thema. Hier im Szenar der Verteidigung nimmt es aber an Gewicht ab, weil die Funktionalität militärischer Systeme eine höhere Bedeutung einnimmt (M=3,57, δ=-0,14). Im Sinne der digitalen Souveränität ist die Sicherstellung interoperabler Systeme wünschenswert, es ist jedoch kein hochpriorisiertes Thema.

(Weiter-)entwicklung von IT-Systemen, da diese notwendig im Szenar sind Den IT-Beratern nach ist davon auszugehen, dass im Falle der Landesverteidigung andere IT-Systeme oder die Weiterentwicklung bestehender IT-Systeme notwendig ist. Um in diesem Szenar souverän agieren zu können, betonen die Interviewten die Notwendigkeit passender IT-Systeme und unterstreichen dies mit einer höheren Gewichtung als im Friedensfall (M=3,5, δ=0,38).

Förderung von Agilität in Projekten, um Geschwindigkeit zu erzeugen Flexibles Handeln bei gleichzeitiger Einhaltung staatlicher Regulierungen, ist nach Meinung der IT-Berater notwendig, um Geschwindigkeit im vorliegenden Szenar zu erzeugen. Unter dieser Prämisse, nimmt die Förderung von Agilität im Vergleich zum Friedenszenar zu (M=3,38, δ=0,21).

Verbesserung der Kommunikation zum Thema digitale Souveränität vor Eintritt des Szenars Für die IT-Berater ist es wichtig, Pfeiler zu setzen, um digitale Souveränität zu treiben. Hierzu bedarf es Kommunikation, die jedoch vor Eintritt des Szenars erfolgen muss, damit innerhalb des Szenars Entscheidungsfreiheit entstehen kann. So nimmt die Gewichtung dieses Faktors im Vergleich zum Friedensfall lediglich leicht ab (M=3,38, δ=-0,33).

Anpassung des Service-Portfolios auf Basis der Anforderungen Das Leistungsportfolio hat sich im Friedensfall als neuer Faktor hervorgetan. Im Verteidigungsfall wird deutlich, dass es insbesondere wichtig ist, dass die Leistung im Sinne des Szenars ausgerichtet ist. Konkret, dass Services militärisch angepasst werden. Die Bedeutung des Faktors nimmt zu (M=3,38, δ=0,32).

Berücksichtigung von Nutzerfreundlichkeit bei den Systemen auch im Krisenfall Es ist sowohl im Verteidigungsfall als auch im Friedensfall

wichtig, dass IT-Systeme nutzerfreundlich gestaltet sind. Die IT-Berater unterstreichen, dass die Nutzerfreundlichkeit einen wesentlichen Einfluss auf das Überleben von Soldaten haben kann. So schätzen die Berater die Bedeutung der Nutzerfreundlichkeit von IT-Systemen im Krisenfall als noch höher ein, als im Friedensfall (M=3,25, δ=-0,31).

Definition von Schlüsseltechnologien vor der Entwicklung der IT-Systeme Es wird aus den Interviews deutlich, wie wichtig es ist, Schlüsseltechnologien zu beherrschen, um für das Szenar sinnstifende, gute IT-Systeme zu entwickeln. Es ist jedoch zu spät, sich erst im Krisenszenar selbst mit dem Thema zu beschäftigen. Das muss vorgelagert passieren. Die IT-Berater gewichten den Faktor im Krisenszenar sogar höher (M=3,75, δ=0,97).

Vermittlung von Bildungsangeboten vor dem Szenar Es wurde im Friedensszenar deutlich, dass es zwar eine untergeordnete Rolle spielt, Bildungsangebote für digitale Souveränität bereitzustellen; der Faktor sollte dennoch nicht untergraben werden. Im Verteidigungsszenar ist eine Vermittlung von Anforderungen weiterhin wichtig, weshalb auch die Gewichtung nur leicht abnimmt (M=3,13, δ=-0,16).

Festlegung von Standards für IT, um die Geschwindigkeit zu erhöhen Das Festlegen von Standards für Strukturen, Prozesse und IT-Systeme, kann einen wesentlichen Beitrag leisten, Geschwindigkeit im Verteidigungsszenar zu erhöhen. Diese ist insbesondere in diesem Szenar wichtig, weswegen die IT-Berater diesen Faktor wichtiger im Verteidigungsszenar einschätzen, als im Friedensszenar (M=3,13, δ=0,13).

Die Schaffung von Prozessen für digitale Souveränität ist lediglich ein unterstützender Faktor Um koordiniert Funktionsfähigkeit im Szenar zu gewährleisten, ist eine Definition und Etablierung von Prozessen für digitale Souveränität für die IT-Berater zwar im Vorhinein wichtig, jedoch deutlich weniger als im Friedensfall (M=2,88, δ=-1,10). Die IT-Berater unterstreichen die unterstützende Funktion von Prozessen. Viel wichtiger scheinen die Themen der Schaffung einer entsprechenden Strategie oder der Gewährleistung von IT-Sicherheit für die Stärkung digitaler Souveränität.

Förderung des Austauschs mit der Forschung Die Förderung und der Austausch mit der Forschung nehmen im neuen Szenar eine etwas weniger

wichtige Rolle ein (M=3,63, δ=0,04). Die IT-Berater betonen in diesem Zusammenhang, dass wenig Raum für Forschungsvorhaben bleibt, sondern eher die Schaffung von Geschwindigkeit angestrebt werden sollte. Dennoch sind Innovationen wichtig, um im Krisenszenar zu bestehen, was mit schnellen Forschungsvorhaben möglich werden könnte.

Harmonisierung von IT-Systemen Die Harmonisierung von IT-Systemen kann zu höherer Angreifbarkeit führen und nimmt deswegen im Verteidigungsszenar an Bedeutung ab (M=2,63, δ=-0,37).

Aufstellen unternehmensinterner Regeln für digitale Souveränität vor dem Szenar Wie im Friedenszenar deutlich wurde, braucht es Maßnahmen, um digitale Souveränität zu erreichen. IT-Berater schlagen die Einführung unternehmensinterner Regulierungen (z.B. Regeln zur Beschaffung oder Regeln zur Zusammenarbeit mit souveränen, sicheren Partnern) vor, finden diese im Verteidigungsszenar jedoch nicht ausschlaggebend (M=2,43, δ=-0,49). Sie gewichten den Faktor deutlich weniger wichtig und betonen, dass das Aufstellen von Regulierungen ebenfalls vorab erfolgen muss.

Nutzen von Benchmarkings nicht ausschlaggebend Sich Benchmarking-ähnlich an anderen zu orientieren, nimmt im Szenar an Bedeutung ab. Der Faktor Benchmarking ist für die IT-Berater in einem Krisenszenar nur von geringem Interesse (M=2,13, δ=-0,81)

Das Analysieren des Kosten-Nutzen-Verhältnisses nimmt im Szenar stark an Bedeutung ab Die IT-Berater machten bereits im Friedensszenar deutlich, dass das Thema Sicherheit mit Kosten einhergehen muss. Im Verteidigungsfall verstärkt sich dieses Bild. Die Bedeutung einer Analyse von Kosten zu Nutzen nimmt im Vergleich zum Friedensfall stark ab (δ=-1,25, M=2).

Berücksichtigung von Nachhaltigkeit wird obsolet Alle IT-Berater machen deutlich, dass Nachhaltigkeit im Verteidigungsszenar obsolet wird (M=1,25, δ=2,19).

4.2.4.2 Neue Cluster im Landesverteidigungsfall

Auf Basis der Ergebnisse wird Nachhaltigkeit als Faktor aus dem Modell herausgenommen, da die Gewichtung des Mittelwerts bei <2 liegt und der Faktor damit im vorliegenden Szenario obsolet ist. Der Faktor Unabhängigkeit

wird eher als übergeordnetes Ziel von den IT-Beratern verstanden; deswegen wird er ebenfalls aus dem Modell entfernt. Resilienz sollte mit Infrastruktur und IT-Systemen der IT-Berater verknüpft werden, sodass sie Resilienz unter diese Themen (IT-Infrastruktur und IT-Systeme) eingebettet ist.

4.2.4.3 Das DISO-L-Modell (Digitale Souveränitätsmodell-Optimierung im Landesverteidigungsfall)

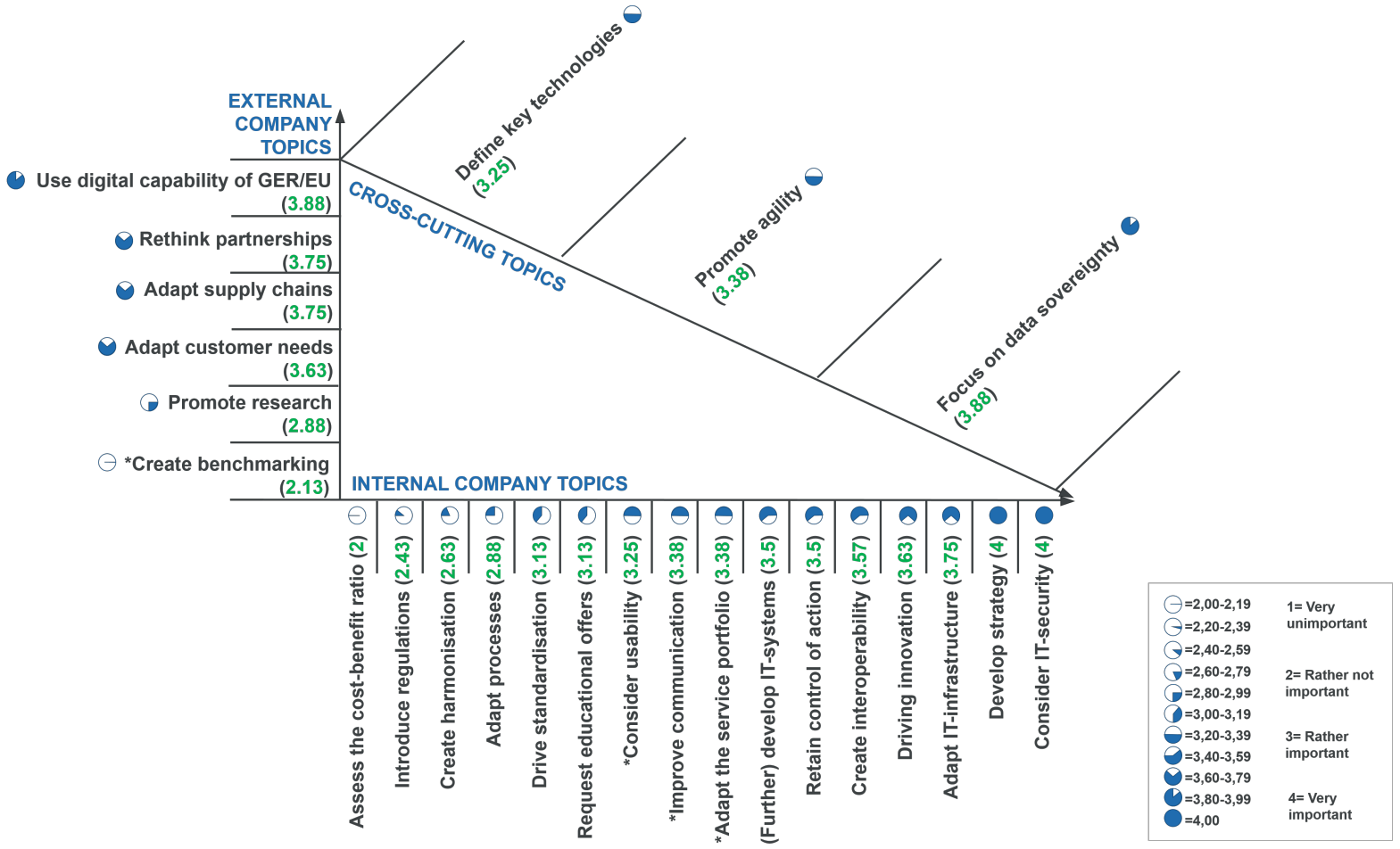
Auf der Grundlage der Ergebnisse wird ein neues Modell entwickelt (vgl. Abbildung 4.8). Es berücksichtigt alle unter den Abschnitten 4.2.4.1 und 4.2.4.2 beschriebenen Ergebnisse.

4.2.5 Zusammenfassung, Limitationen, Ausblick

Die Ergebnisse zeigen, dass die folgenden Faktoren im Fall der Landesverteidigung am wichtigsten sind: (1) die Entwicklung einer Strategie für digitale Souveränität, (2) die Berücksichtigung der IT-Sicherheit und (3) der Rückgriff auf europäische digitale Kompetenzen.

Darüber hinaus gewinnen folgende Faktoren im Vergleich zum Friedensszenario deutlich an Gewicht: die Anpassung der IT-Infrastruktur in Bezug auf Sicherheit und Resilienz, die Entwicklung von IT-Systemen und die Datensouveränität in Unternehmen. Die vorliegende Forschung ist auf die Perspektive der IT-Beratung limitiert.

Der nächste Forschungsschritt sieht vor, die vorangegangenen Ergebnisse um Einblicke von Professoren aus den Fachbereichen Informatik, Wirtschaftsinformatik und Betriebswirtschaftslehre zu erweitern und so eine neue Perspektive zu liefern.



*= factors that can not be found in models of 1) Kar and Thapa, 2020; 2) Pohle, 2020; 3) Friedewald et al., 2022; 4) Joecks-Laß and Hadwich in Hartmann, 2021; 5) Herlo et al., 2022; 6) Kagermann et al., 2021

Abbildung 4.8: DISO-L: Digitale Souveränitätsmodell-Optimierung im Landesverteidigungsfall (2. Version)

4.3 Dritte Fallstudie: Interviewstudie zu Faktoren digitaler Souveränität aus Perspektive von Professoren aus der Informatik, Wirtschaftsinformatik, und Betriebswirtschaftslehre

4.3.1 Einleitung

Die dritte Fallstudie berücksichtigt eine neue Perspektive: die von Professoren aus den Bereichen Informatik, Wirtschaftsinformatik und Betriebswirtschaftslehre. Ziel ist es damit das DISO-L-Modell, das derzeit auf empirischen Daten mit IT-Beratern beruht, um diese neue Perspektive zu erweitern. Von Interesse ist dabei, welche der bereits erarbeiteten Cluster sich bestätigen lassen. Eine offene Fragestellung ist demnach:

- Wie verändert sich das DISO-L-Modell, wenn das Thema digitale Souveränität aus der Perspektive von Professoren aus den Bereichen INF, WINF und BWL betrachtet wird?

Dieses Kapitel unterliegt dem Forschungsinteresse, die Ergebnisse aus den Interviewstudien mit den IT-Beratern vor dem Hintergrund einer anderen Befragungsgruppe zu verifizieren. Es ist wichtig, eine heterogenere Auswahl an Interviewten zu haben, weil dadurch eine breitere, differenziertere und validere Perspektive auf das hier untersuchte Thema gewonnen werden kann. Vor allem in explorativen oder qualitativ angelegten Studien erhöht Heterogenität die Aussagekraft und Tiefe der Ergebnisse (Lorenc et al., 2016).

Auch diese Fallstudie baut wieder iterativ auf dem DISO-L auf. Die Iterationen helfen dabei das Verständnis digitaler Souveränität zu erweitern. Dieses erweiterte Verständnis wird in einem neuen Modell namens DISO-A (Academia) abgebildet.

Dieses Kapitel ist wie folgt strukturiert: In Kapitel 4.3.2 wird das verwendete Forschungsdesign vorgestellt. Danach folgt die Kommunikation der Ergebnisse (Kapitel 4.3.3), eine Zusammenfassung, die Beschreibung von Limitationen und schließlich ein Ausblick (Kapitel 4.3.4).

4.3.2 Forschungsdesign

Wie in Abbildung 4.9 dargestellt, dienen für die folgende Studie die Ergebnisse aus der zweiten Fallstudie als Basis (siehe Kapitel 4.2).

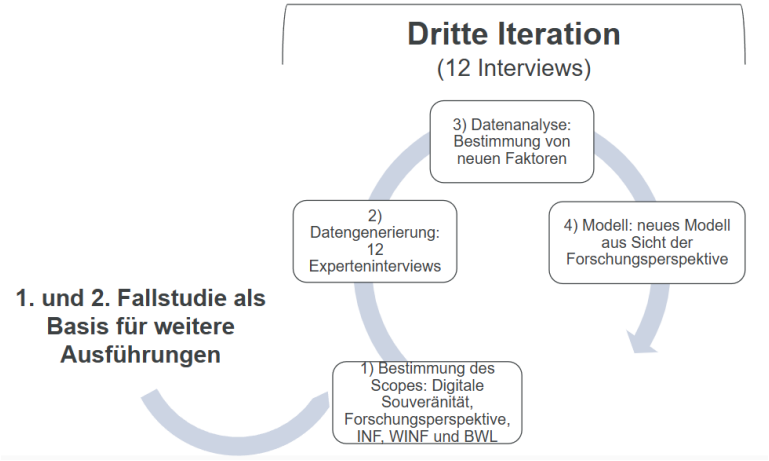


Abbildung 4.9: Forschungdesign dritte Fallstudie

Es werden leitfadengestützte Interviews durchgeführt und die Ergebnisse übergeprüft. Ähnliche Themen werden wieder in Codes zusammengefasst und die Codes zu Themenclustern benannt. Dabei wird geprüft, ob ein Themencluster einem der bereits ermittelten Themencluster aus der zweiten Fallstudie zugeordnet werden kann. Konnte ein Code keinem Themencluster zugeordnet werden, so wird ein neuer Code eingeführt und dieser mit einem neuen Themencluster versehen. Mehrere Nennungen werden kumuliert und in Balkendiagrammen abgebildet, sodass eine Übersicht entsteht, die zeigt, welche der Antworten besonders häufig von den Interviewten gennant werden. Der Forschungsrahmen unterscheidet sich in dieser Studie insofern, dass nicht IT-Berater befragt werden, sondern Professoren. Als Daten dienen elf Experteninterviews. Die Interviews wurden zwischen März und April 2023 durchgeführt. Ziel der Analyse ist die Extraktion neuer Faktoren digitaler Souveränität. Die Professoren sind angestellt an der Hochschule Bremen, der Johannes-Gutenberg-Universität Mainz, der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), der Steinbeis Hochschule Berlin, der Universität Bonn, der Universität Köln, der Universität Bremen und schließlich der UniBw München. Die UniBw München ist in drei Fällen vertreten, die FAU in zwei Fällen. Vier der Professoren sind dem Lehrstuhl für Betriebswirtschaftslehre zuzuordnen, drei dem Lehrstuhl für Informatik und fünf dem Lehrstuhl für Wirtschaftsinformatik.

Für die Datenanalyse soll wieder methodisch auf die qualitative Inhaltsanalyse nach Mayring und Fenzl (2019) zurückgegriffen werden, um aus den Experteninterviews neue Ergebnisse zu gewinnen. Diese neuen Ergebnisse aus Sicht der Professoren werden mit den Ergebnissen aus der zweiten Fallstudie verglichen. Es wird dargestellt, was sich verändert hat oder was bestätigt werden kann. Schließlich fließen die Ergebnisse in ein neues Modell für digitale Souveränität.

4.3.3 Ergebnisse

Dieser Ergebnisteil will die Frage beantworten, ob Professoren die Cluster aus dem vorangegangenen Modell aus Kapitel 4.2 bestätigen oder nicht. Der Fragebogen orientierte sich an den Clustern, die bereits in den ersten beiden Fallstudien ermittelt wurden (siehe Anhang). Die Anzahl der Nennungen von Themen sind im Ergebnisabschnitt kumuliert und dann in Prozent umgerechnet worden.

4.3.3.1 Was hat sich verändert?

Wie in Abbildung 4.10 dargestellt, gibt es im Vergleich zum DISO-L-Modell einige neue Faktoren digitaler Souveränität.

Investitionen (Automobilsektor, KI, 5G, Cloud, Big Data) Alle Professoren äußern die Bedeutung von Investitionen für die Stärkung digitaler Souveränität. Zwei Investitionsbereiche sind besonders hervorgehoben worden: der Automobilsektor und die KI-Forschung. Im Wettbewerb mit Ländern wie China und Amerika scheint es auf Basis der Interviewergebnisse bedeutsam, einen führenden Platz im KI-Wettbewerb zu finden. Aus Sicht von 9% der Professoren ist die Investition in *explainable AI*, also erklärbare KI, ein Bereich, in dem nur wenige Anbieter aus Asien und Amerika leistungsfähige Produkte haben. Damit ist die Erklärbarkeit, Nachvollziehbarkeit und die Entwicklung von Eingriffsmöglichkeiten in KI eine Facette, die es - den Daten nach - stärker zu berücksichtigen gilt. Entscheidend im Wettstreit um bessere Produkte und damit eine Marktvorherrschaft könnten bessere Anwendungsszenare mit Hilfe von KI sein. Ein weiterer Investitionsbereich, der genannt wurde, ist der Mobilitätssektor. 27% der Interviewten nennen in diesem Zusammenhang den Einsatz unterstützender Komponenten wie 5G und Cloud. Mit Hilfe

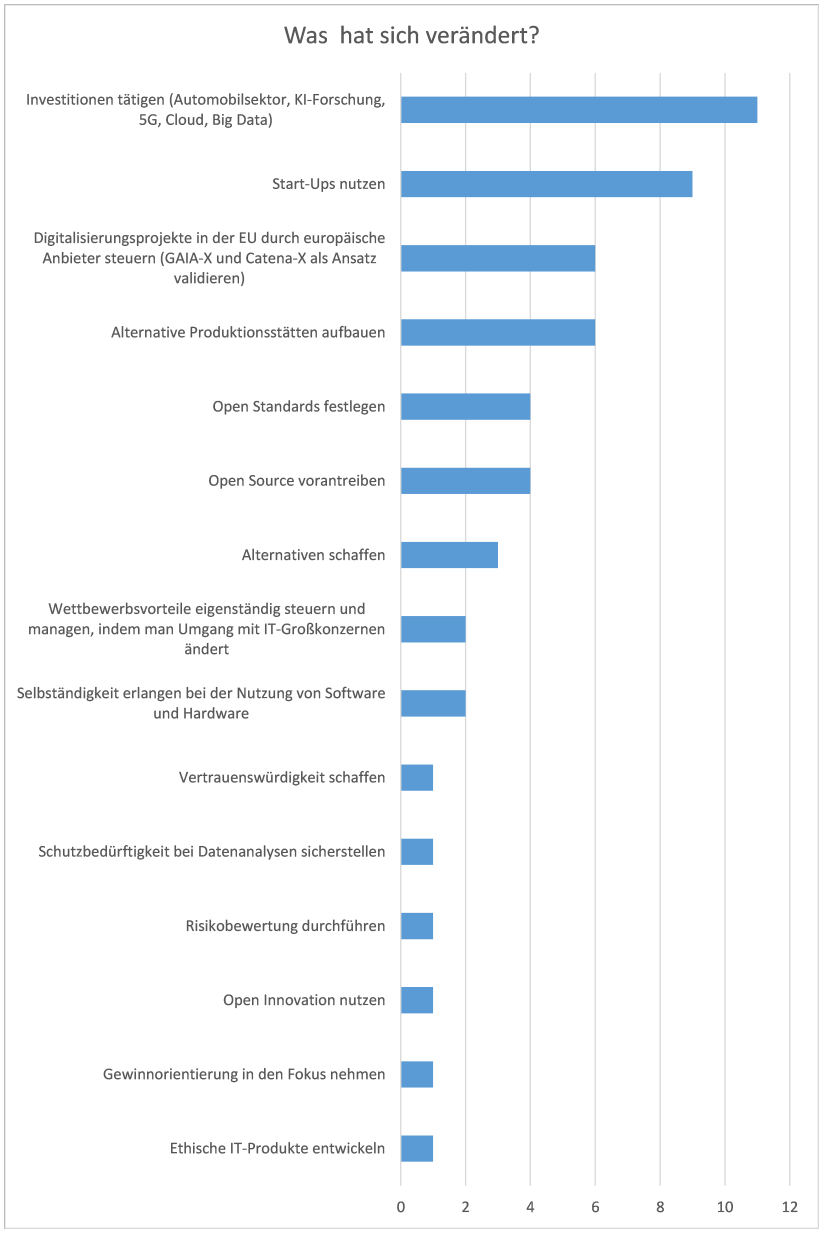


Abbildung 4.10: Neue Faktoren digitaler Souveränität aus Perspektive der Professoren (Bereiche INF, WINF, BWL)

dieser Komponenten glauben die Interviewten eine stärkere technologische Unabhängigkeit in zukunftsweisenden Bereichen erlangen zu können. 9% der Professoren beschreiben wiederrum, dass deutsche Unternehmen derzeit zu wenig Raum nutzen, Dinge, die sie bereits können, umzusetzen. Big Data ist

ebenfalls ein Thema, das laut 9% der Professoren vorangetrieben werden sollte.

Die hier vorliegenden Interviewergebnisse bestätigen die Ergebnisse von Bogenstahl und Zinke (2017), die Investitionen in digitale Technologien als Möglichkeit für Unternehmen sehen, ihre Wertschöpfungskette neu auszurichten und gleichzeitig mehr Souveränität innerhalb der Wertschöpfungskette zu erlangen.

Start-Ups zur Steigerung digitaler Souveränität nutzen Wie der Abbildung 4.10 zu entnehmen ist, äußern 82% (9 von 11) der Professoren, dass sie daran glauben, dass eine Kooperation mit Start-Ups eine Steigerung der digitalen Souveränität in deutschen Unternehmen unterstützen kann. Das ist im Vergleich zu den anderen Faktoren die höchste Anzahl an Äußerungen. So wird von einem der Interviewten betont: „Für mehr Souveränität sind insbesondere diejenigen Start-Ups interessant, die ihre eigenen Ökosysteme schaffen oder ein Subsystem kreieren, nicht die, die Teil eines größeren Ökosystems sind, das durch Unternehmen wie Facebook, Amazon, Google und Apple bestimmt wird." Es bedarf Finanzierungen, Sponsoren und Interessierte, die sich tiefgehend damit auseinandersetzen, wie Start-Ups einen Einfluss auf die digitale Souveränität haben können. 6% der Interviewten äußern wiederum auch, dass es sinnvoll sein könnte, einen Teil der jetzigen Start-Up-Förderung in den Mittelstand fließen zu lassen, und eröffnen damit eine kritische Perspektive auf die Start-Ups. Die Rolle von Start-Ups wird insgesamt von 18% der Interviewten als gering eingestuft, weil sie die Entwicklung komplexer Produkte in den Entwicklungsabteilungen größerer nationaler Unternehmen verorten.

Diese Ergebnisse stehen im Gegensatz zu Friedrichsen und Bisa (2016), die folgende Sichtweise vertreten: „So wie wir jetzt aufgestellt sind, mit 28 zersplitterten nationalen Märkten, wird Europa nie Start-ups hervorbringen, die Google [und] Co einmal Paroli bieten könnten".

Digitalisierungsprojekte in der EU: GAIA X, CATENA X validieren Es ist das Ziel, in den Diskussionen mit den Professoren herauszufinden, ob sie glauben, dass ein europäischer Digitalisierungsansatz dazu führt, dass die digitale Souveränität gestärkt wird. 55% der Interviewten bestätigen. 27% der Interviewten finden, dass die Digitalisierungsprojekte Gaia X und Catena X neu validiert werden sollten, aber weiterhin europaweit gedacht werden muss,

wenn es um großflächige Digitalisierungsvorhaben geht. So wird einerseits in den Interviews darauf hingewiesen, dass es in weiten Teilen sinnvoll ist auf bereits bestehende Technologie zurückzugreifen und Hyperscaler zu nutzen, da dies als eher geringe Abhängigkeit eingeschätzt wird. „Das reine Data Housing scheint eher unproblematisch zu sein. Problematisch wird es erst, wenn man weitere Services nutzt. Und da gibt es Anbieter wie Siemens, die in Deutschland ansässig sind und solche Großprojekte glaubwürdig umsetzen können. Dadurch, dass Gaia-X bereits relativ viel in dem Bereich Modelle aufgebaut hat, kann man sich in verschiedenen Bereichen und Sektoren diesen Modellen anschließen, aber natürlich mit einem gewissen Aufwand und es braucht Kontrollmechanismen", äußert einer der Interviewten.

Eine Revalidierung von den Digitalisierungsprojekten GAIA X und CATENA X ist ein neuer Ansatz, der noch nicht in deutscher oder englischsprachiger Literatur zu digitaler Souveränität zu finden ist.

Alternative Produktionsstätten Um Produktions- und Lieferengpässe im Falle eines Krisenszenars zu umgehen, finden 55% der Interviewten, dass alternative Produktionsstätten eröffnet werden sollten. Dabei sehen die Interviewten eine Verlagerung der Produktion in nähere und vertrauenswürdigere Regionen zeitnah als bedeutsam an, um sich auf mögliche Produktions- und Lieferengpässe vorzubereiten, was auch mit den Ergebnissen von Pohle et al. (2022) einhergeht.

Open Standards und Open Source Jeweils 36% der Professoren sehen open source und open standards als die Grundlage deutscher Wettbewerbsfähigkeit. So auch Autoren wie Biström et al. (2024), Moerel und Timmers (2021) oder Bechara und Lechner (2024). Die Vermutung ist: Wenn man open source nutzt, kann man als Unternehmen unabhängiger von einem spezifischen Player am Markt agieren. In diesem Kontext scheint open access ein wichtiges Element, um verlässlich, sicher und wettbewerbsfähige Software zu bauen. 9% der Befragten weisen darauf hin, dass es utopisch ist zu glauben, dass man alleine digitale Infrastrukturen und Software gut und nachhaltig bauen kann. Um digitale Produkte zu bauen, die sich durchsetzen, braucht es diesen 9% nach open access. Ein Zitat aus der Interviewreihe dazu ist: „Wenn mehrere unabhängig voneinander an derselben Idee forschen, dann verschwenden sie

viel Zeit, weil sie nicht aufeinander Rücksicht nehmen."Das Thema Open Source bringt Vorteile sowie Nachteile mit sich. Die Befragten sehen es als Vorteil an, dass man mit open source, Code nutzen und auf dieser Basis weiterentwickeln kann. Man startet nicht bei nichts. Ein Nachteil ist sicherlich die schwerere Einhaltbarkeit von Sicherheitsstandards und Qualitätsansprüchen. Unternehmen und auch Behörden müssen genauer prüfen, was für Open-Source-Komponenten genutzt worden sind. Würde dies mit Prüfkatalogen oder entsprechenden Prozessen erfolgen, sagen die Befragten, könnte das einen wesentlichen Beitrag zur digitalen Souveränität leisten. Wenn Unternehmen auf open source setzen, entsteht also - im Kontext digitaler Souveränität - die Notwendigkeit, genauere Sicherheitsmechanismen zu implementieren (9%).

Alternativen für mehr Autarkie schaffen 27% der Interviewten finden es wichtig, Alternativen (z.B. durch alternative Produktionsstätten) aufzubauen, um autarker zu werden. Um neue Standorte zu etablieren, ist es jedoch auch eine Frage von Know-How und Patent-Recht. Gleichzeitig zeigen die Diskussionen mit den Interviewten, dass mittelständische Betriebe oft keinen Standortwechsel in europäische Länder bevorzugen, sondern vielmehr im Großraum Asien verbleiben (9%). Anschließend sollten die Professoren darauf antworten, wie deutsche Unternehmen bei einer Invasion Chinas in Taiwan reagieren sollten. Die Interviewten machen deutlich, dass es zielführend wäre, in einem derartigen Szenar, Laptops, Mobiltelefone und E-Autos weiterhin auf nationaler Ebene bauen bzw. verkaufen zu können (73%).

Die Bedeutung der Gestaltung und Implementierung von neuen Alternativen im Markt für die gesamte Volkswirtschaft wird auch bei Floridi (2020) deutlich. Wobei bei seinen Ausführungen noch nicht deutlich wird, wie dies gelingen kann. Damit erweitern die hier vorliegenden Ergebnisse seine Sichtweise.

Wettbewerbsvorteil eigenständig steuern und managen Für 18% der Befragten ist entscheidend, dass die Bundesrepublik in den Ökosystemen einen Wettbewerbsvorteil steuern und managen kann. Um dies erfolgreich zu meistern, geben die Interviewten an, dass man den Umgang mit IT-Großkonzernen wie Google, Amazon, Microsoft, meta, alibaba und Huawei ändern muss.

Dieser Punkt scheint in der Literatur zur digitalen Souveränität umstritten zu sein: Während Kaloudis (2022) eher die Politik in die Verantwortung nimmt,

handeln zu müssen, unterstreicht Metakides (2002), dass eine Mischung aus Industrie, akademischen Akteuren und Individuen für eine bessere Steuerung der digitalen Souveränität einstehen sollte. Bei Pohle (2020) wird eine Mischung von organisatorischen, politischen und individuellen Anstrengungen angestrebt.

Selbstständigkeit erlangen bei Software und Hardware Ebenfalls 18% der Interviewten geben an, dass Unternehmen bei der Nutzung von Software und Hardware mehr Selbstständigkeit erlangen sollten. Dazu ist es den Daten nach notwendig, dass Unternehmen wesentlich mehr Geld in Softwareentwicklung investieren und eine Fehlerkultur etablieren. Um mehr Selbstständigkeit, insbesondere im Bereich der Hardwarebeschaffung, zu erlangen, fordern die Professoren, dass Unternehmen einen Plan für die Beschaffung seltener Rohstoffe haben, die es für die Herstellung digitaler Produkte benötigt.

Diese Ergebnisse finden Parallelen zur wissenschaftlichen Veröffentlichung von Avila Pinto (2018), der für mehr Kontrolle über Daten, Server, Hardware und intellektuelle Ressourcen eintritt.

Die folgenden Faktoren wurden jeweils von 9% der Interviewten genannt:

Vertrauenswürdigkeit Die Interviewten unterscheiden zwischen organisatorischer und technischer Vertrauenswürdigkeit. Bei technischer Vertrauenswürdigkeit ist es hilfreich Kataloge zu haben, damit man mit Hilfe von klaren Merkmalen prüfen kann. Die institutionelle, organisatorische Vertrauenswürdigkeit basiert auf einem unternehmerischen Bauchgefühl und der Frage, mit wem das Unternehmen Handel treiben und ins Geschäft gehen möchte.

Die Erkenntnis, dass Vertrauen ein wichtiger Baustein zur Stärkung digitaler Souveränität ist, spiegelt sich auch in der bestehenden Forschungsliteratur von K. Fritzsche et al. (2022) und Moerel und Timmers (2021) wider.

Schutzbedürftigkeit bei Datenanalysen Die Frage, ob Deutschland bei Datenanalysen mit anderen mithalten kann, sollte stets im Zusammenhang mit der Frage gestellt werden, ob Deutschland dies überhaupt will. Interessant wird der Punkt Schutzbedürftigkeit von Daten, den Interviewten nach, an den Stellen, an denen es einen Drang nach mehr Sicherheit gibt, gleichzeitig der Wille aber ist Schritt halten zu wollen (z.B. beim Thema KI).

In der einschlägigen Fachpublikation, wie der von Moerel und Timmers (2021), lassen sich ähnliche Überlegungen nachvollziehen: Moerel und Timmers

(2021) fordert einen Investitionsboost in Bereiche wie KI und gleichzeitig mehr Arbeit zur Wahrung der Privatsphäre von Nutzern. Eine weitere Forderung von ihm ist die Bewertung von Risikoszenarien, was im Einklang mit den Ergebnissen aus dem nächsten Abschnittes steht:

Risikobewertung vornehmen Unternehmen sollten laut den Befragten eine Risikobewertung vornehmen. Ein Zitat aus den Interviews ist: „Wenn man merkt, ich bin abhängig von Taiwan, dann muss man vor Eintritt einer Krise schauen, dass man diese Abhängigkeit verringert."

Open Innovation Open Innovation wird von den Befragten als bedeutsam angesehen, um Infrastruktur und Wertschöpfung in Deutschland aufrecht zu erhalten. Dabei unterstreichen die Interviewten, dass sie befürchten, dass vereinzelnd Innovationen scheitern, weil der Handlungsspielraum von Unternehmen durch zu viele Verordnungen beschnitten wird. Ziel sollte es daher vielmehr sein, dass Unternehmen Freiheiten erhalten, die sie auf Ideen kommen lassen und ein gesellschaftlicher Diskurs daran angeschlossen wird. Um das Thema digitale Souveränität anzugehen, empfiehlt es sich Experten für IT-Security und Innovation an einen Tisch zu holen.

Diese Resultate liefern neue Denkanstöße.

Gewinnorientierung Folglich geht aus den Interviews Folgendes Vertändnis hervor: „Digitale Souveränität ist nicht ortsgebunden (z.B. in Europa), sondern gewinnorientiert", betont einer der Interviewten. Auf der einen Seite, existieren Unternehmen aus einer Gewinnorientierung heraus. Der Nutzer hingegen ist auf einen Mehrwert fokussiert. Das heißt, den Nutzer interessiert im Zweifel nicht, welche Technologie, Ethik oder Risikoabschätzungen in das digitale Produkt geflossen sind. Das sollte bei der Ausgestaltung digitaler Souveränität Berücksichtigung finden.

Auch dieses Resultat scheint neu zu sein und ist divergent zu den Befunden von Pohle (2020), die argumentieren, dass Überlegungen zur digitalen Souveränität sehr wohl ortsgebunden sein können: nämlich wenn man beginnt, über abgeschottete Internetbereiche zu Zwecken von mehr Regulierung, Schutz und Kontrolle zu diskutieren.

Ethische IT-Produkte Die Debatte rund um das Thema Ethik hat sich geändert, seitdem Menschen, zumindest in der westlichen Welt, sehr

viel stärker auf nachhaltigen, verträglichen Konsum und auch auf emotional angenehme Konsumerfahrungen setzen. Insofern schätzen die Interviewten die Auseinandersetzung mit der Entwicklung ethischer IT-Produkte als Chance für Deutschland ein, da Ethik neuerdings einen wirtschaftlichen Wert hat und eingepreist werden kann. Ethische IT-Produkte könnten damit ein Ermöglicher für mehr digitale Souveränität sein.

Diese Idee zeigt sich auch bei Glasze et al. (2023).

4.3.3.2 Was lässt sich bestätigen?

In Abbildung 4.11 finden sich bestätigende Faktoren wieder. Das heißt, die Abbildung visualisiert diejenigen Faktoren, die auch als Ergebnisse der zweiten Fallstudie hervorgingen.

Partnerschaften neu überdenken 73% der Interviewten glauben, dass die EU mit ihren Unternehmen neue strategische Partnerschaften eingehen muss, um stärkere Handelspositionen aufzubauen und besser auf Krisensituationen vorbereitet zu sein. Dabei wird die EU im Sinne einer Stärkung ihrer digitalen Souveränität eine Entscheidung fällen müssen, ob sie eine strategische



Abbildung 4.11: Bestätigte Faktoren digitaler Souveränität aus Perspektive der Professoren (Bereiche INF, WINF, BWL)

Partnerschaft mit China oder den USA eingehen will. 18% der Interviewten sehen eine stärkere Partnerschaft mit den USA für europäische Unternehmen als richtig an, da die USA von der Rechtsordnung sowie von der Wirtschaftsordnung her der Bundesrepublik ähnlicher sind als die Chinesen. Andererseits geben auch 9% der Interviewten an, dass man versuchen sollte wirtschaftliche Verflechtungen in Richtung China sowie den USA aufrechtzuerhalten. Ebenfalls 9% der Interviewten verweisen auf alternative Partnerschaften über die USA und China hinaus. So könnte Israel ein interessanter strategischer Wirtschaftspartner für Software sein. Israel ist jedoch keineswegs politisch neutral. In Bezug auf Rohstoffe, die es für die Herstellung von Hardware braucht, könnte eine stärkere Zusammenarbeit mit Südamerika von Interesse sein, was jedoch mit stärkerem Kompetenzaufbau einhergeht. Rohstoffhandel betreibt die EU schon jetzt zu großen Teilen mit Afrika, Asien oder Lateinamerika. Ebenfalls 9% der Interviewten sehen Afrika als stärkeren Partner für die Rohstoffgewinnung für Elektrogeräte an. Hier begegnet man jedoch der Herausforderung, dass der afrikanische Rohstoffmarkt bereits stark durch Asien dominiert wird. Nicht nur China bzw. Taiwan, sondern auch Südkorea und Japan sind Zentren für die Chipherstellung und beziehen größtenteils Rohstoffe aus Afrika. Zuletzt verweisen 9% der Interviewten darauf, dass die Entscheidung auf Basis möglicher Preis- und Produktionskosten erfolgen muss, wen man als strategischen Partner wählt. „Es sollte ein geringer Anteil der Wertschöpfung in Deutschland und der EU liegen und dafür ein hoher Anteil über weltweite Zusammenarbeit erfolgen. Aber wir müssen Pläne haben für diese wesentlichen Kernaufgaben, unter anderen mit wem wir kurzfristig unsere kritische Infrastruktur formen können." Die restlichen Interviewten geben keine konkrete Antwort darauf, mit welchen Partnern digitale Souveränität umsetzbar wäre.

Datensouveränität gewährleisten 64% der Interviewten reißen in der Diskussion um mehr digitale Souveränität die Datensouveränität als Themenfeld an. Um Datensouveränität zu gewährleisten, sprechen die Experten verschiedene Dimensionen an: Datensicherheit, Datenschutz, europäische Werte und Zuordnung von Verantwortlichkeiten. Wie auch schon im Abschnitt 4.1.3.3 „(IT-)Sicherheit berücksichtigen" genannt, liegt es den Experten nahe darauf hinzuweisen, dass zu wenig für Datensicherheit getan wird. Entgegen

der Aussagen in dem vorherigen Abschnitt, äußern 9% der Interviewten hier, dass sehr wohl technische Sicherheitswarnungen vor einem konkreten zeithistorischen Hintergrund ausgesprochen werden sollten. Im Abschnitt 4.1.3.3 „Open Standards und Open Source“ wurde bereits deutlichen, dass Open Source ein wesentlicher Faktor sein kann, um digitale Souveränität erfolgreich zu meistern. Bei den Diskussionen rund um das Thema Datensouveränität kritisieren 9% der Interviewten, dass der Datenschutz in Open-Source-Projekten zu sehr untergraben wird. Die Meinungen zum Thema Datenschutz gehen jedoch stark auseinander. Während auf der einen Seite, einige Interviewte darauf plädieren, mehr Maßnahmen wie Synthetisierung, Pseudonymisierung und Anonymisierung einzusetzen, um dem Datenschutz gerecht zu werden (18%), empfindet ein anderer Anteil der Interviewten die Auslegung der Datenschutzgrundverordnung in der EU als zu übergenau (18%). An dieser Stelle wird gesagt, dass Deutschland durch diese Übergenauigkeit Geschwindigkeit verliert, während andere Länder Daten nutzen, digitale Produkte kreieren und im Nachgang prüfen, ob jemand klagt. Ein anderer Interviewter findet, Datenerhebung sollte für ihren Zweck begrenzt werden, trotzdem braucht es eine Lockerung der Vorgaben und damit einen stärkeren Mittelweg, als das nationalstaatliche Logik ist. So stellen 9% der Interviewten fest, dass es wesentlich ist einen Weg zu finden, der den europäischen Werten – u.a. Freiheit und Rechtsstaatlichkeit – entspricht. So heißt es weiterhin von einem der Interviewten, dass „kritische digitale Produkte nicht von Leuten beherrscht werden [sollten], die ihre Einstellung und damit ihr Verhalten ändern können."

Bildungsangebote schaffen „Wir müssen schauen, dass wir in gewissen Kompetenzen im Sinne von Ausbildung und Forschung zumindest kompetitiv sind und mitspielen können.“ 55% der Interviewten finden, dass es mehr Sensibilisierung für digitale Bildung bräuchte. Im Kontext digitaler Souveränität meint dies insbesondere aufgeklärt darüber zu sein, welche Abhängigkeit welche Konsequenz mit sich führen kann. Die Interviewten wurden mit einem Krisenszenar konfrontiert und befragt, welche Konsequenzen eine Einschränkung von Handelswegen für Bürger in Deutschland hervorbringen würde. Die Professoren äußern, dass es einen Plan in Krisensituationen braucht. So sollte konkret am Beispiel Taiwans, gezielte Ausbildung an Universitäten und

Schulen für Wirtschaftsflüchtlinge erfolgen. Wirtschaftsflüchtlinge sollen so gezielt in Qualifikationsbereiche, die man auf dem europäischen Arbeitsmarkt braucht, inkludiert werden.

Nutzung digitaler Fähigkeiten in Deutschland und der EU Laut 45% der Interviewten sollten europäische Unternehmen stärker auf die Stärken der EU setzen, um souveräner zu werden. Projekte wie GAIA-X oder CATENA-X treiben Themengebiete wie Cloud oder Big Data auf Basis europäischer Vorstellungen voran. Außerdem verweisen die Interviewten darauf, dass die EU einen europäischen Weg vorgeben muss. Dieser kann sich in den Bereichen *trusted AI* oder *ethical AI* bewegen, also in Bereichen, in denen es einer stärkeren Reflexion hinsichtlich größerer Transparenz von KI-Anwendungen bedarf (siehe auch Abschnitt 4.1.3.3 „Investitionen (Automobilsektor, KI, 5G, Cloud, Big Data)“). Die größte Stärke Deutschlands, auf die die meisten Interviewten verweisen, ist die Automatisierungstechnik. Um auch in Zukunft in diesem Bereich handlungsfähig zu sein, braucht es den Professoren nach unternehmensübergreifende Prozessveränderungen, Orchestrierungskonzepte für neue Wertschöpfungsketten und den Einsatz von KI- und Cloud-Technologie. Nur 9% der Interviewten glauben, dass der Automobilsektor zukunftsweisend für Deutschland sein wird.

Beschaffung/Lieferketten neu managen „Digitale Souveränität bedeutet ja auch, dass ich digitale Lieferketten absichere.“ In Krisensituationen ist es wichtig, für kritische Produkte weiterhin beschaffen zu können (z.B. Halbleiter), finden 45% der Befragten. Ein kurzfristiger Einbruch der Halbleiterbeschaffung kann starke Auswirkungen auf Deutschland haben. Mittel-, und langfristig, so 9% der Befragten, gilt es diese Auswirkungen zu reduzieren, indem eigene Halbleiterproduktionsstätten aufgebaut werden. Mit dem European Chip Act versucht die Europäische Union bereits dieser Abhängigkeit zu begegnen (Directorate-General-Communication, 2025).

Preis gegenüber Kosten abwägen 36% der Interviewten verweisen darauf, dass digitale Souveränität mit einer Preis- und Kostenabwägung einhergehen muss, denn schlussendlich muss der Endkonsument noch bereit sein, Produkte europäischer Unternehmen zu kaufen. Wenn es irgendwann nicht mehr erschwinglich ist europäische Produkte zu kaufen und der Absatz

nicht mehr da ist, werden europäische Unternehmen zwangsweise nicht in dem internationalen Wettbewerb bestehen können. Das heißt, es kommt darauf an, ob Unternehmen sich die Investition überhaupt leisten können, Maßnahmen zu ergreifen, die zu mehr Unabhängigkeit führen. Denn IT-Sicherheit, Verlässlichkeit und Stabilität wird sicherlich höhere Preise erfordern.

IT-Infrastruktur anpassen Bei digitaler Souveränität geht es darum IT-Infrastrukturen so aufzubauen und einzusetzen, dass Freiheit, Demokratie und Rechtsstaat möglichst gut gewahrt werden: Das findet sich in 36% der Interview-Antworten wieder. Die Interviewten nennen zwei weitere Dimensionen im Rahmen der Diskussion. Einerseits finden sie, dass Voraussetzungen geschafft werden müssen, nicht wie im Ukraine-Konflikt antastbar zu sein. Das heißt, zu gewährleisten, dass digitale Infrastrukturen auch in verschiedenen Krisenszenaren verfügbar sind. Andererseits, sollte Infrastruktur, die die Bundesrepublik oder Unternehmen als kritisch einstufen, einer besonderen Prüfung unterliegen. Es ist im Sinne stärkerer Selbstbestimmung notwendig digitale Komponenten, wenn eine Beschaffung nicht aus Europa möglich ist, aus vertrauenswürdigen Ländern zu beziehen, sofern sie wirksame und günstige Komponenten anbieten können.

Auf Schlüsseltechnologien setzen „Die Frage, auf welche Schlüsseltechnologien Europa setzen sollte, ist eine sehr schwierige, denn es lässt sich nur spekulieren, welche Technologien zukunftsweisend sein könnten". Dennoch soll an dieser Stelle auf drei Technologien verwiesen werden, die die befragten Professoren derzeit im stärkeren Maße erforschen und im Rahmen dieser Erhebung nennen: KI, Quantum und Blockchain. Im Bereich künstlicher Intelligenz sehen die Befragten insbesondere im Bereich Prüfkataloge für überprüfbare KI und die Schaffung von mehr Datensouveränität trotz der Nutzung von KI eine interessante Nische. Gemeinsam mit den Amerikanern sind deutsche Forschende im Bereich Quanten Computer relativ früh mit dabei gewesen, was langfristig zu einem Vorsprung gegenüber anderen Nationen führen könnte. Blockchain als Technologie ist zwar bereits länger schon erforscht, kann aber mit seinen ganz spezifischen Vor- und Nachteilen in bestimmten Sektoren sinnvoll eingesetzt werden. So sehen die Professoren hier insbesondere die Manipulationssicherheit als wesentlichen Vorteil, der beispielsweise im Rahmen der Beschaffung digi-

taler oder kritischer Komponenten eine tragende Rolle spielen kann. 36% der Interviewten empfinden eine Auseinandersetzung mit dem Thema Schlüsseltechnologien als tragend für eine erfolgreiche Stärkung digitaler Souveränität.

Resilienz mitdenken 36% der Interviewten finden es wichtig, Resilienz aufzubauen. Zur Gewährleistung von Resilienz für mehr digitale Souveränität beschreiben die Interviewten, dass es wichtig ist, Hackerangriffe vorzubeugen, Sicherheitswarnungen herauszugeben und einen Plan zu erstellen, wie man IT-Systeme schnell wiederaufgebaut bekommt (siehe Diskussionen zu Resilienz aus Fallstudie 1 und 2). Auch die Resilienz von Lieferketten wird von den Interviewten genannt. Hier gilt es, die richtige Lieferkette für die richtige Situation zu finden - eine Aussage, die durch Fischer und Marshall (1997) geprägt wurde. Schließlich verweisen die Interviewten darauf, dass Resilienz – auf welcher Ebene sie auch ausgetragen wird – kostet und dass jedes Unternehmen für sich individuell entscheiden muss, wie viel es investieren kann und will.

(IT-)Sicherheit berücksichtigen (u.a. Maßnahmen gegen Hackerangriffe) „Das Thema IT-Sicherheit ist ein sehr schwieriges Thema im Kontext digitaler Souveränität", sagt einer der Interviewten. Denn die Ergebnisse zeigen, dass zwar alle Interviewten eine Auseinandersetzung mit dem Thema für die Stärkung digitaler Souveränität als wichtig erachten, es aber in der Art und Weise der Umsetzbarkeit wesentliche Unterschiede in den Meinungen gibt. Während 9% der Interviewten eher ein frühzeitiges Finden von Sicherheitslücken und damit ein Vorbereiten auf eine Konfliktsituation als wichtig erachten, ist es für 18% der Interviewten eine technische Abschottung, die im Vordergrund steht. Viele IT-Strukturen sind an sich auf Offenheit und Durchlässigkeit angelegt (z.B. das Internet). Aber je offener sie sind, desto anfälliger sind sie für Attacken, Sicherheitsrisiken und Hackerangriffe. Besonders im Bereich der kritischen Infrastrukturen argumentiert man stärker mit digitaler Souveränität. Man sagt, IT-Strukturen müssen eben auch abgesteckte, sichere Zonen haben, die dafür sorgen, dass sie von außen nicht attackierbar sind. Zwei weitere Themen, die in den Diskussionen aufkamen, sind Sicherheitswarnungen und Informationssicherheit. Beim Thema Sicherheitswarnungen gibt es Beispiele für gezielte Hackerangriffe aus gewissen Ländern auf europäische Unternehmen, z.B. aus Russland. Jeweils 9% der

Interviewten sagen, man sollte hier vorsichtig sein und keine zu voreiligen politisch-motivierten Schlussfolgerungen ziehen, wie es beispielsweise im Fall Kasperksy im Jahr 2022 durch das BSI der Fall war (Kipker, 2022). Vielmehr sollte man einen Plan haben, wie man IT-Systeme schnell wiederaufgebaut bekommt. Beim Thema Informationssicherheit ist die Hoffnung, dass alle Beteiligten ein gewisses Interesse haben, sich an die Informationssicherheit zu halten. 9% der Interviewten betonen, dass man versuchen sollte zu erreichen, dass alle einen gleichen Informationssicherheitsstandard haben. Um das Thema IT-Sicherheit strategisch anzugehen, empfehlen die Interviewten, Experten zum Thema IT-Sicherheit und Innovation zusammen zu bringen und eine entsprechende Strategie auszuarbeiten, die die genannten Facetten aufgreift.

Forschung fördern Laut 9% der Interviewten sollten Beiträge aus der Forschung, die einen wesentlichen Einfluss auf die digitale Souveränität haben können, ernster genommen werden. Ein konkretes Beispiel, das durch einen Interviewten genannt wird, ist das Papier „Is Google enough? Comparison of an internet search engine with academic library resources“ von Jan Brophy und David Bawden aus dem Jahr 2005 (Brophy & Bawden, 2005).

Nachhaltigkeit berücksichtigen Die Interpretation des Nachhaltigkeitsbegriffs variiert je nach Befragungsgruppe. Während die IT-Berater den Nachhaltigkeitsbegriff eher an Projekt- und Unternehmensziele koppeln, fällt auf, dass bei den Professoren eher der Klimaschutz darunter verstanden wird. 9% der Interviewten betonen, dass das Thema Nachhaltigkeit einen Einfluss auf die digitale Souveränität hat. Denn wenn man unter Nachhaltigkeit den Klimaschutz meint, dann ist er ein Treiber, der ganz unabhängig von Kriegs- oder Krisengefahren dafür sorgt, dass auch lange Transportwege möglicherweise für eine klimabewusste Welt nicht mehr tragbar sind. In diesem Kontext gilt es Pläne zu schaffen und sich unter Berücksichtigung dessen darauf vorzubereiten, dass Knappheiten sehr viel wahrscheinlicher geworden ist, als es in der Vergangenheit der Fall war.

4.3.3.3 Das DISO-A-Modell (Digitale Souveränitätsmodell- Optimierung Academia)

Auf Grundlage der Ergebnisse aus Kapitel 4.3.3.1 und 4.3.3.2 wird das DISO-A-Modell erstellt. Es ist der Abbildung 4.12 zu entnehmen.

4.3.4 Zusammenfassung, Limitationen, Ausblick

Diese Forschung leistet einen Beitrag zum aktuellen Wissensstand, indem Erfahrungen von Professoren aus den Bereichen INF, WINF und BWL in die Debatte rund um digitale Souveränität in Unternehmen einbezogen werden. Professoren sehen im Gegensatz zu IT-Beratern die folgenden Faktoren als wichtig für die Stärkung digitaler Souveränität in Unternehmen: 1) Investitionen (in den Automobilsektor, KI-Forschung, 5G und Big Data), 2) Förderung von Start-ups, 3) Förderung von Digitalisierungsprojekten innerhalb der EU (Validierung von GAIA-X und CATENA-X), 4) Schaffung alternativer Produktionsstandorte (z. B. für die Chipfertigung), 5) Definition offener Standards, 6) Förderung von Open Source und anderen. Diese Studie basiert im Wesentlichen auf Interviews mit Professoren. Damit beruhen die Faktoren auf dem Erfahrungsschatz und den Meinungen dieser Personengruppe.

Als nächster Forschungsschritt folgt nun die Beantwortung der Forschungsfrage 2: Wie kann man digitale Souveränität - auf Basis des neu erlangten Verständnisses - erreichen? Oder anders gefragt: Kann man digitale Souveränität tatsächlich mit den Faktoren des DISO-A-Modells erreichen? Es sind detailliertere Analysen einzelner Faktoren notwendig. Um Klarheit darüber zu gewinnen, was Unternehmen tun können, um die digitale Souveränität zu stärken, wurde eine Auswahl an Themen zusammengestellt, die zur Beantwortung dieser Frage beitragen soll. Konkret sind das folgende Themen:

1. Der Stand der digitalen Souveränität in Unternehmen und die Beziehung zwischen digitaler Souveränität und Schlüsseltechnologien wie künstlicher Intelligenz und Blockchain

2. Die Erhebung von Herausforderungen bei der Umsetzung digitaler Souveränität in Open Source Projekten

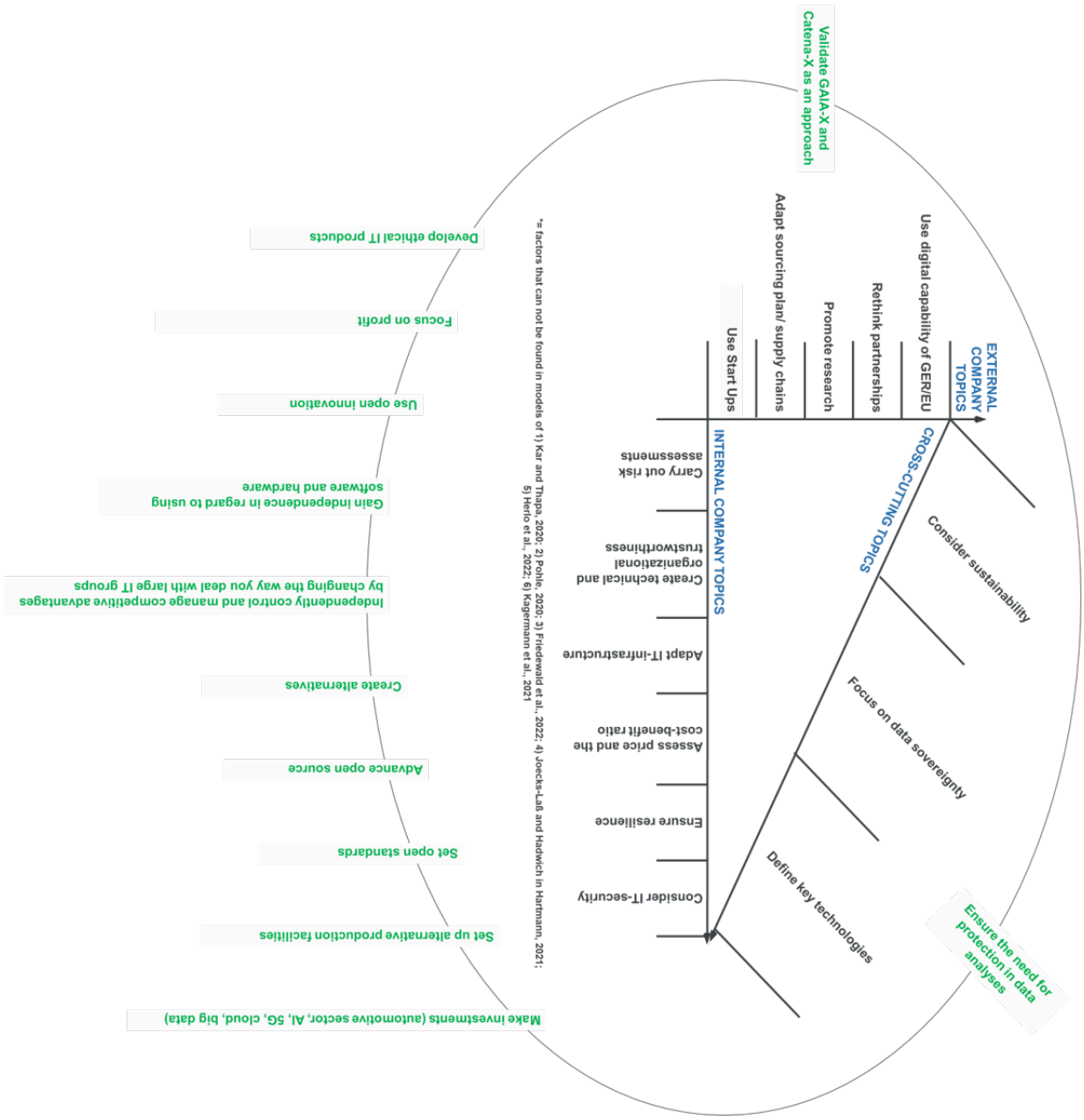


Abbildung 4.12: DISO-A: Digitale Souveränitätsmodell- Optimierung Academia (3. Version)

3. Analyseergebnisse mittels der Affordanztheorie, um strukturell digitale Angebote für mehr digitale Souveränität aufzuzeigen

4. Unternehmensherausforderungen beim Umgang mit digitaler Souveränität und digitaler Transformation im Software-Lebenszyklusprozess verstehen und Mapping der zuvor erlangten Ergebnisse zu digitaler Souveränität als Erweiterung der Norm ISO/IEC/IEEE 12207:2017

5. Architektur-, Management- und Nutzerperspektiven auf souveräne Clouds und Herausforderungen, souveräne Clouds als Ermöglicher digitaler Souveränität zu verstehen

6. Darstellung eines Referenzmodells für Unternehmen, um die digitale Souveränität zu stärken

Dem Abschnitt 4.3.3.1 ist zu entnehmen, dass eine bessere Erklärbarkeit und Eingriffsmöglichkeiten in KI-Systeme eine Facette sein könnte, die es im Kontext digitaler Souveränität genauer zu betrachten gilt. Die Professoren nannten als Schlüsseltechnologien KI und Blockchain. Das führt als nächstes zu dem Forschungsinteresse, diese Schlüsseltechnologien genauer im Zusammenhang mit digitaler Souveränität untersuchen zu wollen.

5

Werkzeuge zur Umsetzung digitaler Souveränität

5.1 Werkzeug Schlüsseltechnologien: Umfrage zum aktuellen Stand digitaler Souveränität in Unternehmen und Implikationen sowie Diskussionen über die Schlüsseltechnologien künstliche Intelligenz und Blockchain

Dieses Kapitel wurde bereits in einer ersten Version hier veröffentlicht: *Klare, M., Verlande, L., Greiner, M. and Lechner, U. (2023). How Blockchain and Artificial Intelligence influence Digital Sovereignty. In: Papadaki, M., Rupino da Cunha, P., Themistocleous, M., Christodoulou, K. (eds) Information Systems. EMCIS 2022. Lecture Notes in Business Information Processing, vol 464. Springer, Cham. https://doi.org/10.1007/978-3-031-30694-5_1.* Dieses Papier ist in Zusammenarbeit mit Lisa Verlande und Maximilian Greiner entstanden. Die Konzeption der Studie erfolgte gemeinsam, so auch die Verschriftlichung der Einleitung, der Methodik und des Anteils theoretische Hintergrund und die Schlussfolgerungen. Ich wandte mich der Akquise von

Umfrageteilnehmern und der Verschriftlichung des Ergebnisabschnitts zu digitaler Souveränität (siehe Abschnitt 5.1.4.1 bis 5.1.4.4) zu.

5.1.1 Einleitung

Wie steht es um die digitale Souveränität in Unternehmen? Können gewisse Schlüsseltechnologien zu mehr digitaler Souveränität führen? Sind sie ein Befähiger oder Hinderer im Kontext digitaler Souveränität?

Geopolitische Spannungen und Fragen hinsichtlich Unabhängigkeit, Vertrauen und Glaubwürdigkeit in Systemen nehmen an Bedeutung zu und tragen dazu bei, dass im Wandel der digitalen Transformation die Berücksichtigung von disruptiven Technologien bei gleichzeitiger Stärkung digitaler Souveränität bedeutsam wird (Friedrichsen & Bisa, 2016). Zwei wachsende Technologien in der Literatur sind Künstliche Intelligenz (KI) und Blockchain (Chatterjee & Chatterjee, 2017; Klare et al., 2022; Lee et al., 2019). Die Interpretation wie mit den genannten Technologien digitale Souveränität gestärkt oder aufgebaut werden kann, bleibt jedoch offen. Konkrete Anforderungen an die Technologien sind bei den vielen politischen und wissenschaftlichen Vorschlägen rar. Forscher im Bereich Wirtschaftsinformatik schlagen beispielsweise Fernauswertungen oder offene Netzwerke für mehr Datensouveränität vor (Bruckner & Howar, 2021; Dalmolen et al., 2020). Unser Ansatz besteht darin, die Auswirkungen von KI und Blockchain auf die digitale Souveränität in Unternehmen und deren Beziehungen kritisch zu untersuchen. Die Verknüpfung der drei Konzepte (digitale Souveränität, KI, Blockchain) leistet einen neuen Beitrag für alle drei Forschungsbereiche. Daher trägt diese Auseinandersetzung zum Wissensstand bei, indem er auf der Grundlage empirischer Daten die Auswirkungen neuer Technologien auf die Stärkung der digitalen Souveränität von Unternehmen beschreibt. Die Verbindung zwischen digitaler Souveränität und KI wird deutlich, wenn man vertrauenswürdige und glaubwürdige KI-Systeme entwickeln will (Vogt, 2021). Blockchain ist aufgrund der Möglichkeit, mit verteilten Autoritäten mehr Manipulationssicherheit gewährleisten zu können, wesentlich im Kontext digitaler Souveränität zu untersuchen (Hinckeldeyn, 2019). Konkrete Maßnahmen für Unternehmen zum Umgang mit digitaler Souveränität bei der Einführung von KI und/oder Blockchain, geben Auskunft

über einen möglichen Einsatz. Es werden diese Forschungsfragen adressiert:

- Wie steht es um die digitale Souveränität in Unternehmen?
- Wie unterstützen KI und Blockchain die Wahrnehmung, digitale Souveränität der Unternehmen stärken zu können?
- Wie kann die digitale Souveränität durch KI und Blockchain gestärkt werden?

Die folgende Analyse soll dazu beizutragen, zu verstehen, wie sich digitale Souveränität auf die Entwicklung und Nutzung von KI und Blockchain auswirkt. Zusätzlich sollen Herausforderungen aufgezeigt werden. Es wird aufgedeckt, inwieweit die Technologien die digitale Souveränität unterstützen. Unser Forschungsinteresse besteht darin verstehen zu wollen, ob diese beiden Technologien einen positiven Einfluss auf die digitale Souveränität haben können.

Das folgende Kapitel ist wie folgt aufgebaut: Es beginnt mit einer Vorstellung von theoretischen Grundlagen; hier werden ausgewählte Schlüsseltechnologien (künstliche Intelligenz und Blockchain) vorgestellt (siehe Abschnitt 5.1.2). Es schließt eine Darstellung der hier verwendeten Methodik an (siehe Abschnitt 5.1.3). In Abschnitt 5.1.4 finden sich die Ergebnisse aus der Umfrage. Das Kapitel schließt mit einer Schlussfolgerung und einem Ausblick unter Abschnitt 5.1.5.

5.1.2 Theoretische Grundlagen

5.1.2.1 Schlüsseltechnologien für digitale Souveränität

Aus Hummert (2023), Peuker (2020), Gräf et al. (2018) geht hervor, dass Schlüsseltechnologien ein Befähiger für mehr digitale Souveränität sein können. Weitere neben den oben genannten Autoren gehen davon aus, dass digitale Souveränität dazu beitragen kann, die digitale Transformation voranzutreiben, indem Staaten, Unternehmen oder Einzelpersonen klären, wie sie Hardware, Software und digitale Fähigkeiten nutzen wollen (Merkel et al., 2021; Philipp, 2022). Im digitalen Sinne bedeutet dies, dass sich Politik, Forschung und Entscheider in Unternehmen verstärkt die Frage stellen sollten, welche technischen, organisatorischen und konzeptionellen Voraussetzungen für

Schlüsseltechnologien notwendig sind, um tatsächlich souveräner zu werden (Die Bundesregierung, 2021). Da sich diese Dissertationsschrift der Forschungsfrage widmet, wie digitale Souveränität für Unternehmen gestärkt werden kann, ist eine Inklusion wesentlicher Schlüsseltechnologien bei der Betrachtung digitaler Souveränität fundamental. Als konkrete Beispiele begrenzt sich die Betrachtung in dieser Arbeit auf die Schlüsseltechnologien KI und Blockchain.

Künstliche Intelligenz Das in dieser Arbeit vorliegende Verständnis von KI ist ein System, das auf der Grundlage von vorhandenen Datenquellen und Algorithmen Entscheidungen treffen und Vorhersagen durchführen kann. Dabei zielen KI-Algorithmen auf die Abbildung folgender menschlicher kognitiver Prozesse ab: Schlussfolgern, Lernen und Reflektieren (Shinde & Shah, 2018). In dieser Arbeit sollen auch Teilbereiche von KI, darunter maschinelles Lernen oder Trainingskonzepte wie Federated Learning, genauer betrachtet werden. Federated Learning ist ein Ansatz des maschinellen Lernens, der im Gegensatz zu herkömmlichen Zentralisierungen den Ansatz einer Dezentralisierung beim Training verwendet und so die Möglichkeit unterstützen will, mehr Datenschutz einzuhalten (Zhang et al., 2021). Ein Einblick in die Bedenken, Hindernisse und die aktuelle Nutzung von KI-Systemen in Unternehmen ist von hoher Bedeutung, um KI-Systeme in einer digital souveränen Weise für die Zukunft zu gestalten. Hierbei ist es entscheidend, die Ziele, die für digitale Souveränität im Zusammenhang mit KI gelten, aufzudecken.

Blockchain Blockchain ist eine Art der Distributed Ledger Technology (Brühl, 2017). Es wird für digitale Transaktionen genutzt und ermöglicht so B2B- und B2C-Unternehmen zunehmend, Handlung auf dem digitalen Markt (Massaro, 2021). Akter et al. (2020) zeigen, dass Blockchain neben seiner bekannten Art als Transaktionsmittel auf dem digitalen Markt auch als Beschleuniger im Rahmen von Geschäftsprozessen in Unternehmen gesehen werden kann. Die Technologie schafft eine Möglichkeit, Fälschungen vorzubeugen und mehr Transparenz zu schaffen (Buhl et al., 2017). In dieser Arbeit ist das Verständnis von Blockchain: Blockchain ist eine technische Lösung, mit der Daten durch vertrauenswürdige und nachvollziehbare Prozesse sowie einer dezentralen Instanz fälschungssicher verwaltet werden können (Carayannis et al., 2022). Dabei sind für diese Arbeit insbesondere folgende Vorteile einer Blockchain

wesentlich: 1) eine eindeutige Sicht auf ein Ereignis, 2) Toleranz gegenüber Ausfällen in Knoten, 3) überprüfbare Aktivitäten und 4) Kontrolle über Dateneigentum (Christidis & Devetsikiotis, 2016). Angesichts dieser Vorteile ist von einer soliden Verbindung zu digitaler Souveränität auszugehen, da Fragen der Autorität, des Vertrauens, der Transparenz, des Eigentums und der Ethik auch bei digitaler Souveränität eine besondere Rolle spielen. Wie skizziert, birgt der Bereich Blockchain und digitale Souveränität erhebliches Forschungspotenzial. Um die aktuelle Situation zu verstehen und Annahmen abzuleiten, ist es entscheidend, die jüngsten Entwicklungen, den Stand der Technologie und die möglichen Auswirkungen auf die digitale Souveränität zu untersuchen.

5.1.3 Methodik

Die Analyse in diesem Kapitel ist geprägt von der Methode von Rea und Parker (2014), die einen Leitfaden zur Erstellung von Umfragen entwickelt hat. Der für diese Umfrage verwendete Leitfaden kann dem Anhang entnommen werden (vgl. Abbildung 39 bis 51, Anhang). Im Rahmen der Studie werden folgende Schritte umgesetzt: 1) Zielgruppe bestimmen, 2) Fragebögen erstellen, 3) Pretests durchführen, 4) Daten erheben und 5) Daten analysieren. Die Umfrage ist in deutscher Sprache formuliert und besteht aus geschlossenen sowie halboffenen Fragen. Filter-Fragen dienen dazu, dass die Teilnehmer der Umfrage ausschließlich die Fragen beantworten, mit denen sie am meisten vertraut sind. Zusätzlich werden Multiple-Choice-Optionen sowie eindimensionale Skalen vorgegeben. Die Teilnehmer für die Umfrage wurden teilweise aus dem eigenen persönlichen Netzwerk akquiriert, zu großen Teilen aber durch soziale Netzwerke gewonnen. Die Datenerhebung erfolgte im Zeitraum zwischen Juli und August 2022. Die Umfrage richtet sich an Entscheidungsträger in Deutschland und wurde in deutscher Sprache durchgeführt. Insgesamt konnten 163 Datensätze, davon 134 vollständig ausgefüllte Datensätze, erhoben werden. 77 der Datensätze stammen aus Großunternehmen und 57 aus kleinen oder mittelständischen Unternehmen, unter Berücksichtigung einer Fehlerquote von 10%. In Anlehnung an Müller-Böling und Klandt (1996) werden die Daten zunächst statisch ausgewertet. Die Bildung von Clustern hilft dabei, Ähnlichkeiten zu kommunizieren, und Netzwerkdiagramme bieten

eine anschauliche Darstellung. Danach schließt eine Detailanalyse an.

5.1.4 Ergebnisse

Aufgrund des Neuheitsgrads des Themas digitale Souveränität, ist ein Anliegen dieser Studie, den Bekanntheitsgrad in deutschen Unternehmen zu ermitteln. Mit Hilfe der Umfragedaten wird ersichtlich, welche Maßnahmen Entscheider in Unternehmen bereits ergriffen haben, um digitale Souveränität zu stärken.

5.1.4.1 Gegenwärtiger Stand in deutschen Unternehmen hinsichtlich digitaler Souveränität

Den Umfrageergebnisse nach setzen sich Unternehmen mit der Idee der digitalen Souveränität auseinander, denn 79% der Befragten ist das Thema bekannt. Während 48% ihr Unternehmen als stark oder sehr stark digital souverän beschreiben würden, äußern 44% der Befragten, dass ihr Unternehmen kaum oder gar nicht digital souverän ist (vgl. Abbildung 5.1). Unter Berücksichtigung einer 8%-Enthaltungsquote ergibt sich eine relativ ausgeglichene Masse an Umfrageteilnehmern, die ihr Unternehmen souverän oder nicht souverän einschätzen.

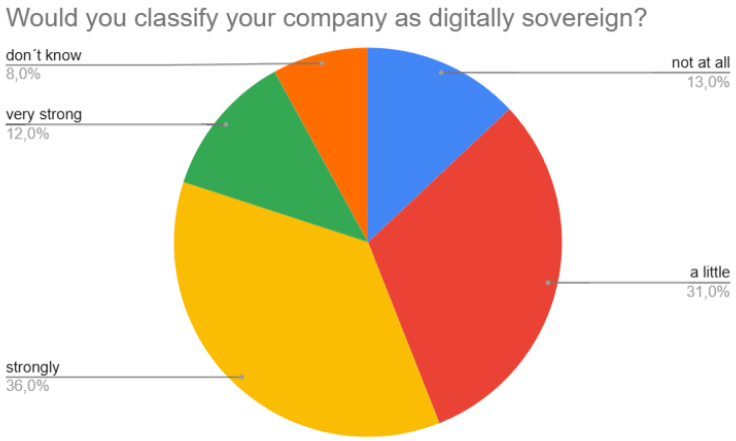


Abbildung 5.1: Einstufung der Unternehmen hinsichtich digitaler Souveränität

Das Interesse an dem Konzept der digitalen Souveränität ist bei 67% der Befragten stark bis sehr stark ausgeprägt (siehe Abbildung 5.2). 60% der Befragten geben an, dass die Bedeutung des Themas für ihr Unternehmen hoch bis sehr hoch ist. 51% der Befragten haben sich bereits mit digitaler

Souveränität befasst und 58% empfinden es als wichtig sich auch in Zukunft ein wenig, viel oder sehr viel mit dem Thema digitale Souveränität zu befassen.

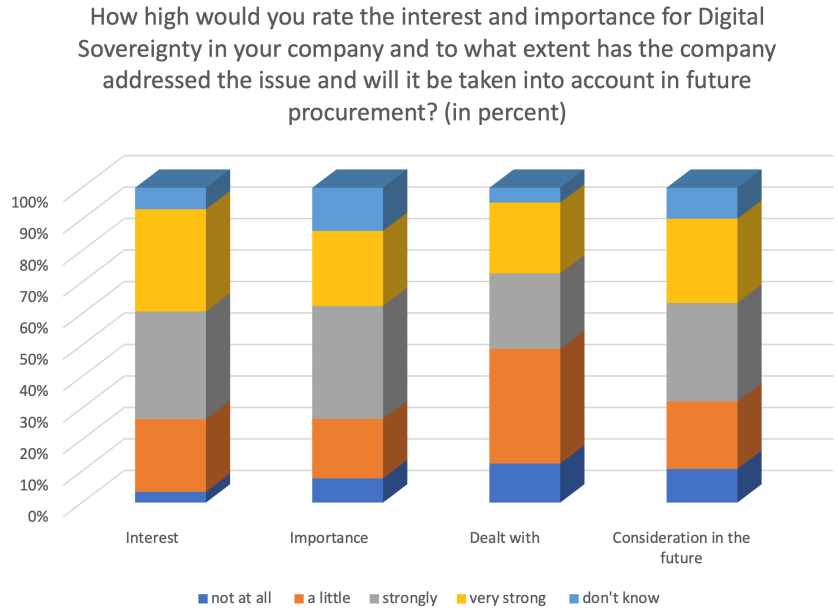


Abbildung 5.2: Interesse für digitale Souveränität, Bedeutung des Themas und Abhängigkeiten

Die nächste Frage an die Entscheider zielte darauf ab, wie der Stand der digitalen Souveränität des Unternehmens im Vergleich zum Wettbewerb ist. Die Ergebnisse zeigen, dass sich die Mehrheit der Entscheider im Mittelfeld einordnen. Die Entscheider wurden gefragt, welche Bereiche in ihrem Unternehmen digital souverän sind. Es wird deutlich, dass den Entscheidern nicht klar ist, wo in ihrem Unternehmen digitale Souveränität eine Rolle spielt und warum.

5.1.4.2 Zwei Gruppen: Unternehmen mit niedriger Souveränität vs. Unternehmen mit hoher Souveränität

Anhand ihrer Selbsteinschätzung zur digitalen Souveränität konnten die Befragten in zwei Gruppen aufgeteilt werden. Während sich in Gruppe 1 die Befragten eher als digital unsouverän einschätzen, ist Gruppe 2 durch eine hohe digitale Souveränität gekennzeichnet. Auffallend ist, dass Gruppe 2 ihre Systeme (31%), Verantwortlichkeiten (31%) und die Transparenz (14%) in ihrem Unternehmen als Gründe dafür sehen, während in Gruppe 1 eine niedrige Da-

tensouveränität (84%) als Kernproblem angesehen wird (vgl. Abbildung 5.3).

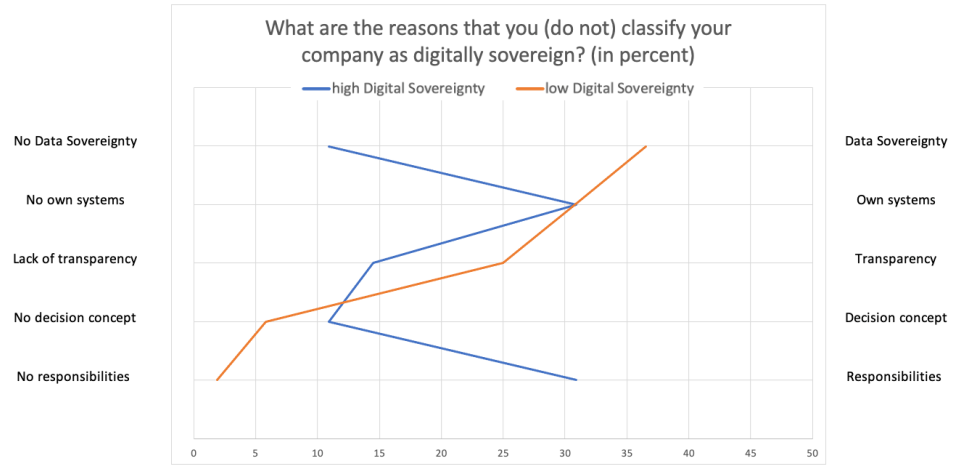


Abbildung 5.3: Gründe, weswegen sich Unternehmen (nicht) digital souverän einstufen

Die Ergebnisse der Gruppe 2 stehen im Einklang mit denen von Blossfeld et al. (2018). Sie finden heraus, dass die richtigen Technologien, Mitarbeiter und Prozesse ausschlaggebend für die Stärkung digitaler Souveränität sind.

5.1.4.3 Erkenntnisse aus der Vergangenheit und Empfehlungen für zukünftige Maßnahmen

Die Befragten aus der Gruppe 2 (hohe digitale Souveränität) sollten beantworten, welche Maßnahmen ihr Unternehmen bereits zur Stärkung von digitaler Souveränität eingesetzt hat (vgl. Abbildung 5.4). 30% der Befragten geben an, dass herstellerunabhängige Module in der Vergangenheit genutzt wurden. 26% wählen aus, dass IT-Lösungen eingesetzt wurden und 13%, dass eine Strategie entwickelt wurde. Eine erhebliche Zahl der Befragten gibt jedoch auch an, dass ihr Unternehmen bei der Beschaffung nicht auf digitale Souveränität achtet (63%).

Als nächstes wurden die Befragten aufgefordert zu beantworten, mit welchen Mitteln sie glauben, dass digitale Souveränität gestärkt werden kann. Dabei konnten sie zwischen Mitteln unterscheiden, die in der Vergangenheit und in der Zukunft umgesetzt werden sollen. Die meisten Befragten sehen das Thema Datensouveränität als sehr wichtig an, um digitale Souveränität zu stärken

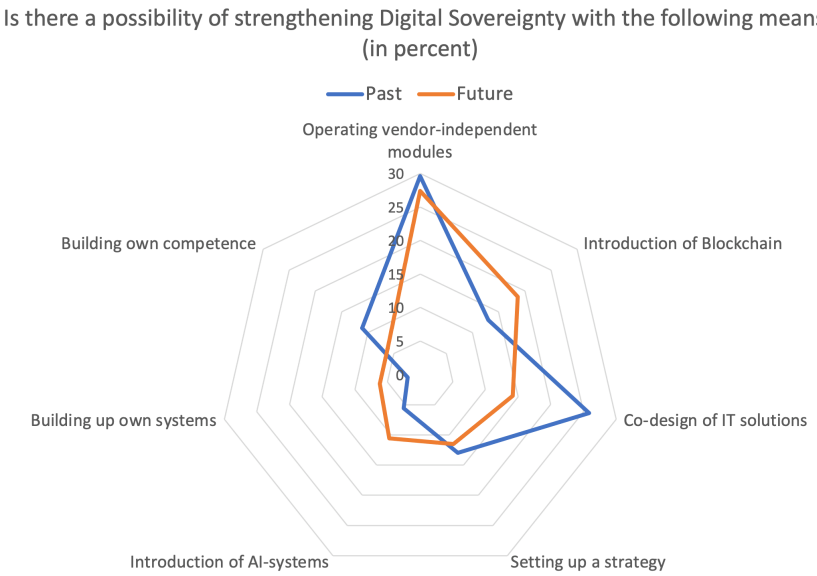


Abbildung 5.4: Maßnahmen, um digitale Souveränität zu stärken

(89%). Nach Meinung der Befragten sollte mehr Datenkontrolle erlangt werden. Immerhin 34% der Befragten sehen Forschung und Entwicklung als hilfreich an. In Zukunft sollten nach 27% der Befragten herstellerunabhängige Module eingesetzt werden, um mehr digitale Souveränität zu erreichen. Mit 6 mehr Prozentpunkten gegenüber der Vergangenheit scheint Blockchain ein Mittel zu sein, das in Zukunft genauer in Erwägung gezogen werden sollte. Die Befragten geben auch der KI als Mittel 5%-Punkte mehr als in der Vergangenheit. *Federated Learning* wird als Alternative von den meisten Befragten als positiver Ansatz zur Stärkung der digitalen Souveränität gesehen. Nur 10% verneinten, dass *Federated Learning* gegenüber klassischen KI-Systemen helfen würde. 13% der Befragten glauben, dass eine Strategie ihnen in Zukunft helfen wird, das Thema digitale Souveränität zu verstehen. Nach Ansicht der Befragten sind Herausforderungen bei der Stärkung digitaler Souveränität die IT-Infrastruktur, Informationsdefizite und fehlende Zuständigkeiten als auch die Finanzierung. Darüber hinaus sollten die Befragten beantworten, welche Erwartungen sie an die Politik haben. 34% nennen die Förderung von Forschung und Entwicklung, 22% die Unterstützung bei der Gewährleistung von mehr Interoperabilität und 13% die Entwicklung einer deutschen Daten-

strategie, die Unternehmen als Orientierung dienen soll. 12% der Befragten fordern auch eine stärkere Zusammenarbeit zwischen den einzelnen EU-Mitgliedsstaaten, 10% die Schaffung von mehr Bildungsmöglichkeiten und 5% die Entwicklung einer Open-Source-Strategie. Diese Ergebnisse bestätigen die zuvor beschriebenen Ausführungen aus dem DISO-A-Modell (vgl. Kapitel 4.3).

5.1.4.4 Erweiterung des Verständnisses von digitaler Souveränität

Das Verständnis digitaler Souveränität anderer Forscher wird durch unsere Umfrageergebnisse verifiziert. Die Ergebnisse liefern jedoch auch neue Erkenntnisse, die zuvor nicht im DISO-A-Modell visualisiert wurden, zum Beispiel die Daten-Compliance. Unsere Umfrageergebnisse stützten die Einschätzung von Weber (2022), die mehr Führung und Compliance durch das Management fordern, um digitale Souveränität zu stärken. 70% der Befragten sehen Compliance als einen Schlüsselfaktor für eine erfolgreiche Integration digitaler Souveränität. Faktoren wie Unabhängigkeit bei der Wahl von IT-Systemen und –Produkten und die Gewinnung von mehr Entscheidungsfreiheit lassen sich aus dem DISO-A-Modell bestätigen. Laut 77% der Befragten ist die Unabhängigkeit bei der Wahl von IT-Systemen und –Produkten sehr wichtig für mehr digitale Souveränität. Pohle (2020) sehen ebenfalls die Unabhängigkeit bei der Wahl von IT als zentrales Element für mehr digitale Souveränität. In dem DISO-A-Modell wurde es sogar als übergeordnetes Thema aufgenommen. Viele Befragten (88%) sehen Entscheidungsfreiheit als einen wichtigen Faktor für digitale Souveränität, was zeigt, dass die Einschätzungen von Kagermann (2021) bestätigt werden können, die Entscheidungsfreiheit als politisches Ziel bei der Adressierung digitaler Souveränität mehr Gewicht zuschreiben. Auch unternehmensspezifische Faktoren spielen eine Rolle bei digitaler Souveränität. 77% der Befragten finden, dass unternehmensinterne IT-Architekturen transparenter gestaltet werden sollten und 58%, dass die Zusammenarbeit mit Unternehmen bevorzugt werden sollte, die ein ähnliches Werteversprechen haben. Ähnlich viele Befragte (57%) äußern, dass die Quellcodes in ihrem Unternehmen nicht hinreichend zugänglich sind.

5.1.4.5 Künstliche Intelligenz und Blockchain: mögliche Schlüsseltechnologien für digitale Souveränität?

In diesem Kapitel werden die Anwendbarkeit, der Zweck und die Eigenschaften der beiden Technologien KI und Blockchain dargestellt. Die Befragten wurden gefragt, ob sie glauben, dass die Technologien die digitale Souveränität unterstützen und inwieweit ihr Unternehmen mit diesen Technologien arbeitet.

Einsatz künstlicher Intelligenz in Unternehmen Wie die Ergebnisse zeigen, ist KI vielen Befragten bekannt, aber das Verständnis darüber, wie die Technologie genau funktioniert, ist mangelhaft. Interessanterweise sagen 75% der Befragten, dass sie gar nichts oder nur wenig über KI wissen, obwohl die Technologie bereits in vielen alltäglichen Bereichen Anwendung findet. Die bekanntesten Anwendungen sind laut unseren Ergebnissen intelligente KI-Systeme (25%), Sprachsteuerungssysteme (15%) und Texterkennungssysteme (13%). 60% sind in ihrer Arbeit mit KI konfrontiert. 39% haben bereits KI-Projekte umgesetzt und 21% befinden sich in der Planungsphase. Außerdem wurden auch die Gründe für ein Scheitern von KI und Blockchain untersucht. Obwohl die Technologien in unterschiedlichen Bereichen eingesetzt werden und sehr unterschiedlichen Zwecken dienen, ergibt sich ein nahezu gleiches Bild bei den Antworten darauf, warum die Technologien scheitern (vgl. Abbildung 5.4).

Einsatz von Blockchain in Unternehmen Ein hoher Anteil der Befragten gibt in der Umfrage an, dass sie schlecht über Blockchain informiert sind (74%). Folgende Umfrageergebnisse können mit dem Bekanntheitsgrad in Verbindung gebracht werden: 33% der Befragten sagen, dass es geplante oder bereits umgesetzte Projekte in Unternehmen gibt. 30% hingegen kennen den Status der Blockchain-Projekte in ihrem Unternehmen nicht. Die restlichen 11% haben keine Aussage getroffen. Folgende Anwendungen auf Basis der Blockchain-Technologie werden am häufigsten in Unternehmen angewandt: 21% Zertifikatsmanagement, 19% Kryptowährung, 16% Sensordaten. Die Vorteile von Blockchain werden darüber hinaus in folgenden Bereichen gesehen: 15% nennen die Dezentralisierung bei Informationsspeicherung, weitere 15% die Ausfallsicherheit, 25% die Manipulationssicherheit und 28% die Unveränderbarkeit der Daten. Wie oben ersichtlich, ist das Interesse an den Technologien von KI und Blockchain sehr hoch. Der häufigste Grund für das Scheitern ist laut der Befrag-

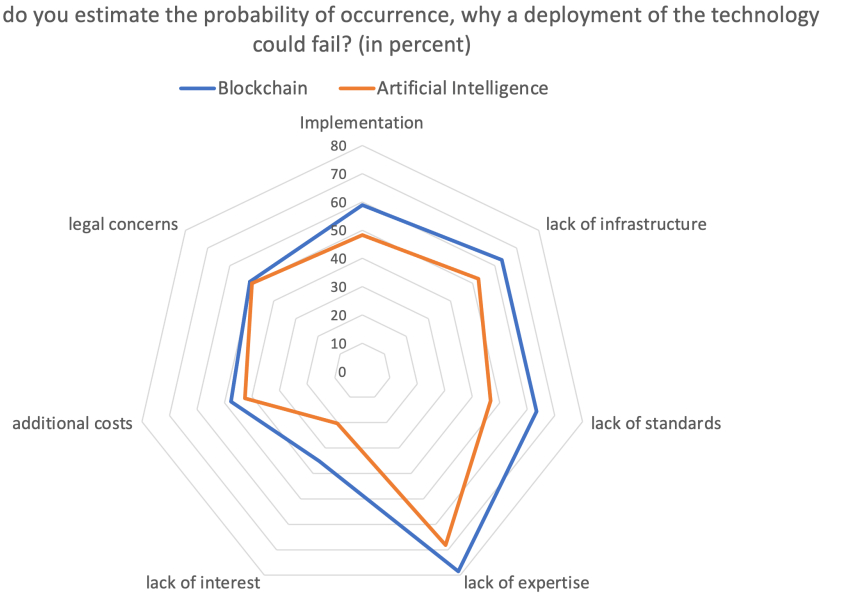


Abbildung 5.5: Wahrscheinlichkeit und Gründe, dass eine der Technologien scheitert

ten mangelndes Fachwissen (79%). Weitere Gründe sind fehlende Standards (62%), alte IT-Infrastrukturen (62%), Fragen hinsichtlich der Implementierung (60%), rechtliche Bedenken (51%) und hohe zusätzliche Kosten (49%).

Digitale Souveränität ist ein strategisches Ziel. Den Daten nach liegt eine Notwendigkeit vor, förderliches Lernen als Ersatz für klassische KI-Systeme und Blockchain als Technologie anzugehen, um auf dieses strategische Ziel hinzuarbeiten.

Die folgenden sieben Maßnahmen aus Abbildung 5.6 zielen auf die Entwicklung einer strategischen Vision digitaler Souveränität auf Basis der Umfrageergebnisse ab. Zur Untermauerung dieser Maßnahmen wurden die erhobenen Daten mit dieser Forschungsgruppe in zwei Workshops analysiert. Die erste Runde diente der Sammlung von Maßnahmen und die zweite Runde dem Abgleich und einer Verfeinerung. Dabei ergab die Datenanalyse, dass die folgenden Maßnahmen für zukünftige Ansätze relevant sind (vgl. Abbildung 5.6).

1. Datensouveränität vorantreiben Unsere Datenanalyse zeigte, dass mehr Datensouveränität ein grundlegendes Ziel für die Befragten ist, um digitale Souveränität zu stärken (vgl. Abbildung 5.3). Mit Hilfe von *Federated Learning*

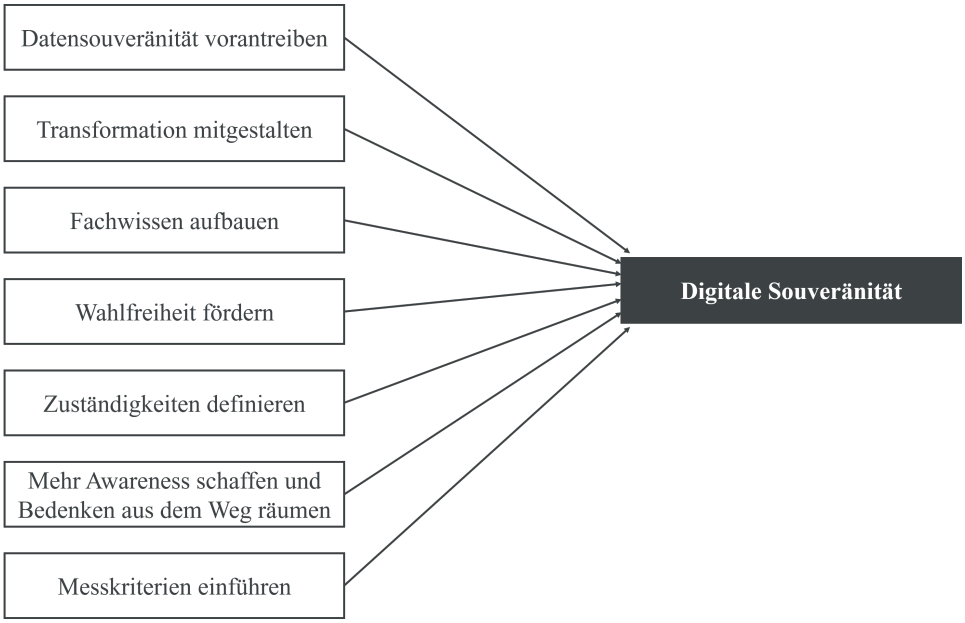


Abbildung 5.6: Maßnahmen zur Entwicklung einer Vision für digitale Souveränität

kann mittels eines dezentralen, neuen Ansatzes ein Modell verwendet werden, das die Privatsphäre von Nutzern schützt (McMahan et al., 2017). Um die Datensouveränität voranzutreiben, können sich über 90% der Befragten vorstellen, *Federated Learning* einzusetzen und so die Datenteilung im Sinne des Datenschutzes einzuschränken (vgl. Abschnitt 5.1.4.5). Auch die Blockchain-Technologie kann verwendet werden, um die Datensouveränität voranzutreiben. Aufgrund der Möglichkeit Daten dezentralisiert und ausfallsicher zu speichern, kann mehr Kontrolle über die eigenen Daten gewährleistet werden (Fill et al., 2020; Meinel et al., 2018). So ist die Blockchain-Technologie prädestiniert dafür digitale Souveränität voranzutreiben. Unsere Umfrageergebnisse zeigten, dass der Großteil der Befragten die Unveränderbarkeit und Manipulationssicherheit der Daten schätzen (vgl. Abschnitt 5.1.4.5). Gleichzeitig ist die Schaffung von mehr Transparenz ein weiterer Vorteil, der durch Blockchain erreicht werden kann (Sunny et al., 2020). Somit kann die Blockchain-Technologie dazu beitragen, ein souveräneres und sichereres Unternehmen zu schaffen. Lu et al. (2019) verweisen darauf, dass auch die digitale Kommunikation durch die Nutzung einer Blockchain-Technologie in Verbindung mit KI sicherer

gestaltet werden kann. Somit kann die Verbindung beider Technologien einen nicht unerheblichen Effekt auf die Datensouveränität von Unternehmen haben (Lu et al., 2019).

2. Transformation mitgestalten Wie Pohle (2020), Blossfeld et al. (2018) und Wittpahl (2018) zeigen ist das Interesse für digitale Souveränität als Basis für die Meisterung der digitalen Transformation groß. Dabei wird in unterschiedlicher Literatur (Friedrichsen und Bisa (2016), Wittpahl (2018) und Pohle (2020)) darauf hingewiesen, dass die Unternehmensführung die Aufgabe einnehmen muss, eine Weiterentwicklung zu fördern. Den Umfrageergebnissen nach wird Co-Design von IT-Lösungen nicht als Mittel zur Stärkung digitaler Souveränität in der Zukunft angesehen, aber als erfolgversprechend in der Vergangenheit (vgl. Abbildung 5.4). Diese unterschiedliche Bewertung des Mittels könnte darauf zurückzuführen sein, dass 21% der Befragten ein schlechtes Verständnis von digitaler Souveränität haben (vgl. Abschnitt 5.1.4.1). Hier wurde die gesamte Befragungsgruppe befragt; in der Vergangenheit jedoch nur diejenigen Personen, die zuvor angaben, dass bereits Projekte im Zusammenhang mit digitaler Souveränität in ihrem Unternehmen umgesetzt worden waren. Technologien wie KI (insbesondere in diesem Zusammenhang *Federated Learning*) und Blockchain können die digitale Transformation unterstützen, indem sie das Know-How in der Organisation wahren (siehe Abschnitt 5.1.4.5). Insbesondere unter Berücksichtigung des Fachkräftemangels ist die Bündelung von Wissen ein wesentlicher Baustein für die digitale Transformation (Anding, 2018) sowie die Gewährleistung von mehr digitaler Souveränität (Pohle, 2020). Darüber hinaus sind Governance-Ansätze in Unternehmen, das Aufbrechen alter Strukturen, die Ausrichtung auf neue Wege, die Gewährleistung von Rollen und die Einführung von Prozessen entscheidend (Manita et al., 2020; Martens & Zscheischler, 2022). Dies steht entgegen der Argumentation von Dreo et al. (2020), der die Gewährleistung einer stärkeren Autarkie zur Stärkung digitaler Souveränität als wesentlich ansieht.

3. Fachwissen ausbauen Wie in der Datenanalyse dargestellt, ist ein wesentliches Hindernis fehlendes Fachwissen und fehlende Expertise (vgl. Abbildung 5.4). Fachkräfte sollten somit sensibilisiert und auf die Veränderung vorbereitet werden. Neben der Erstellung einer Souveränitätsstrategie sollten

Ausbildungs- und Weiterbildungsmaßnahmen in Angriff genommen werden. Die Managementebene sollte Mitarbeiter ermutigen, Offenheit zu fördern und Anreize zu schaffen, sich in Forschung und Entwicklung zu engagieren, um neue Ideen zu verwirklichen. Auch gegenüber externen Partnern ist eine offene Kommunikationsstrategie zu wählen. Dies unterstreicht auch die Ergebnisse aus dem DISO-A-Modell (vgl. Kapitel 4.3). Bestätigt werden können insbesondere die Äußerungen hinsichtlich Forschung und Entwicklung, der Souveränitätsstrategie und die Prozess-Überlegungen.

4. Wahlfreiheit fördern Wahlfreiheit bei der Wahl von IT-Systemen, -Produkten und Dienstleistungen ist ein wichtiges Kernelement der digitalen Souveränität (Pohle et al., 2022). Unternehmen sollten ihre Wahlfreiheit weiterhin wahren. Wie die Befragten angaben, sollten Unternehmen Einschränkungen bei der Wahlfreiheit wahrnehmen und zu starke Monopol-Stellungen als mögliche Hindernisse für die Stärkung digitaler Souveränität verstehen (vgl. Abschnitt 5.1.4.3). KI-Systeme, die mittels *Federated Learning* trainiert werden und Blockchain nutzen, leisten einen wesentlichen Beitrag zur Erreichung von mehr Flexibilität, Interkonnektivität zwischen Diensten und zur Gewinnung von mehr Autonomie (vgl. Abschnitt 5.1.4.5). So scheint eine Integration von KI und Blockchain von wesentlicher Bedeutung für die digitale Souveränität zu sein und kann als Befähiger gesehen werden.

5. Zuständigkeiten definieren Für die Befragten, die ihr Unternehmen als sehr digital souverän einschätzen, ist die Definition klarer Zuständigkeiten bedeutsam, um digitale Souveränität zu stärken. Weill und Ross (2004) stellen ebenfalls fest, dass Governance-Ansätze, die mit der Entwicklung von Entscheidungskonzepten und der Schaffung von Rollen und Verantwortlichkeiten einhergehen, entscheidend für ein erfolgreiches Unternehmen sind. Auf diese Weise sollten Informationsdefizite reduziert werden, die in den Ergebnissen als Hindernis für eine erfolgreiche Integration von KI und Blockchain identifiziert wurden (vgl. Abbildung 5.5).

6. Mehr Awareness schaffen und Bedenken aus dem Weg räumen Den Daten zufolge ist ein klareres Bild erforderlich, was digitale Souveränität ist und wie sie umgesetzt werden kann (vgl. Abschnitt 5.1.4.1). Demnach scheint es bedeutsam zu sein, mehr Awareness für das Thema zu schaffen und Bedenken

bezüglich des Konzepts auszuräumen. Ein klareres Bild über die Ziele digitaler Souveränität und die Integrationsmöglichkeiten in Unternehmen ist notwendig. Diese Umfrageergebnisse zeigten, dass einerseits über 50% der Befragten angaben, dass sie ihr Unternehmen als digital souverän bezeichnen würden. Andererseits geben die meisten Befragten ebenfalls an, dass sie mit dem Thema nicht vertraut sind (vgl. Abschnitt 5.1.4.1). An dieser Stelle wird eine Diskrepanz deutlich, die darauf schließen lässt, dass die Befragten ein sehr unterschiedliches Bild davon haben, was sie unter digitaler Souveränität verstehen und wie eine Integration des Konzeptes in deutschen Unternehmen gelingen kann. Die Daten untermauern die Einschätzung, dass auch mehr Awareness für die Technologien KI und Blockchain geschaffen werden muss: So stellt man fest, dass 75% der Befragten wenig oder gar nichts über KI wissen, obwohl KI bereits Anwendung im täglichen Leben findet. 74% der Befragten geben an, dass sie schlecht über das Thema Blockchain informiert sind (vgl. Abschnitt 5.1.4.5). Die Bereitstellung von Schulungen für Mitarbeiter in Unternehmen kann einen Beitrag leisten, um das Verständnis für die jeweiligen Themen zu steigern und einer erfolgreichen Integration entgegenzuwirken.
7. Messkriterien einführen Eine weitere Maßnahme ist die Einführung von Messkriterien für digitale Souveränität. Wie in 4.4.3.3 deutlich wird, wird das Konzept der digitalen Souveränität auf politischer Ebene überströmt. Es braucht mehr kontrollierbare und messbare Kriterien für Unternehmen. Aus betriebswirtschaftlicher Sicht sollte die Umsetzung digitaler Souveränität erleichtert werden, indem mehr Messansätze die Zielerreichung quantifizieren. Es war zu sehen, dass keiner der Befragten angibt, dass solche Messkriterien bereits in ihrem Unternehmen Anwendung findet, wobei diese explizit bei Kaloudis (2022) gefordert werden.

5.1.5 Zusammenfassung, Limitationen, Ausblick

Auf Basis der vorliegenden Umfrage sind KI und Blockchain zwei Technologien, die laut den befragten Unternehmen zur Stärkung digitaler Souveränität beitragen können. Die Ergebnisse zu den Auswirkungen von KI und Blockchain auf digitale Souveränität erweitern den bestehenden Wissensstand, indem sie sowohl unternehmerische als auch technologische Anforderungen an die

Stärkung digitaler Souveränität liefern. Aus einem Vergleich zwischen den Umfrageergebnissen und der bestehenden Literatur zu digitaler Souveränität konnten folgende Maßnahmen formuliert werden, die als Empfehlung auf Basis der Datenlage zu verstehen sind: Erstens ist das Thema Datensouveränität in Unternehmen zu klären und damit zusammenhängend mehr Kontrolle über Daten zurückzugewinnen sowie die Privatsphäre der Nutzer zu schützen. Hierbei kann vor allem Federated Learning als Konzept einen entscheidenden Beitrag leisten. Die Umfrageergebnisse unterstreichen, dass auch die Blockchain das Potenzial hat, mehr Datensouveränität zu erreichen. Zweitens sollte die Managementebene ihre Mitarbeiter für das Thema digitale Souveränität sensibilisieren. Drittens sind Verantwortlichkeiten mit Rollen zu koppeln, um sich viertens im Rahmen geeigneter Prozesse neu auszurichten. Fünftens sollte das Know-How bei den Themen digitale Souveränität, KI und Blockchain mittels Schulungen gestärkt werden. Sechstens ist es wichtig, das Bewusstsein zu steigern und Bedenken auszuräumen. Und siebtens sollten betriebswirtschaftliche Messkriterien eingeführt werden, um eine Orientierung für Unternehmen im Kontext digitaler Souveränität zu bieten und eine Zielerreichung besser messbar zu machen. Zusammenfassend sollten diese Ziele alle darauf ausgerichtet sein, eine Strategie für digitale Souveränität zu entwickeln, die auf die unternehmensspezifischen Risiken ausgerichtet ist.

Insbesondere die Messkriterien für digitale Souveränität und die Erstellung eines strategischen Plans für Unternehmen sind Ansätze, die anhand von Designstudien konkreter analysiert und validiert werden sollten.

Das nächste Kapitel widmet sich dem Thema Open Source. Open Source ist eine Facette, die im DISO-A-Modell ebenfalls als wesentlicher Treiber zur erfolgreichen Umsetzung digitaler Souveränität, identifiziert wurde. Die angehende Forschung unterliegt dem Interesse, verstehen zu wollen, ob Open Source tatsächlich dieses Potenzial hat.

5.2 Werkzeug Open Source: Gap-, und Affordanzanalyse zu Herausforderungen digitaler Souveränität in Open Source Projekten

Eine erste Version dieses Kapitels wurde bereits hier veröffentlicht: *Klare, M., and Lechner, U. (2025). Digital Sovereignty: Affordances in Open Source Projects. In E. Papatheocharous, S. Farshidi, S. Jansen and S. Hyrynsalmi (Hrsg.), Software Business (pp. 20–34). https://doi.org/https://doi.org/10.1007/978-3-031-85849-9_2.*

5.2.1 Einleitung

In dieser Arbeit ist es ein Ziel, der Frage nachzugehen, ob Open Source tatsächlich zu mehr digitaler Souveränität beitragen kann. Andere Autoren fordern von Unternehmen, dass diese Treiber von Open Source sind und die Politik lediglich Rahmenbedingungen schafft (Burgfried & Reckert-Lodde, 2022; Farrand & Carrapico, 2022). So stellt sich die Frage, ob dies ein gangbarer Weg für Unternehmen ist, mit welchen Herausforderungen sie konfrontiert sind und wie man den Herausforderungen begegnen kann, um einer erfolgreichen Transformation entgegenzuwirken. Somit sind in diesem Kapitel - in Abgrenzung zu anderen Fachartikeln (Glasze et al., 2022; Kagermann, 2021) - praktische Ansätze aus der Wirtschaft und damit aus den Unternehmen heraus fokussiert worden, um einen Weg zur Erreichung digitaler Souveränität, verknüpft mit Open Source Zielen, zu beschreiben. Um einen stärkeren Einblick in die organisatorische Umsetzung digitaler Souveränität zu gewinnen, sollen in dieser Studie zwei erfolgreich durchgeführte Open Source Projekte analysiert werden, die einerseits auf Basis von Kubernetes und andererseits mit Hilfe des matrix communication protocols umgesetzt wurden.

Folgende Forschungsfragen werden adressiert:

- Was sind die Herausforderungen in Entwicklungsteams bei der Nutzung von Open Source, um die digitale Souveränität zu stärken?
- Wie können Affordanzen in Open Source Projekten verändert werden, um mehr digitale Souveränität zu erlangen?

Zur Beantwortung dieser Forschungsfragen werden Ergebnisse aus einer

Retrospektive, Anforderungen der Projekte, die Architekturen, Prozesse, Qualitätsmerkmale und schließlich die Affordanzen analysiert.

In Kapitel 5.2.2 wird die theoretische Grundlage für dieses Kapitel gelegt: unter anderem wird die Affordanz-Theorie eingeführt. Kapitel 5.2.2.4 bis 5.2.2.7 ist zu entnehmen, wie Anforderungen, Architekturen, Prozesse und Qualität in diesem Kapitel modelliert werden sollen. Eine detaillierte Beschreibung des Forschungsdesigns findet sich anschließend in Kapitel 5.2.3, bevor in Kapitel 5.2.4 und 5.2.5 die Analyseergebnisse der beiden Projekte (Informationssteckbrief und Messenger) vorgestellt werden. Nach einer Darstellung von Ergebnissen aus der Ist-Analyse (Kapitel 5.2.4 und 5.2.5), der Soll-Analyse (Kapitel 5.2.6) und der Gap-Analyse (Kapitel 5.2.7 und 5.2.8) können Affordanzen abgeleitet und Empfehlungen zur Anpassung dieser Affordanzen gegeben werden (Kapitel 5.2.10). Den Schluss bildet eine Beschreibung von Limitationen und ein Ausblick für weiterführende Forschung (Kapitel 5.2.11).

5.2.2 Theoretische Grundlagen

Da zur Erhebung von Daten aus den Projektteams eine Retrospektive durchgeführt wird, wird die Retrospektive in diesem Kapitel als Begriff eingeführt. Zudem wird geklärt, wie die Affordanztheorie zu Zwecken der Analyse in dieser Arbeit verwendet werden soll.

5.2.2.1 Retrospektive

Im Rahmen von agilen Projektarbeiten versteht man unter einer Retrospektive einen Termin, der genutzt wird, um die Vergangenheit zu reflektieren (Andresen, 2017; Derby et al., 2006). In dieser Arbeit wird die Methode der Retrospektive verwendet, um einen Blick auf die vergangene Projektarbeit zu werfen und aus ihr zu lernen. Laurent (2004) schlagen als Alternative zu klassischen, leitfadengestützten Interviews vor, sogenannte retrospektive Interviews zur Erhebung von Fachwissen bei Experten zu verwenden. Vorteil dieser Methode sieht Laurent (2004) in der Möglichkeit, mit Retrospektiven die Leistung der Projektteams auf eine andere Weise zu untersuchen. Mit Hilfe der Aussagen der Projektmitarbeiter kann durch eine Retrospektive herausgefunden werden, warum Dinge von den Erwartungen abwichen oder welche Dinge in der Vergangenheit gut gelaufen sind (Kerth, 2013; Laurent, 2004).

5.2.2.2 Affordanz-Theorie und digitale Souveränität

James Gibson analysierte erstmals 1986, wie ein Objekt von verschiedenen Lebewesen unterschiedlich wahrgenommen und genutzt werden kann. Seine Definition: *„Die Affordanzen der Umgebung sind das, was sie dem Tier bietet, was sie bereitstellt oder liefert, sei es zum Guten oder zum Schlechten“* (Gibson, 1977). In der Psychologie, aus der der Begriff *Affordanz* stammt, wird er zunehmend als die Möglichkeit verstanden, Handlungen anhand von Objekten in der Umwelt wahrzunehmen (Jones, 2018).

In der Wirtschaftsinformatik wurde das Konzept weiterentwickelt. Es wird genutzt, um das Nutzerverhalten bei der Verwendung technischer Objekte zu analysieren oder Handlungen im Zusammenspiel von Anwender, Technik und Kontext (Fromm et al., 2020). Dadurch verfestigt sich das Verständnis, dass informationstechnische Objekte Hinweise darauf geben, wie sie verwendet werden sollen und dass Affordanzen die Wirkung von IT-Artefakten auf Organisationen, Prozesse und Nutzerverhalten beeinflussen. Volkoff und Strong (2017) zeigen auf, wie die Affordanztheorie in der Wirtschaftsinformatik-Forschung genutzt werden kann: Sie definieren Affordanzen als handlungsanbietende Merkmale, die eine Wechselwirkung zwischen einem Objekt und Akteuren ermöglichen können. In dieser Arbeit ist unter einem *Objekt* ein technisches Objekt oder eine wirtschaftliche Dienstleistung zu verstehen und unter *Akteur* ein Akteur in einem Unternehmen.

Affordanzen werden häufig mit Funktionen verwechselt, können aber auch Einschränkungen darstellen (Volkoff & Strong, 2017). Affordanzen - im Verständnis dieser Arbeit - sind jedoch keine isolierten Handlungsmöglichkeiten, sondern ein integraler Bestandteil von Handlungen (Leonardi, 2023). An der Schnittstelle zwischen Mensch, Maschine und Institutionen entstehen Affordanzen, die sowohl förderlich als auch hemmend oder einschränkend sein können. Die Affordanztheorie ist für diese Forschung entscheidend, da sie Handlungsspielräume im Kontext digitaler Souveränität sowie IT-bezogener und organisatorischer Veränderungen erklärt. Digitale Souveränität meint die Fähigkeit, selbstbestimmt, sicher und unabhängig im digitalen Raum agieren zu können. Um herauszufinden, wie Affordanzen angepasst werden müssen, um die digitale Souveränität zu stärken, ist es notwendig, die Herausforderungen

und Risiken von Open Source im Hinblick auf die Souveränitätsziele zu verstehen. Um die Affordanztheorie im Kontext digitaler Souveränität anzuwenden, ist es notwendig, relevante Aspekte einer IT-Strategie in die Betrachtungsweise zu inkludieren. Ziel ist es also, IT-Affordanzen in Open-Source-Projekten zu identifizieren und zu verstehen, wie diese angepasst werden müssen, um IT-Strategien zu stärken und so Ableitungen für digitale Souveränität treffen zu können. So helfen Affordanzen dabei zu analysieren, welche Technologien digitale Souveränität behindern oder ermöglichen. Affordanzen können auch genutzt werden, um zu untersuchen, welche wirtschaftlichen Dienstleistungen förderlich oder hemmend für die Autonomie sind. Beispiel: Open Source affordiert mehr Kontrolle, benötigt aber gewisse Fähigkeiten.

5.2.2.3 Anforderungen, Architekturen, Prozesse und Qualität im Zusammenhang mit digitaler Souveränität

Architekturen und Prozesse sind wesentliche Leitplanken für Unternehmen, um digitale Souveränität zu erreichen. Diese Sichtweise ist in dieser Arbeit besonders dann notwendig, wenn genauer analysiert wird, wie man Software digital souverän bauen kann. Die folgenden Abschnitte liefern eine Definition für Anforderungen, Architekturen, Prozesse und Qualität. Es gibt verschiedene Arten, wie Anforderungen, Architekturen, Prozesse und Qualität modelliert werden können. Aus diesem Grund wird zusätzlich festgelegt, welche Art der Modellierung gewählt wird und warum.

5.2.2.4 Anforderungsmodelle

Was versteht man unter einer Anforderung? Unter einer Anforderung versteht man nach DIN 610.12-1990 eine Bedingung, die ein User benötigt, die ein System erfüllen soll oder eine Dokumentation dieser Bedingung (IEEE, 1990). Nach Pretschner et al. (2007) versteht man unter einer Anforderung, eine Eigenschaft, die ein Produkt, ein Prozess oder ein System erbringen soll. Die Kombination dieser beiden Definitionen soll das Verständnis einer Anforderung in dieser Dissertationsschrift sein.

Wie modelliert man Anforderungen? Es gibt unterschiedliche Arten, wie man Anforderungen modellieren kann. Eine Art der Modellierung ist die klassenbasierte Modellierung (Balzert, 2009). Bei klassenbasierten Modellierun-

gen ist eine der bekanntesten Formen der Methodik die Anforderungsanalyse (Németh, 1992). Eine andere Art der Modellierung ist die strömungsorientierte Modellierung (Mandl & Fischer, 2000).

Abbildung 5.7 zeigt eine agile, strömungsorientierte Modellierung: diese basiert in diesem Beispiel auf den Bausteinen *Requirement*, *Epic*, *User Story* und *Test*. In der agilen Softwareentwicklung verwendet man *Agile Requirements Engineering*, um Kundenanforderungen darzustellen (Rubin & Rubin, 2011). Hierzu überführt man die Anforderungen in Epics (in Aufgaben, die zu groß sind, um sie in einem zu erledigen) (Pashchenko, 2024). Ein Epic ist eine Anforderung auf einem hohen Abstraktionsniveau, das analog des Scrum Guides formuliert wird (Opt & Sims, 2015). Eine detailliertere Beschreibung der Anforderung inkl. der Funktionalitäten erfolgt gemäß dem Scrum Guide in der User Story (deutsch: Anwender-Geschichte) (Bolloju et al., 2017). Im Rahmen des Tests wird formuliert, wie der Entwickler die Anforderung technisch umsetzen will (Genaid et al., 2012).

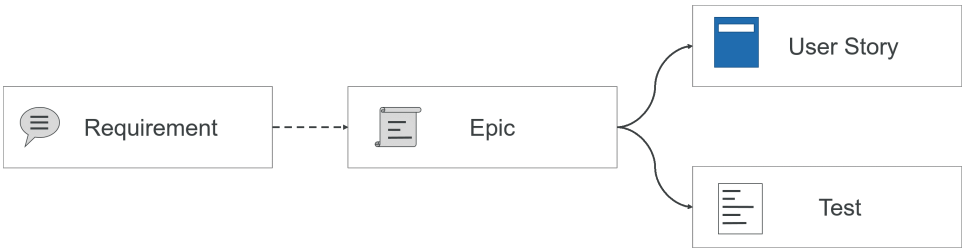


Abbildung 5.7: Ein Beispiel für eine agile Anforderungsmodellierung (Agile Requirements Modeling)

Es ist ein anschauliches Abbild der Realität, auf die strömungsorientierte Modellierung zurückzugreifen, dabei jedoch agile Prinzipien zu berücksichtigen, da in dieser Arbeit agile Projekte analysiert werden. Im Regelfall werden Technologien, Funktionalitäten und Komponenten in einem präferierten Tool dargestellt. Ist ein Software-Modell fertiggestellt, so wird geprüft, inwieweit das Modell den Anforderungen *Einfachheit*, *Widerverwendbarkeit* und *flexible Anpassbarkeit* genügt (Starke, 2020). Bei der Notation der Anforderungen wird auf die Software-Anwendung Git-Mind zurückgegriffen.

5.2.2.5 Architekturmodelle

Was versteht man unter einer Architektur? In der Informatik spricht man von einer Architektur, wenn die Zusammensetzung und das Zusammenwirken verschiedener Bestandteile von informationstechnischen Systemen dargestellt werden sollen (Vogel et al., 2011). Man modelliert Software oder Services mit Architekturen (Richter et al., 2005).

Wie modelliert man Architekturen? Bei der Architekturmodellierung unterscheidet man zwischen dem klassischen Architekturvorgehen und dem agilen (Szvetits & Zdun, 2016). Beim klassischen Architekturvorgehen ist die Entkopplung von Funktionalität und Technologie ein wesentlicher Schritt, um eine solide Modellierung aufzusetzen (Dustdar et al., 2023). Beim agilen Architekturvorgehen geht man iterativ und inkrementell vor (Gundelsweiler et al., 2004). Es finden agile Architekturrollen sowie Stakeholder einen Platz (Toth & Vigenschow, 2013). Mit der gleichen Argumentation wie zuvor (Analyse von agilen Projekten ist der Fokus dieses Kapitels), erfolgt die Entscheidung für die agile Architekturmodellierung.

5.2.2.6 Prozessmodelle

Was versteht man unter einem Prozess? In Unternehmen spricht man nach DIN 9001: 2015 von Prozessen, sobald man eine logische Abfolge von Aktivitäten mit einem Wert als Ergebnis erhält, das ein spezielles Ziel hat (Brugger-Gebhardt, 2016).

Wie modelliert man Prozesse? Man kann Prozesse unterschiedlich modellieren. Bei der Prozessmodellierung unterschiedet man zwischen dem Wasserfallmodell (Royce, 1987), das eine Folge von Aktivitäten als sequenzielle Gliederung vorsieht oder einem ergebnisorientierten Phasenmodell (Nohe, 1999), bei dem man sich in der Modellierung an Meilensteinen, also Zeitabschnitten und Phasen, abarbeitet, um eine Folge zu erzeugen. Bei dem sogenannten Spiralmodell sind die Modellierungsschritte am Risiko orientiert (B. Boehm, 1986; B. W. Boehm, 1988). Es ergibt sich eine zyklische, spiralähnliche Abfolge. Anders beim Wachstumsmodell. Hier werden nacheinander Lieferschritte modelliert. Es zeigt sich, dass sich zunehmend zwei Standards in der Prozessmodellierung durchsetzen. Das eine ist der BPMN-Standard (Chinosi

& Trombetta, 2012). BPMN ist eine standardisierte Notation, die es ermöglicht Zusammenhänge zwischen Geschäftstransaktionen und Leistungszusammenarbeit im Rahmen der Geschäftsabläufe zu modellieren. Durch die standardisierte Art und Weise der Modellierung ist eine vereinfachte Kommunikation des Inhalts möglich. Das Ziel von BPMN ist es, dass Stakeholder die Geschäfte gut verstehen und sie ihre internen Geschäftsbedingungen schnell anpassen können. Dem gegenüber steht die Modellierung von agilen, schlanken oder in manchen Fällen auch leichtgewichtigen Prozessen, die der zunehmend aufstrebenden agilen Software-Entwicklung entstammt (Grund, 2013). Die BPMN-Notation scheint sinnvoll für diese Arbeit, da sich diese Art der Modellierung als Quasi-Standard durchgesetzt hat. Nichts desto trotz ist es notwendig, die Prinzipien agiler Prozessmodellierung in den agilen Entwicklungsteams zu berücksichtigen, dabei vor allem *Einfachheit*, *Schlankheit* und *Verständlichkeit*.

5.2.2.7 Softwarequalitätsmodelle

Was versteht man unter Softwarequalität? Der Begriff Softwarequalität bezieht sich auf die Anforderungen, die als erforderliche Voraussetzungen erfüllt sein müssen, um festzustellen, wie geeignet ein Merkmal für den Wert eines Softwareprodukts ist (Balzert, 1998). In der ISO 9126 sind Qualitätskriterien für Software definiert. Darunter fallen Merkmale wie *Anwendbarkeit*, *Effizienz*, *Funktionalität*, aber auch *Zuverlässigkeit*, *Übertragbarkeit* und *Benutzbarkeit* der Software.

Wie modelliert man Softwarequalitätsmodelle? Man verwendet Qualitätsmodelle, um den Begriff der Softwarequalität zu detaillieren und zu operationalisieren. Cavano und McCall (1978) legen drei Schichten für die Modellierung von Qualität fest. Diese Schichten bestehen aus 1) Faktoren, 2) Kriterien und 3) Metriken/Merkmalen (vgl. Abbildung 5.8).

Modellierungsansätze wie die von Seffah et al. (2001) sehen vier Schichten vor. Neben den im Modell von Cavano und McCall (1978) genannten Schichten (Faktoren, Kriterien, Metriken/Merkmale), sehen die Autoren noch Indikatoren (z.B. Daten) als notwendige Modellierungsschicht an (Seffah et al., 2001).

Um in diesem Buch ein besseres Verständnis darüber zu gewinnen, welche Herausforderungen es bei der Einhaltung von Softwarequalität gibt, ist es

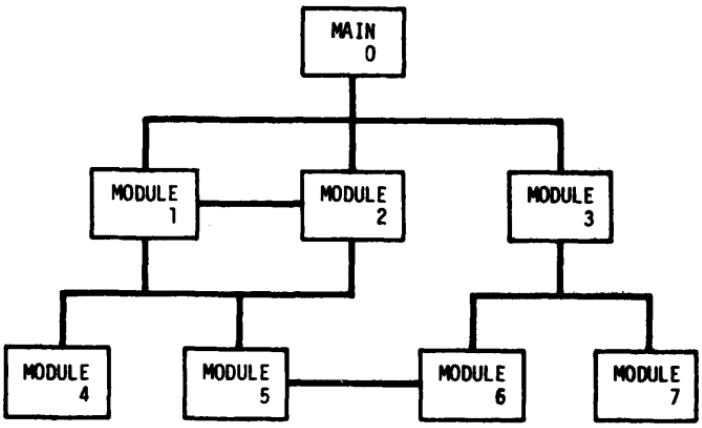


Abbildung 5.8: Ebenen für Qualitätsmodelle (Cavano und McCall, 1978)

bedeutsam, die Qualität von Softwareentwicklung mit digitaler Souveränität zu koppeln. Hierzu soll sich an Seffah et al. (2001) orientiert werden.

5.2.3 Forschungsdesign

Die zentrale Methode dieser Arbeit ist die Gap-Analyse (vgl. Abbildung 4.10). Eine Gap-Analyse basiert auf einem Vergleich zwischen Ist- und Soll-Situation (Jennings, 2000; Kim & Ji, 2018).

Während in dieser Studie die Ist-Situation durch Online-Retrospektiven mit Projektteams repräsentiert wird, sind im Soll-Zustand Ziele und Anforderungen an digitale Souveränität in Anlehnung an die Herausforderungen erhoben worden. In der darauffolgenden Gap-Analyse wird auf die Affordanztheorie zurückgegriffen, um zu zeigen, welche Affordanzen innerhalb der erfolgreich durchgeführten Open Source Projekte „Messenger" und „Informationssteckbrief' angenommen wurden und wie die Affordanzen angepasst werden müssen, um digitale Souveränität zu stärken. Die Analyse orientiert sich an Volkoff und Strong (2013), die die Affordanztheorie als Analyseinstrument in der Wirtschaftsinformatik beschreiben.

Die Daten wurden zwischen Oktober 2023 und Januar 2024 erhoben und die Retrospektiven mit Mitarbeitern aus Projektteams in Deutschland durchgeführt. Es wurde besonders Wert darauf gelegt, zwei Projekte zu finden, die einen Zusammenhang zu digitaler Souveränität haben. Bei den zwei Projekten

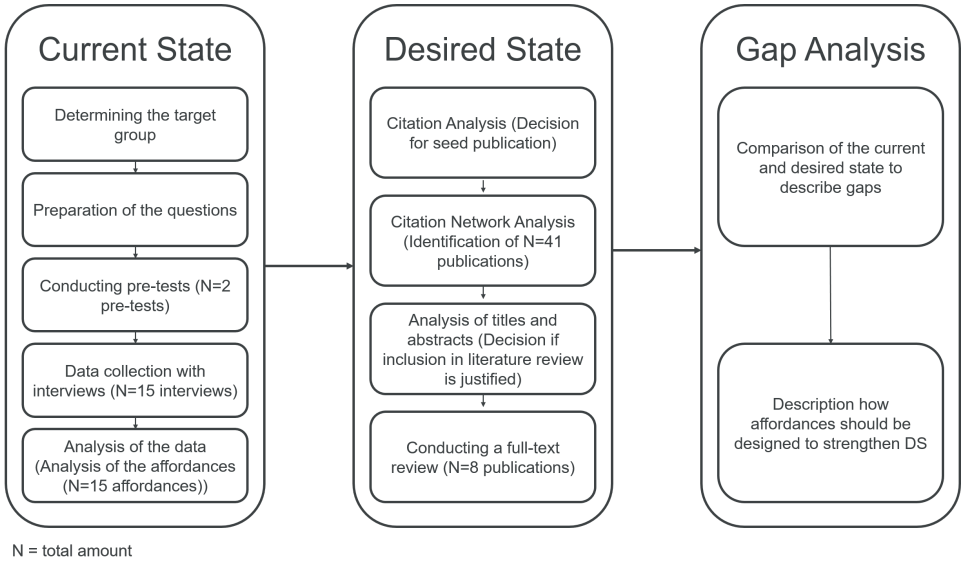


Abbildung 5.9: Forschungsdesign für die Gap-Analyse

handelt es sich um öffentliche Bundes-Projekte, die aus einer Motivation entstanden sind, unabhängiger von amerikanischen Anbietern zu sein und eine eigene, sichere Lösung bereitzustellen.

Nr.	**Rolle**
Interview 1	Projektleitung
Interview 2	Product Ownerin
Interview 3	Scrum Master
Interview 4	Data Engineer
Interview 5	BackEnd Entwicklerin
Interview 6	FrontEnd-Entwickler
Interview 7	Consultant

Tabelle 5.1: Teilnehmer an der Retrospektive (Projekt: Informationssteckbrief)

Wie in Tabelle 5.1 dargestellt, konnten mit den Projektmitarbeitern des Projekts „Informationssteckbrief“ eine Retrospektive mit der Projektleitung, zwei Entwicklern, dem Product Owner, dem Scrum Master und einem Consultant

durchgeführt werden. Auch im Projekt „Messenger“ war eine Retrospektive mit einem Teil des Projektteams möglich. Akquiriert werden konnten hier: die Product Ownerin, ein Scrum Master, ein IT-Architekt und fünf Entwickler (vgl. Tabelle 5.2).

Nr.	Rolle
Interview 1	Product Ownerin
Interview 2	Scrum Master
Interview 3	IT-Architekt
Interview 4	DevOps Engineer & Entwickler
Interview 5	Geo Information System-Expert & Entwickler
Interview 6	Frontend-Entwickler
Interview 7	Backend-Entwickler
Interview 8	Backend-Entwickler

Tabelle 5.2: Teilnehmer an der Retrospektive (Projekt: Messenger)

Die Personen wurden teilweise in Einzelterminen, teilweise in Gruppenterminen von etwa einer Stunde interviewt. Im Rahmen dieser Termine wurden für die beiden Projekte die gleichen Fragen gestellt, um eine Vergleichbarkeit der Ergebnisse zu erzielen (siehe Anhang). So dienten folgende Fragen als Basis für die Retrospektive: I. Was ist die Historie des Projektes? II. Welche Erfahrungen mit Open Source zur Vermeidung von Vendor-Lock-Ins gab es? II. a) Was würdest du mehr tun? II. b) Was würdest du weiterhin so tun? II. c) Was würdest du aufhören zu tun? II. d) Womit würdest du nun anfangen? II. e) Wovon würdest du weniger tun?

Es werden Anforderungen, Architekturen, Prozesse und Qualitätsmerkmale als Basis für weiterführende Analysen modelliert. Es ist sinnvoll, Anforderungen, Architektur, Prozesse und Qualitätsmerkmale von Projekten zu analysieren, um digitale Souveränität fundiert zu untersuchen, weil diese Aspekte zentrale Einflussfaktoren für Unternehmen sind.

5.2.4 Ist-Analyse Informationssteckbrief (Kubernetes Projekt)

Die folgenden Abschnitte umfassen die Ergebnisse aus den Retrospektiven, Anforderungs-, Architektur-, Prozess- und Qualitätsmodellierungen. Zum Ende des darauf folgenden Abschnitts findet sich eine Zusammenfassung der Ergebnisse und eine Ableitung von Herausforderungen wieder (siehe Kapitel 5.2.4.2.1).

5.2.4.1 Darstellung der Ergebnisse aus der Retrospektive

I. Was ist die Historie des Projekts?

Auf Basis eines Kundenauftrags startete das Projekt 2022 mit einer Funktions- und Technologie-Studie, um zu evaluieren, ob man Open Source oder proprietäre Software einsetzen sollte. Der Kunde kann derzeit keine Prognosen über potenzielle Krisengebiete durchführen, möchte dies aber mit der Entwicklung des Informationssteckbriefes ermöglichen. Für einen Einsatz von Open Source spricht die Entscheidungsfreiheit bei der Auswahl von Produkten sowie die eigenständige Entscheidung hinsichtlich des Speicherortes. Zusätzlich kann jede Bibliothek auf enthaltene Daten, Datenflüsse und Lizenzen geprüft werden. Für den Einsatz proprietärer Software spricht die Verfügbarkeit der Lösung und die Schnelligkeit bis zur Nutzung. Eine wesentliche Funktion, die sich bereits ableiten ließ, war die Notwendigkeit einer breiten Geo-Lokation. Außerdem war es ein Ziel, KI-Anwendungen einzubetten. Hier gilt es auch den wirtschaftlichen Aspekt nicht außer Acht zu lassen. Der Kunde wünscht sich eine transparente Teilung der Modelle. Schließlich war das Projekt wie folgt aufgestellt: beim Backend sowie beim Web-Frontend wurde vollständig auf Open Source gesetzt. Beim Mobile-Front-End entwickeln die Entwickler Open Source, binden aber für die Karte proprietäre Software ein. In diesem Projekt soll Souveränität gewährleistet werden, indem verstärkt auf Open Source gesetzt wird und der Kunde seine sowie externe Daten DSGVO-konform gebündelt und sinnstiftend dargestellt bekommt.

II. Welche Erfahrungen mit Open Source zur Vermeidung von Vendor-Lock-Ins gab es?

II. a) Was würdest du mehr tun? Aus der Retrospektive mit den Mitarbeitern des Projektteams geht hervor, dass mehr Verwundbarkeitsscans

durchzuführen sind, um Schwachstellen zu ermitteln und diese frühzeitig zu melden. Es ist zu prüfen, an welchen Stellen die Software angreifbar ist. Auch Lizenzscans sollten durchgeführt werden.

II. b) Was würdest du weiterhin so tun? Den Daten zufolge empfindet das Projektteam es als bedeutsam, sich weiterhin nicht zu sehr vom Markt zu verschließen. Damit ist gemeint, dass das Projektteam beobachten sollte, ob es ein kommerzielles Produkt gibt, das besser ist, als die Open Source Variante. Zusätzlich sollte man zwischenzeitlich prüfen, ob die verwendeten Frameworks weiterhin dem ursprünglichen Zweck dienen.

II. c) Was würdest du aufhören zu tun? Ab einem gewissen Punkt sollte man aufhören Entscheidungen für Frameworks zu hinterfragen, auch wenn man eine kleine Leistungssteigerung erreichen. Open Source verleitet dazu, Frameworks schnell zu verwerfen, da man ohne einen langwierigen Einkaufsprozess schnell etwas Neues wählen kann. Deswegen ist es bei Open Source von besonders hoher Bedeutung, Dokumentation zu führen, warum man sich für was entschieden hat.

II. d) Womit würdest du nun anfangen? Es gilt, als nächstes mehr Spezialisten dazuzuholen. Wenn es Spezialisten für Frameworks gibt, dann ist es mehrwertstiftend, sie für das Projekt zu gewinnen. Externe Meinungen sind zulässig, da die neuen Perspektiven Fragen aufwerfen, die man zuvor noch nicht in dieser Art adressiert hat.

II. e) Wovon würdest du weniger tun? Diskussionen sind fruchtbar, doch zu viele Diskussionen - zum Beispiel zum Einsatz verschiedener Frameworks - kommen dem Team-Gefüge nicht zu gute. Architektur-Entscheidungen sollten durch Abstimmung der Team-Mitglieder erfolgen. Zudem sollte man sich frühzeitig Gedanken dazu machen, was passiert, wenn ein Lead-Entwickler geht. Wenn ein Lead-Entwickler etwas begonnen hat, das niemand weiter fortführen kann, kann das das gesamte Projekt gefährden.

5.2.4.2 Darstellung Anforderungsmodelle, Prozessmodell, Architekturmodell und Qualitätsmodell

Was sind Anforderungen im Projekt? Ziel des Projekts ist es, dem Kunden eine Prognose zu ermöglichen, ob in einem Land demnächst eine Krise

politischen Ursprungs ausbrechen könnte. Hierfür wird eine Studienumgebung aufgesetzt und Anforderungen definiert (vgl. Tabelle 5.3).

1	Extraktion von Informationen externer Websites
2	Extraktion von Text und Metadaten aus Dokumenten
3	Extraktion von Tweets zu bestimmten Themen, Orten oder von ausgewählten Usern
4	Extraktion von Text aus Bildern
5	Extraktion von Meldungen aus den Titeln verschiedener Zeitungen
6	Extraktion von Daten aus den Tabellen in Dokumenten (im Text integriert und Bilder)
7	Audiospur eines YT-Videos extrahieren
8	Erstellung einer Zusammenfassung von Text
9	Senimentanalyse für den eingegebenen Text durchführen
10	Prognose, ob in einem Land demnächst eine Krise politischen Ursprungs ausbrechen wird – Krisenprognose für Länder der Studienumgebung

Tabelle 5.3: Anforderungen Informationssteckbrief

Als Datenbasis dienen verschiedene Datenquellen. So erscheinen Extraktionen von Informationen aus Websites sinnvoll, um Informationsprodukte zu bündeln. Eine weitere Extraktion von Text und Metadaten aus Dokumenten ermöglicht es Schlagworte aus Dokumenten zu erhalten. Tweets zu bestimmten Themen, Orten und ausgewählten Usern reichern die bereits gewonnen Ergebnisse an. Eine weitere Anforderung des Kunden ist die Generierung von Text aus Bildern. Hierbei soll einerseits der in Bildern inkludierte Text extrahiert werden, andererseits der Gesamtkontext des Bildes in Worte gefasst werden. Die nächste Anforderung folgt dem Interesse, News-Meldungen einzubinden sowie interne Datenquellen (insbesondere PDF-Dokumente), die vom Kunden direkt bereitgestellt werden. Schließlich sind auch die Audiospuren von Videos zu extrahieren. Die aus den vielen Extraktionen generierten Texte sollen maschinell zusammengefasst und eine Sentimentanalyse durchgeführt werden, um einen Einblick in das Stimmungsbild über einen Ort auf Basis der generierten Daten zu erhalten.

Wie sehen Anforderungsmodelle für den Informationssteckbrief

aus?

Die folgende Abbildung 5.10 stellt eine agile Anforderungsmodellierung (AA-Modellierung) für die ersten beiden Anforderungen dar. In der ersten Anforderung möchten die Entwickler externe Websites extrahieren. Hierzu wird ein Testfall aufgestellt. In diesem Testfall legt man fest, dass das Informationsprodukt Informationen zu Personen, Orten, Organisationen, Koordinaten und damit Geo-Informationen erhält. Ziel der zweiten Anforderung ist es, Auskunft über Textpassagen oder Metadaten zu Dokumenten zu erhalten. Dafür sehen sich die Entwickler in der Verantwortung, diese Schlagworte aus Texten und Metadaten zu extrahieren. Im Anschluss wird eine Suchfunktion nach Metadaten sowie eine Ausgabe von Schlagwörtern aus den Dokumenten im Bereich FAQ bereitgestellt.

Abbildung 5.11 zeigt das AA-Modell für die dritte und vierte Anforderung. Mit dem Ziel, Auskunft über Personen durch aktuelle Tweet-Inhalte zu erhalten, haben sich die Entwickler vorgenommen, zehn ausgewählte Personen sowie Orte und Themen zu extrahieren. Im Informationsprodukt findet sich dieses Feature im Bereich aktuelle Nachrichten wieder. Dass Auskunft über Textinhalte verschiedener Bilder gegeben wird, ist in der vierten Anforderung formuliert. Die Entwickler möchten den Text aus den Bildern extrahieren und auch unter dem Bereich FAQ die Ergebnisse aus dieser Bildextraktion ergänzen und bereitstellen.

Die fünfte Anforderung sieht die Anzeige aktueller Beiträge aus Nachrichtenportalen vor. Hierzu extrahieren die Entwickler die Meldungen aus den RSS-Feeds und binden diese ebenfalls in den Bereich aktuelle Nachrichten ein. Der Kunde möchte mit der sechsten Anforderung Daten aus Tabellen in Dokumenten extrahieren. Im Testing werden diese Extraktionen um die obigen angereichert, ein Deployment im Informationssteckbrief vorgenommen und geprüft, inwiefern sie im Bereich FAQ richtig ausgegeben werden (vgl. Abbildung 5.13).

Eine weitere Anforderung war die Einbindung von Inhalten aus Videos (vgl. Anforderung Nr.7 in Abbildung 5.13). Hierfür extrahieren die Entwickler die Audiospuren von YT-Videos und reichern erneut den Bereich FAQ an. Schließlich sollte im Bereich FAQ eine Zusammenfassung von Texten ausgegeben werden, die die Entwickler mit einer text summarization, entwickelt

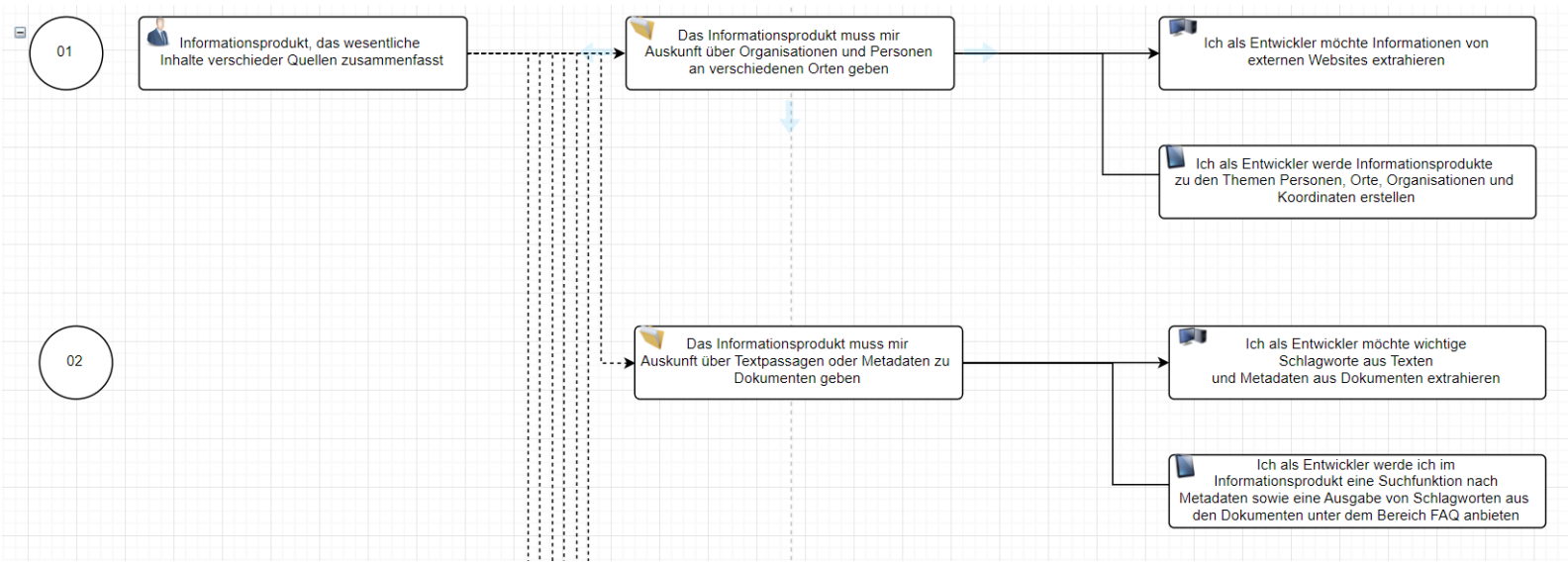


Abbildung 5.10: AA-Modellierung für Anforderung Nr.1 und 2 (Informationssteckbrief)

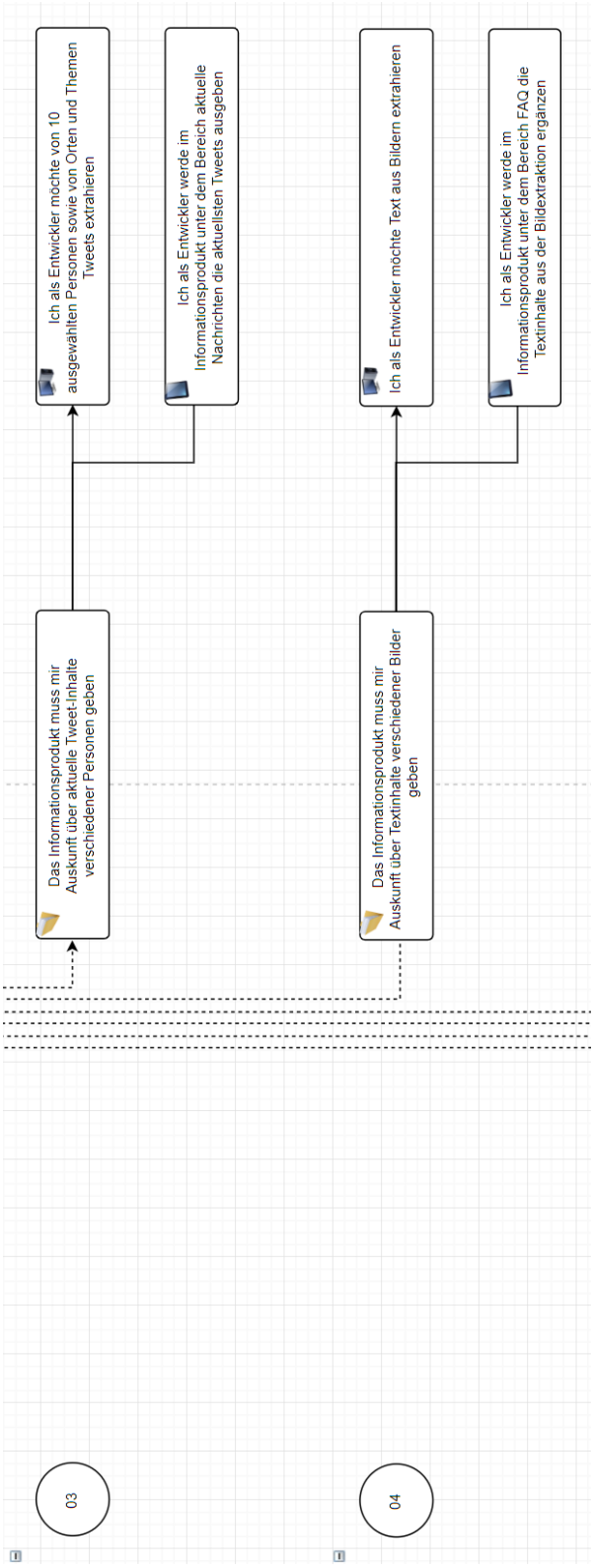


Abbildung 5.11: AA-Modellierung für Anforderung Nr.3 und 4 (Informationssteckbrief)

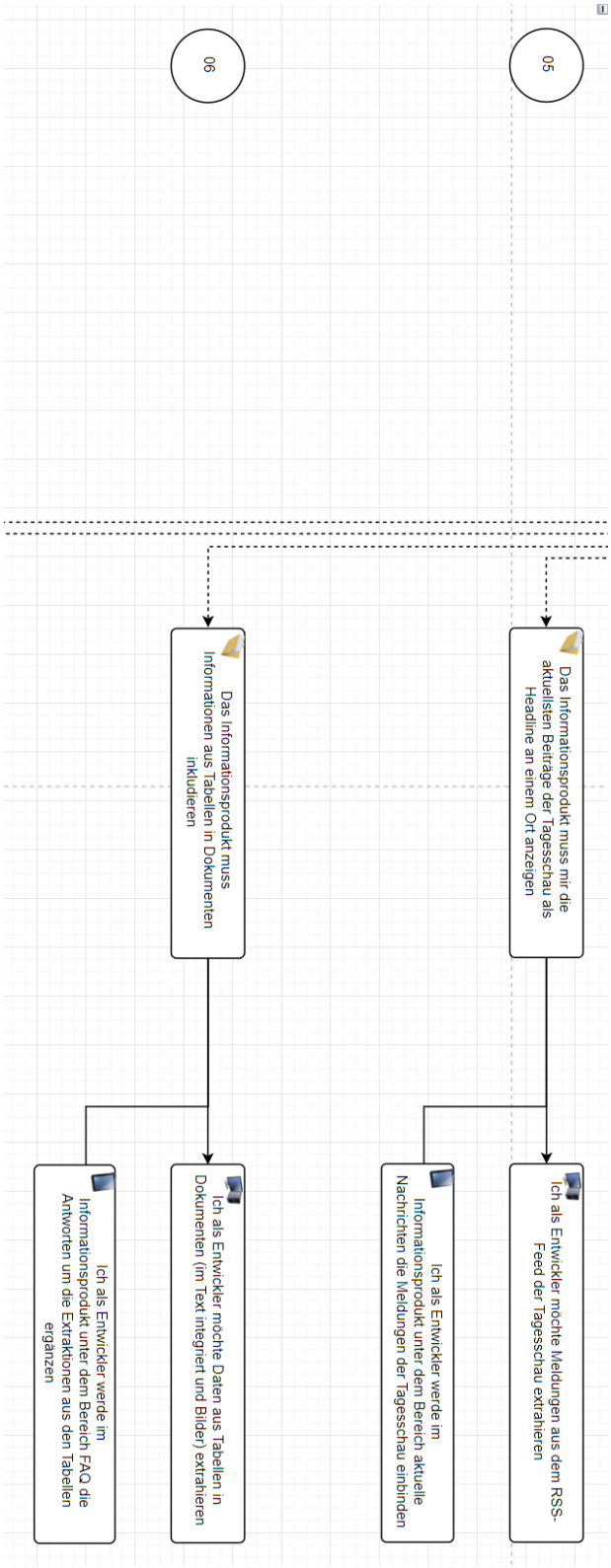


Abbildung 5.12: AA-Modellierung für Anforderung Nr.5 und 6 (Informationssteckbrief)

mit Python, lösen (vgl. Anforderung Nr.8 in Abbildung 5.13).
Die neunte Anforderung sieht den Erhalt eines Stimmungsbildes in einem bestimmten Ort vor (vgl. Abbildung 5.14). Diese wird entwicklungstechnisch mit Hilfe einer Sentimentanalyse umgesetzt. Datenbasis sind die generierten Texte aus html, jpg, pdf, mp4 und den Geo-Informationen, die extrahiert wurden. Die Ergebnisse aus dem Stimmungsbild fließen in den Bereich Stimmungsbild im Informationsprodukt ein. Um die Prognose stellen zu können, ob in einem Land demnächst eine politische Krise ausbrechen könnte, binden die Entwickler ein KI-Modell ein, das auf Basis der historischen Daten sowie unter Einbezug interner und externer Faktoren eine Vorhersage berechnet.

Wie sieht ein Architekturmodell für den Informationssteckbrief aus?

Die Projekt-Architektur teilt sich in Daten, Back-End, Front-End und User (vgl. Abbildung 5.15).

Auf der Daten-Ebene finden sich die externen Websites, Dokumente, Bilder und Audios wieder. Während die Informationen von den externen Websites gescraped werden, erfolgt bei den Dokumenten, Bildern und Audios ein Datenabruf. Ebenfalls auf der Daten-Ebene finden sich zwei Datenbanken, die einerseits die strukturierten, andererseits die unstrukturierten Daten speichern. Über eine ETL Strecke findet der Übergang in die Datenbanken über eine Transferzone statt. Im Backend werden die Daten analysiert und für eine Bereitstellung vorbereitet. Die Architektur sieht vor, dass eine text extraction von html, jpg, pdf, mp4, eine information extraction mit NLP (natural language processing) und geo information extraction erfolgt. Die Brücke zur einfachen Ausführung der Anwendung bildet der sogenannten BackEnd (Spring Boot). Dieser ist gekoppelt an 1) den Cognitive Service, der eine Sammlung von Algorithmen und Programmschnittstellen zur Bereitstellung von KI-Anwendungen zur Verfügung stellt, und 2) einer semantic search, die eine kontextuelle Suche ermöglicht. Das Herzstück des Front-Ends ist das Dashboard, das vier Reiter umfasst. Die User können das Dashboard sehen. Der Administrator, im Projektbeispiel auch ein Entwickler, kann Konfigurationsobjekte anpassen und Rollen und Rechte für den Informationssteckbrief vergeben.

Wie sieht ein Qualitätsmodell für den Informationssteckbrief aus?

Abbildung 5.16 zeigt ein Qualitätsmodell des Informationssteckbriefs. Die

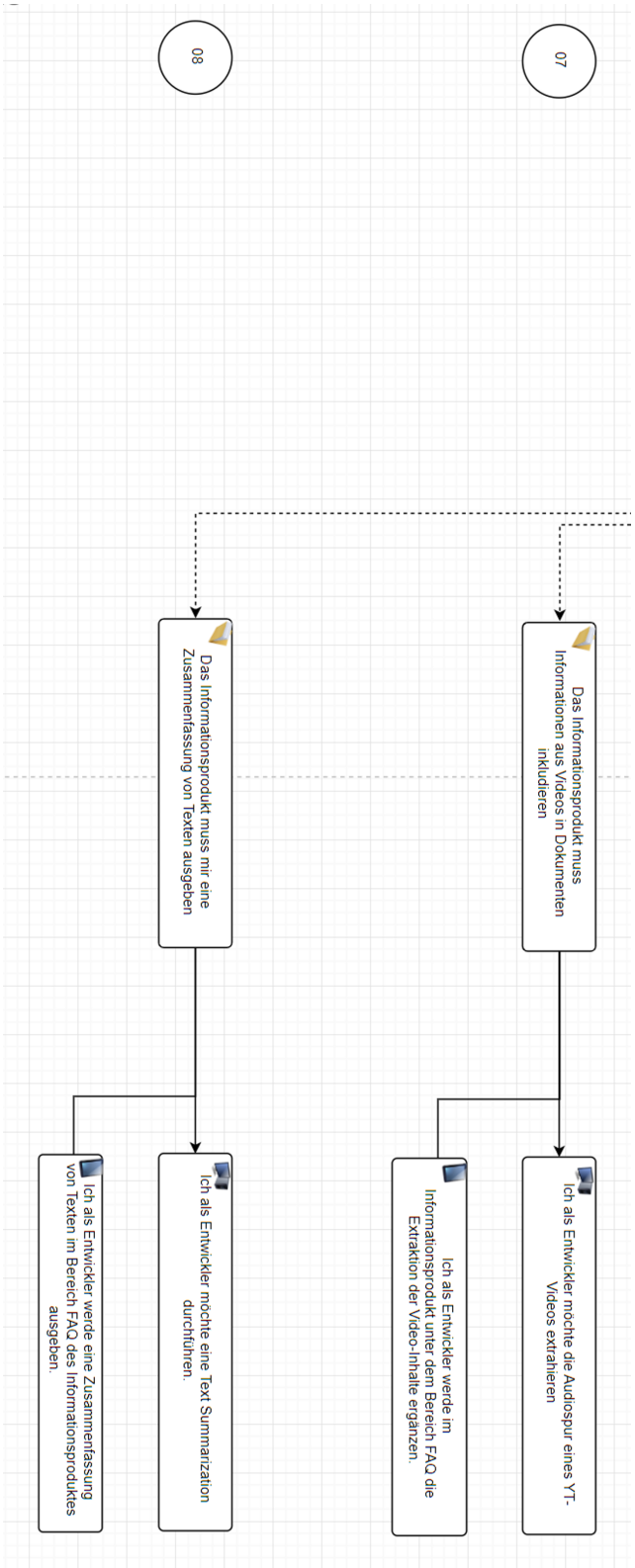


Abbildung 5.13: AA-Modellierung für Anforderung Nr.7 und 8 (Informationssteckbrief)

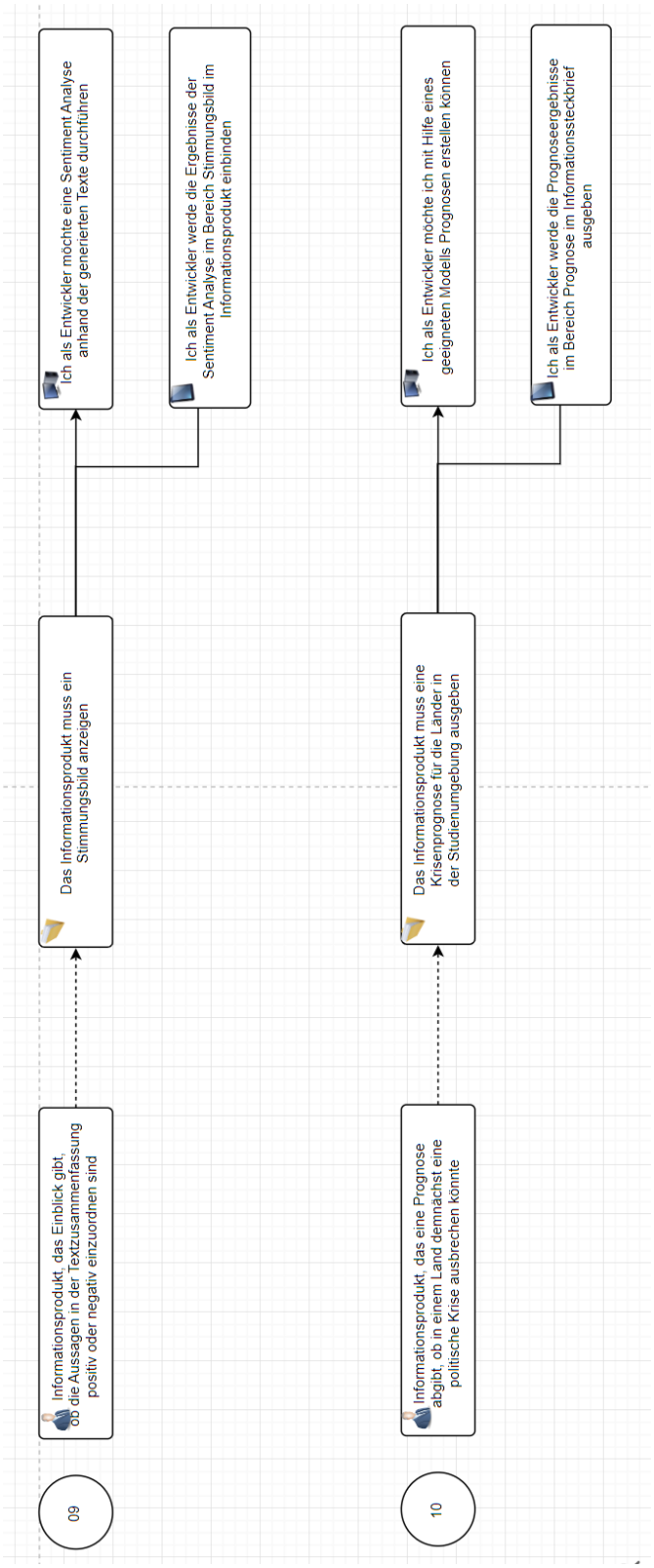


Abbildung 5.14: AA-Modellierung für Anforderung Nr.9 und 10 (Informationssteckbrief)

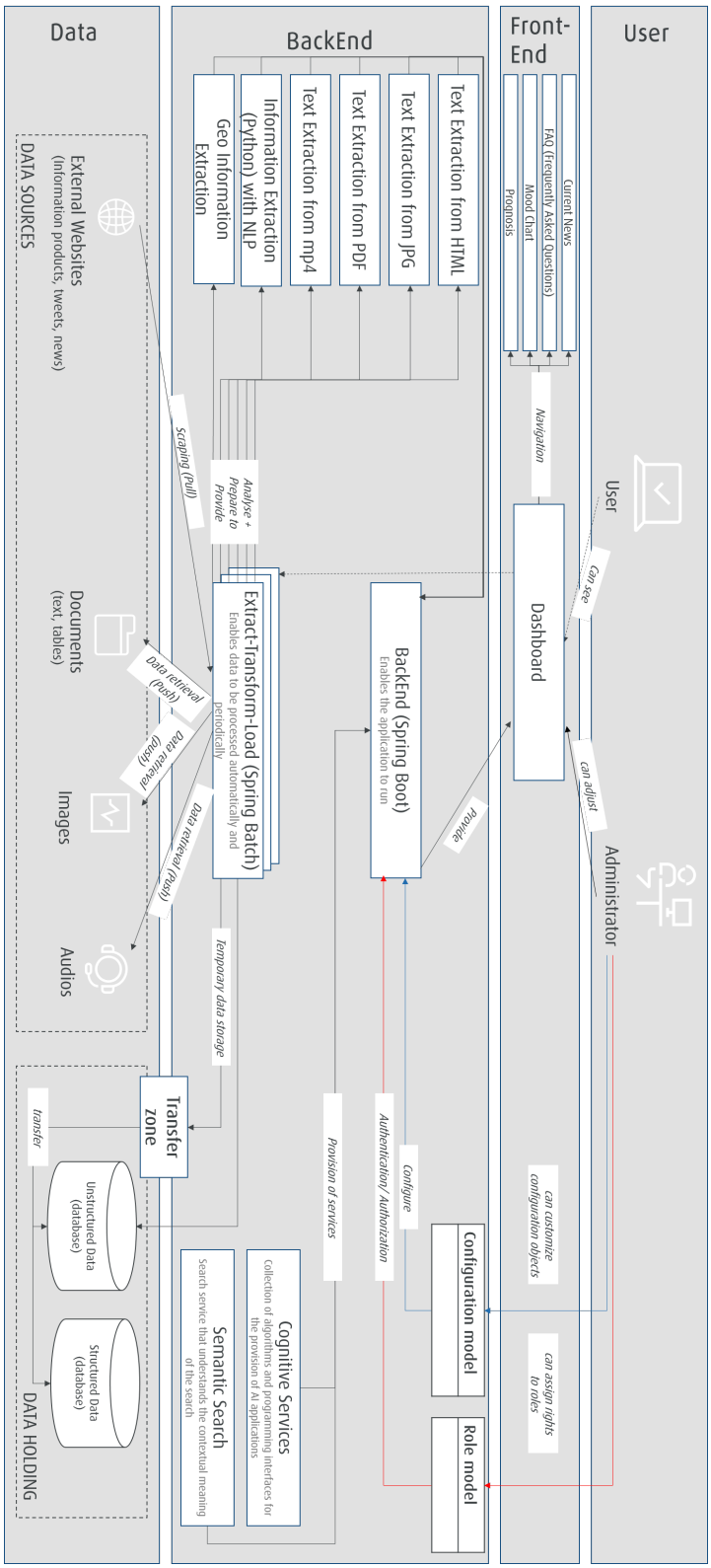


Abbildung 5.15: Projekt-Architektur für den Informationssteckbrief

Qualitätsmerkmale Zugänglichkeit, Benutzerfreundlichkeit, technische Korrektheit, Sicherheit und Ansprechbarkeit sind in Qualitätsmerkmale und dann wiederum in Qualitätsindikatoren heruntergebrochen worden.

So soll der Prototyp browser- und geräteabhängig sein. Erreicht werden soll dieses Qualitätsmerkmal, indem die Kompatibilität auf Tablets, Laptops und Handys (iOs und Android) geprüft wird. Ein weiteres Qualitätsmerkmal sieht eine gezielte Ausrichtung auf den Prototypen vor. Dies soll durch die Einbindung der Nutzer in Anforderungsworkshops und die Umsetzung priorisierter Anforderungen der Nutzer realisiert werden. Darüber hinaus ist dem Benutzer eine einfache Navigation anzubieten. Der Prototyp berücksichtigt Richtlinien zur Validität, indem er auf Fehlerfreiheit geprüft wurde, eine gute Softwaredokumentation vorliegt und die Nutzungsbedingungen fachlich korrekt wiedergegeben worden sind. Weiterhin sind wesentliche Sicherheitsbestandteile zu berücksichtigen. Darunter zählen ein Rollen- und Rechtekonzept (inkl. Authentifizierung/Autorisierung), ein Konfigurationsmanagement, das ausschließlich über Admins steuerbar ist und Datenschutzbestimmungen. Zuletzt ist sicherzustellen, dass der Prototyp optisch ansprechend ist. Um dies zu erreichen, wird das Layout dem Inhalt angepasst, die Farbgestaltung einheitlich gestaltet und geeignete Designelemente ausgewählt.

Wie sieht ein Prozessmodell für den Informationssteckbrief aus? Abbildung 5.17 visualisiert ein vereinfachtes Prozessmodell für den Informationssteckbrief. Das Prozessmodell stellt die User-Schritte bei der Verwendung des Informationssteckbriefs dar. Um auf den Informationssteckbrief zugreifen zu können, muss der User erst einmal die entsprechende Website öffnen. Im Anschluss kann sich der User auf der Website einloggen. Nach dem Log-In wird auf der Back-End-Ebene ein initialer Ladeprozess angestoßen. Hat dieser stattgefunden, so kann der User nun nach einem Ort suchen. Auf seinem Bildschirm erscheint eine Kachel mit der aktuellen Nachrichtenlage. Um hier Detailinformationen zu erhalten, klickt der User auf die aktuellen Nachrichten. Klickt der User aus dem Detailfenster heraus oder schließt das Detailfenster, so kann er sich nun weiter auf der Startseite navigieren. Der nächste Reiter ist der FAQ-Reiter. Hat der User diesen gesichtet, so kann als nächstes das Stimmungsbild und das finale Prognoseergebnis angesehen werden.

Abbildung 5.16: Qualitätsmodell für den Informationssteckbrief

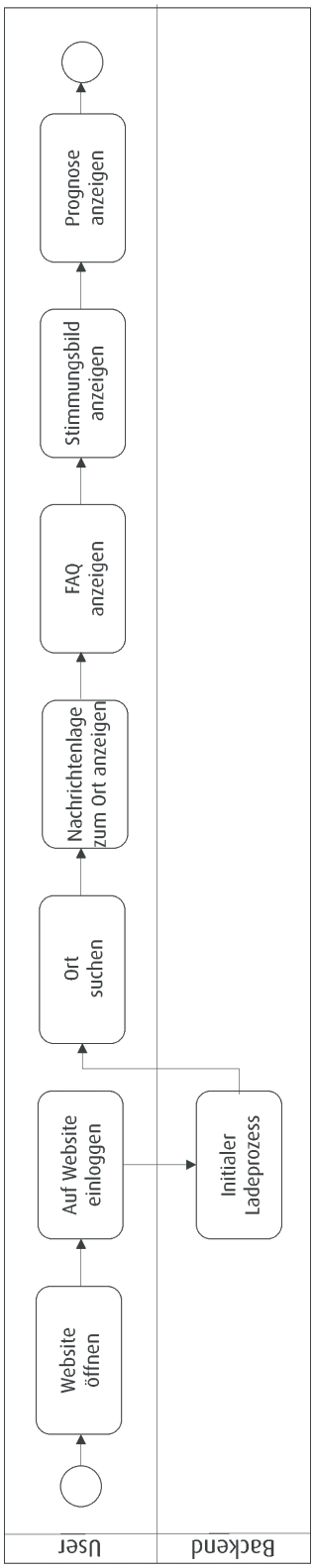


Abbildung 5.17: Prozessmodell für den Informationssteckbrief

5.2.5 Ist-Analyse Messenger (Matrix Projekt)

5.2.5.1 Darstellung der Ergebnisse aus der Retrospektive

I. Was ist die Historie des Projektes?

Ziel des Projektes ist es einen sicheren Messenger für den öffentlichen Sektor zu bauen. Der Messenger ist ein Open Source Produkt auf Basis des Matrix Protokolls. Neben einer Ende-zu-Ende-Verschlüsselung des kompletten Datenverkehrs sieht der Messenger den Betrieb der Lösung auf eigener IT-Infrastruktur des Kunden vor, was zu einer verstärkten Souveränität über seine eigenen Daten führen soll. Sämtliche Daten werden verschlüsselt in einer eigenen Umgebung, anstatt im nativen Speicher des Smartphones abgelegt. Matrix Foundation ist des Weiteren eine Open Source Community, die Entwicklern Vorgaben für die Nutzung des Kommunikationsprotokolls liefert. Manchmal gehen auch Neuerungen von Seiten der Matrix Foundation aus. Übergeordnetes Ziel der Foundation ist es, Matrix-Standards festzulegen und es zu ermöglichen über Matrix eine Verbindung mit Gatekeepern (wie z.B. WhatsApp) herzustellen. So können Nutzer künftig bei Nutzung von Matrix auch mit anderen Messaging-Diensten kommunizieren.

II. Welche Erfahrungen gab es mit der Verwendung von Open Source zur Vermeidung von Vendor-Lock-Ins?

II. a) Was würdest du mehr tun? Da innerhalb des Projektes zwei Unternehmen in der Entwicklung gleichzeitig tätig sind, gilt es, die Änderungen, die vorgenommen werden, kontinuierlich in das Open Source Team zurückzuspielen. Innerhalb der Open Source Community bietet es sich an, Ergebnisse so häufig wie möglich zu präsentieren, damit Fehlentwicklungen schnell aufgedeckt werden können. Alternativ könnte eine Ausbildung oder eine Einstellung eines Kryptographie-Experten zur Reduktion des oben genannten Vendor-Lock-Ins führen. Auf strategischer Ebene müsste das gesamte Thema „zukunftsfähige Softwareentwicklung“ innerhalb des Unternehmens stärker aufgegriffen sowie Maßnahmen zur Reduktion von Abhängigkeiten umgesetzt werden.

II. b) Was würdest du weiterhin so tun? Da die Erfahrungen im Rahmen der Zusammenarbeit mit der Open Source Community derart positiv waren, sollte weiterhin mit der Open Source Community zusammengearbeitet werden.

Arbeit an der Verschlüsselung und Sicherheit ist für das Projektteam ungemein wertvoll und war in der Community in der Vergangenheit fruchtbar. Um den Einfluss des Unterauftragnehmers zu reduzieren, sind auch interne Vorhaben, wie die Entwicklung eines DevLabs, das Schnittstellen für alternative Tools und Frameworks bietet, sinnvoll. Hier sind bereits Anstrengungen aus der Vergangenheit erkennbar, die es weiterhin zu verfolgen gilt. Da Entwicklungen schnell und dynamisch erfolgen müssen, sollten die Entwickler weiterhin die Freiheit haben, sich auf ihre Kernaufgabe - die erfolgreiche Entwicklung des Messengers – konzentrieren zu dürfen und nicht zu sehr mit verschiedenen Unternehmensprozessen konfrontiert zu werden. Aus Entwicklungssicht sind Feature Flags und String Tables eingebunden worden. Feature Flags helfen bei der Aktivierung oder Deaktivierung von Features, wobei keine Änderung des Quellcodes für diese Art der Bereitstellung erforderlich ist. Die Einführung eigener String-Tables führt dazu, dass Text an einem Ort zentralisiert ist und Entwickler so einfacher auf die jeweilige Zeichenkettentabelle verweisen können.

II. c) Was würdest du aufhören zu tun? In Zukunft sollte nicht mehr verstärkt auf den Einsatz von proprietärer und damit einhergehender sehr spezialisierter Software gesetzt werden. Im Sinne von DevOps sollten das Entwicklungs- und das Operationsteam in einem Team zusammenarbeiten. Das ist in dem Projekt noch nicht der Fall. Deswegen sollte man diese Aufteilung aufheben und die Zusammenführung der Teams anstreben. In der Zusammenarbeit gilt es außerdem, nicht mehr Softwarekonzepte nachzuahmen, die wissentlich Vendor-Lock-Ins erhöhen. Eine weitere Einschätzung des Projektteams ist, dass die Zusammenarbeit mit einzelnen Unterauftragnehmern zu lange dauert.

II. d) Womit würdest du nun anfangen? Man sollte mehr Expertise bei der Verschlüsselungsthematik aufbauen, um die Geschehnisse besser verstehen und interpretieren zu können. Unternehmensinterne Prozesse, die einen Zeitverzug für das Projektteam bedeuten, sollten geprüft werden. Die Erstellung von Sicherheitskonzepten beispielsweise könnte automatisiert werden. Außerdem ist es sinnvoll, sich in der Matrix Foundation einzubringen, um Entwicklungen des Matrix-Kommunikationsprotokolls besser zu Gunsten der eigenen Interessen steuern zu können.

II. e) Wovon würdest du weniger tun? Im Falle der Entwicklung des

Messengers, wo Sicherheit eine große Rolle spielt, macht zu viel Ausprobieren später die Arbeit in Richtung Prüfung auf Schwachstellen jedoch schwerer. Außerdem wird einmal im Monat der Open Source Stand zwischen Auftraggeber und Auftragnehmer ausgetauscht. Je mehr Anpassungen im Quellcode vor der Abnahme erfolgt sind, desto höher ist die Wahrscheinlichkeit für Doppelarbeit. Diese gilt es zu reduzieren. Zusätzlich bietet es sich an, die Anzahl der Drittpartei-Komponenten zu reduzieren. Kritische Abhängigkeiten von diesen Komponenten sind zu prüfen, die Risiken zu bewerten und entsprechende Maßnahmen zum Umgang mit den Risiken zu definieren.

5.2.5.2 Darstellung Anforderungsmodelle, Prozessmodell, Architekturmodell und Qualitätsmodell

Was waren Anforderungen an das Projekt?

Tabelle 5.4 zeigt die Anforderungen von Seiten des Kunden an die Messenger-Entwicklung.

1	Die App muss ausschließlich für den Kunden und seine Partner zugänglich sein
2	Die App muss erhöhte Sicherheitsanforderungen abbilden können
3	Die App muss performant sein
4	Die App muss Audio- und Videokonferenzen ermöglichen
5	Die App muss Design-Elemente des Kunden aufgreifen
6	Die App muss Gruppenchats zulassen
7	Die App muss neben der klassischen Chat-Funktion, die Möglichkeiten bieten, Dateien auszutauschen
8	Die App muss ein Rollen-, und Rechtesystem haben (Bsp: Admin kann ausgewählte Personen zu Gruppe einladen)
9	In der App muss die Erstellung eines persönlichen Accounts möglich sein
10	Die App muss auch auf anderen Devices, als dem Diensthandy, herunterladbar sein

Tabelle 5.4: Anforderungen Messenger

Tragende Anforderung an die zu entwickelnde Messenger-App ist, dass diese ausschließlich für den Kunden gebaut wird. Das heißt, dass der Kunde

und seine Partner Zugang zum Messenger haben müssen. Außerdem muss die App performant und einfach handhabbar sein. Designtechnisch soll die App Elemente des Kunden aufgreifen. Feature-technisch sind einerseits Gruppenchats, andererseits Chat-Funktionen zu implementieren, die die Möglichkeit bieten Dateien auszutauschen oder zu telefonieren. Die App sollte ein Rollen- und Rechtesystem haben, damit beispielsweise ein Admin ausgewählte Personen zu einer Gruppe einladen kann. Personalisierung ist ebenfalls eine Anforderung. So soll die Erstellung eines persönlichen Accounts möglich sein. Letzte Anforderung an die App ist es, dass diese nicht ausschließlich auf dem Diensthandy, sondern auch auf anderen Devices herunterladbar sein soll.

Wie sehen die Anforderungsmodelle für den Messenger aus?

Die folgende Abbildung 5.18 zeigt, dass die App zur Kommunikation zwischen dem Kunden und einer beliebigen anderen Person genutzt werden kann.

Die Entwickler nehmen sich vor, eine Anmeldefunktion vorzuschalten, sodass man nur Zugriff auf die App erhält, wenn man den entsprechenden Benutzernamen und das Passwort eingibt. Als Testfall wird ein beispielhafter Benutzername und ein Test-Passwort vergeben. Die zweite Anforderung sieht eine sichere Kommunikation von Inhalten auf der App vor, indem Olm- und Megolm als offene Standards eingebunden werden, um eine E2E-Verschlüsselung zu ermöglichen. Der Kunde schreibt zusätzlich vor, dass das Projektteam halbjährlich einen Penetrationstest durchführen muss, damit Sicherheitslücken kontinuierlich aufgedeckt und schnell behoben werden können.

In Abbildung 5.19 finden sich wiederum die dritte und vierte Anforderung für die Messenger-Entwicklung. Die App soll performant sein. Um dies zu gewährleisten, testen die Entwickler die App auf verschiedenen Geräten: dienstlichen sowie privaten Smartphones, Tablets und Laptops. Mit einem intelligenten Caching überprüfen sie, ob der Code optimiert werden kann. Der Endanwender wünscht sich, dass neben der Chat-Funktion auch Audio- und Videokonferenzen mit einem Chatteilnehmer durchführbar sind. Hierzu entwickeln die Entwickler einen Test-Case mit einigen ausgewählten Kunden. Mit Hilfe von Web RTC können die Entwickler Telefonate und Videos initiieren. Ein Befehl über ein Telefon- oder Video-Icon erreicht den Chatteilnehmer auf der anderen Seite, der den Audio- oder Video-Anruf annehmen oder ablehnen kann.

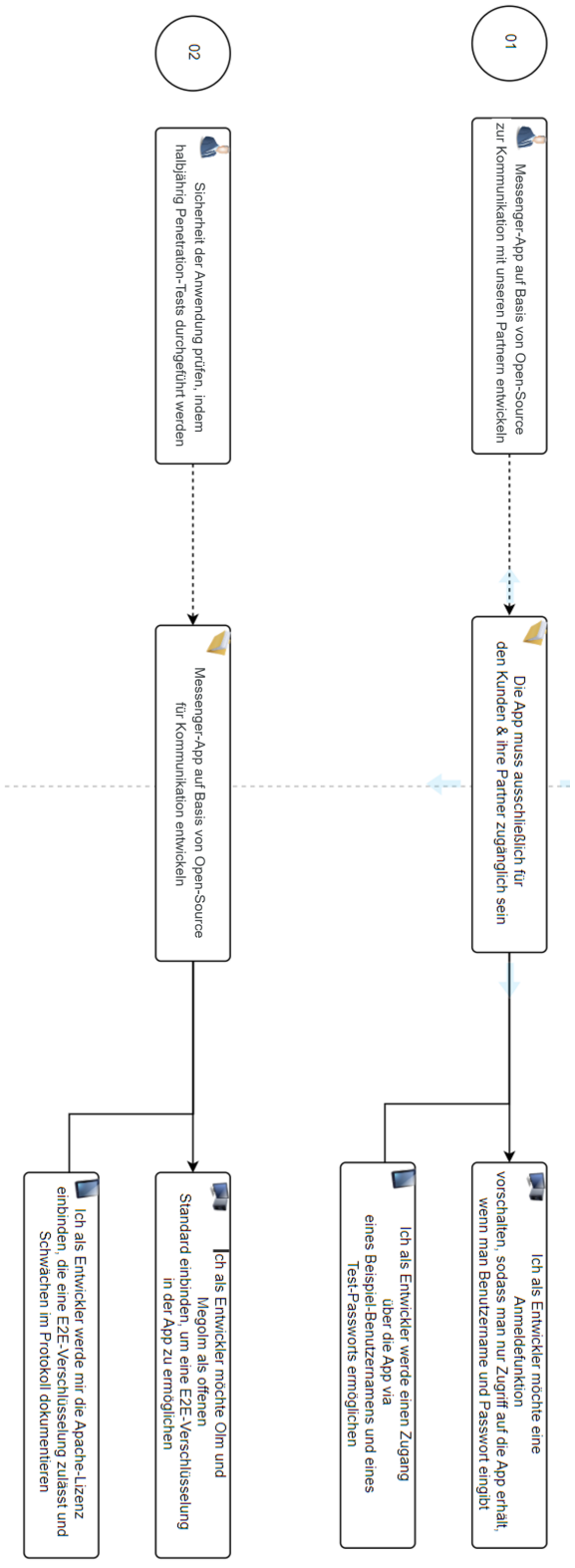


Abbildung 5.18: AA-Modellierung für Anforderung Nr.1 und 2

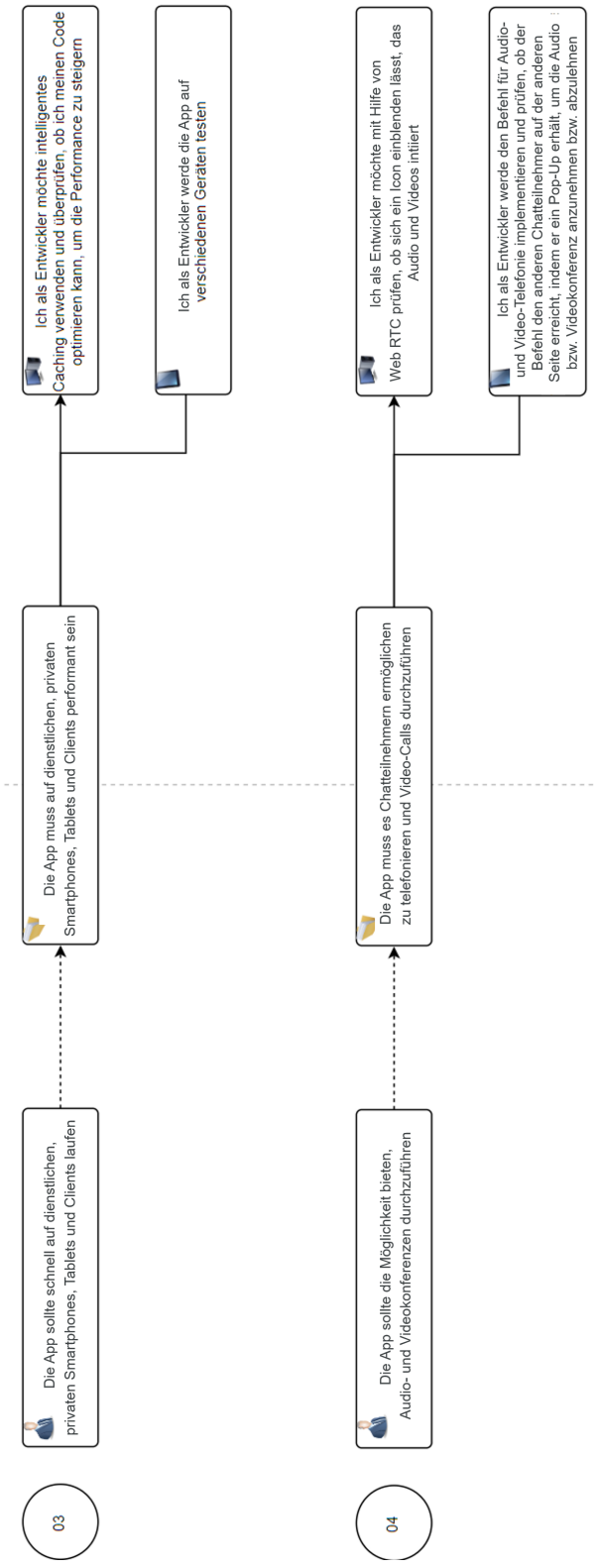


Abbildung 5.19: AA-Modellierung für Anforderung Nr.3 und 4

Der Kunde wünscht sich eine optisch ansprechende App, die zugleich leicht handhabbar ist (vgl. Abbildung 5.20). Dies soll durch eine Front-End-Optimierung erreicht werden. Die Entwickler verwenden ein einheitliches Design, das sich an Standards (z.B. WhatsApp) bei der Platzierung von Komponenten orientiert. Gleichzeitig greifen sie für den Kunden bekannte Design-Elemente (z.B. Logo) auf, um eine Wiedererkennbarkeit zu gewährleisten. Das Front-End wird in einer neuen Test-Schleife mit dem Kunden iterativ evaluiert. Feature-seitig soll es mit der App möglich sein, Gruppenräume zu öffnen. Im Test-Case wollen die Entwickler drei verschiedene Möglichkeiten implementieren: Erstens kann der User einem Raum beitreten und in diesem Raum alleine schreiben. Es gibt keine weiteren Teilnehmer. Der User kann zweitens eine zweite Person einladen, einem Raum beizutreten und chatten. Es handelt sich um einen klassischen Chat. Drittens, sobald der User eine dritte Person einlädt, dem Raum beizutreten und zu chatten, handelt es sich um einen Gruppen-Chat.

Die nächste Anforderung sieht die Möglichkeit vor, Dateien auszutauschen (vgl. Abbildung 5.20). Als Test-Case wird festgelegt, dass erst bei einem Chat mit mehr oder genau zwei Personen ein Datei-Austausch-Icon aufpoppt. Die Entwickler nutzen eine standardisierte API. Bei Klick auf das Datei-Austausch-Icon erfolgt eine Zugriffs-Abfrage auf das jeweilige Device, das gerade genutzt wird. Im Anschluss kann eine Datei ausgewählt werden, die im Chat hochgeladen wird. Anforderung Nr. 8 sieht ein Rollen-, und Rechtekonzept vor. Es wird zwischen Admin, Power-User und Regular User differenziert. Die Entwickler legen in einem Test-Case folgende Rechte fest: 1) Wer schreiben darf, 2) Wer moderieren darf, 3) Wer administrieren darf, 4) Wer Dritte einladen darf.

Die nächste Anforderung, das Anlegen eines Profils, bietet dem User mehr Individualisierung innerhalb der App (vgl. Abbildung 5.21). Dazu sind im Test-Case zunächst drei Dinge umzusetzen, um die Anforderung zu adressieren. Erstens kann der User einen Namen vergeben. Zweitens, der User kann ein Profilbild hochladen. Drittens kann das Profil mit einer Telefonnummer oder E-Mail-Adresse verknüpft werden. Um die letzte Anforderung seitens des Kunden, die App über unterschiedliche Devices herunterladen zu können, zu erfüllen, veröffentlichen die Entwickler die App als Testversion im App- und

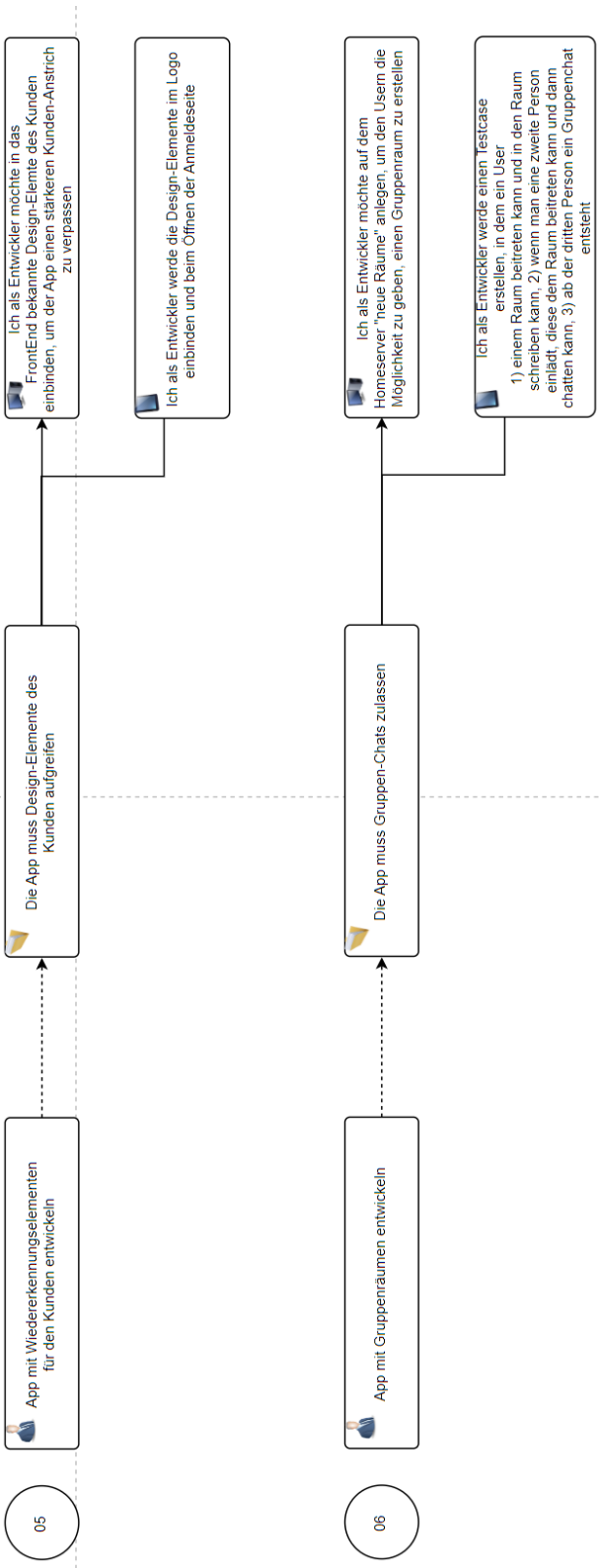


Abbildung 5.20: AA-Modellierung für Anforderung Nr.5 und 6

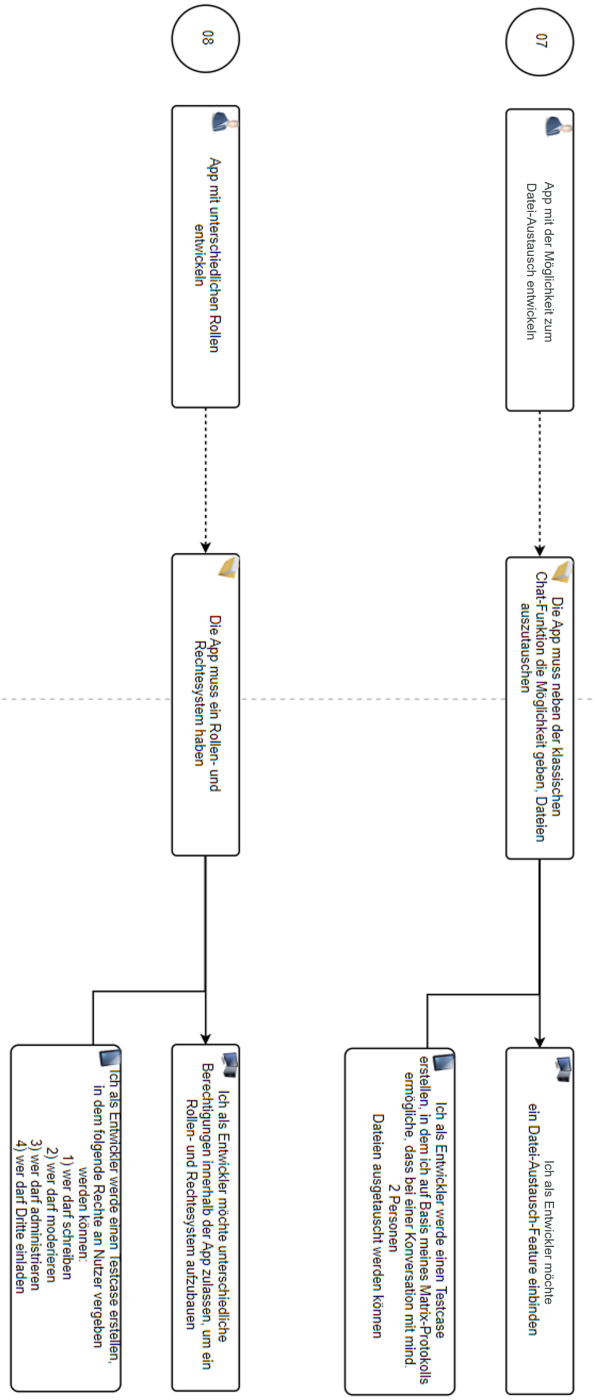


Abbildung 5.21: AA-Modellierung für Anforderung Nr.7 und 8

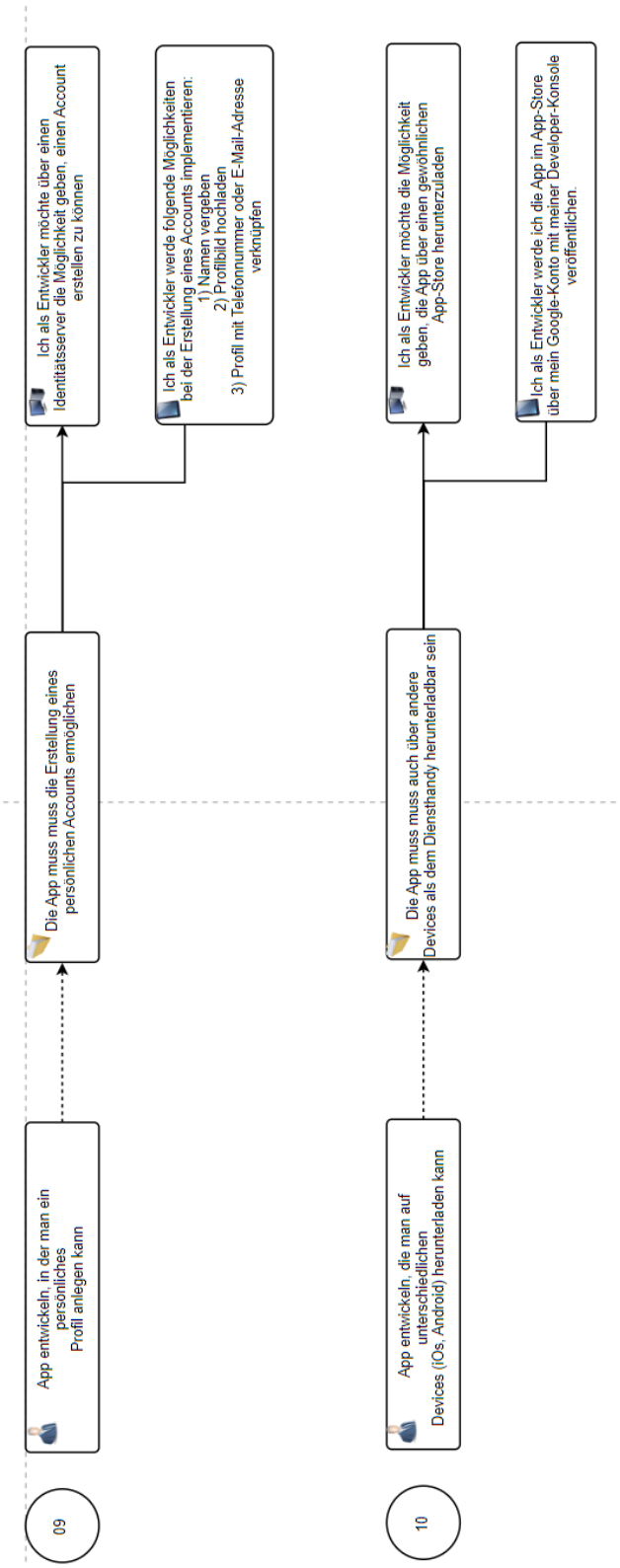


Abbildung 5.22: AA-Modellierung für Anforderung Nr.9 und 10

Google-Play-Store (vgl. Abbildung 5.22). Mit dem Aufsetzen einer Developer-Konsole können die Entwickler dem potenziellen User die Möglichkeit geben, die App über die zwei genannten App-Stores und damit über iOS und android herunterzuladen.

Wie sieht ein Architekturmodell für den Messenger aus?

Die Projekt-Architektur sieht vier Ebenen vor: die Datenbasis, die Chat-App-Cloud Infrastruktur, den Geo-lokalisierten Server und die User-Ebene (vgl. Abbildung 5.23).

Auf der untersten Ebene zieht sich das Projekt aus der Metadata-Datenbank die Daten für die Erstellung von Benutzergruppen und Chats. Zwei weitere Datenbänkanwendungen sind die Hot Chat History und die Cold Chat History. Aus der Hot Chat History kann man letzte Meldungen extrahieren. Aus der Cold Chat History lassen sich archivierte Chats wiederherstellen. Die Chat App Infrastruktur basiert auf einer public cloud. Eine Message Queue dient dazu, dass eine Nachrichtenschlange entsteht, wenn der Empfänger keine Nachricht abruft oder das Zielsystem grade nicht abrufbar ist. Das sorgt dafür, dass ein Warteschlangenbetrieb entkoppelt verarbeitet werden kann. Lösungstechnisch wurde auf den Open Source Standard Apache Kafka zurückgegriffen. Das User Profile Management bietet Entwicklern die Möglichkeit, Multi-Faktor-Authentifizierungen, Kontoüberprüfungen bzw. Wiederherstellungen oder Profil- und Kontoverwaltungsoptionen für den Benutzer einzubinden. So können Benutzer in ihren späteren Einstellungen je nach administrativer Konfiguration ihre Einstellungen im Benutzerprofil nach ihren Wünschen anpassen. Um in der App später die Verwendung von Emojis zu ermöglichen, wurde ein Emoji Service eingebunden. Der Prozess hierzu wird durch commits an ein Github-Repository ausgelöst. Das heißt, die Entwickler stellen Bereitstellungspipelines zur Verfügung. Der Server Health Check wurde eingebunden, um zu prüfen, wie gut der Zustand eines Servers ist. Bewertungskriterien hierfür sind Festplattenkapazität, RAM-Verfügbarkeit und CPU-Nutzung. Mit Hilfe von WebRTC können Datei-, Video- und Audio-Konferenzen initiiert werden. Der Homeserver speichert die Account-Informationen in einer history und vergleicht die Daten mit den Homeservern der User. Dies ermöglicht einen nahtlosen Austausch auch zwischen unterschiedlichen Devices. Auf dem geo-lokalisierten

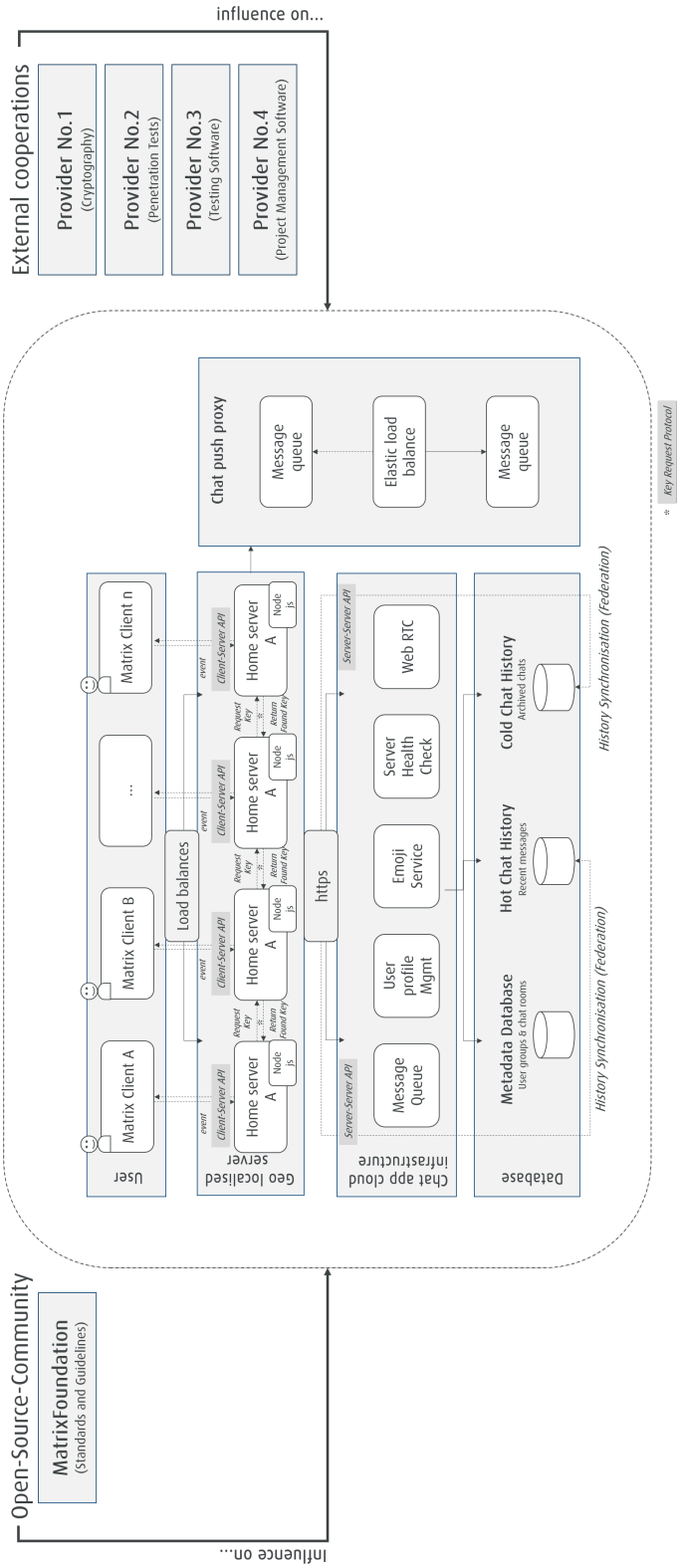


Abbildung 5.23: Projekt-Architektur für den Messenger

Server werden Java-Script-Codes ausgeführt. Node js ist eine Open Source Laufzeitumgebung, die dies ermöglicht. Mittels der in der Architektur dargestellten Load Balances verteilen sich der Datenverkehr und die Anfragen gleichmäßig auf die Server, um so die Geschwindigkeit zu erhöhen und die Kapazitätsauslastung zu minimieren. Auf diesem Wege wird sichergestellt, dass kein Server überlastet ist. Zudem haben die User durch die Matrix Clients die Möglichkeit, sich einen Server für die Erstellung einer Verbindung zu ziehen. Durch den Chat Push Proxy werden Push-Benachrichtigungen für die Anwendung möglich. Die Projektarchitektur stützt sich stark auf externe Kooperationspartner. Ein Unterauftragnehmer kümmert sich um den Anteil Kryptografie und ein anderer um die Penetrationstests. Ein weiterer stellt die eingesetzte Testing Software und jemand anderes Projektmanagement-Tools. Zuletzt ist ein weiterer Unterauftragnehmer für die Bereitstellung von kompatiblen Kubernetes-Clustern, On-Premises oder Clouds zuständig. Die Matrix Foundation als Open Source Community, die Vorgaben für die Verwendung des Matrix Kommunikationsprotokolls vorgibt, hat ebenfalls Einfluss auf das Projekt und wird deswegen in der Projektarchitektur als wesentlicher Einflussfaktor berücksichtigt.

Wie sieht ein Qualitätsmodell für den Messenger aus?

Im Rahmen der App-Qualität ist ein besonderes Augenmerk auf die Metriken Nutzbarkeit, Sicherheit und Zuverlässigkeit gelegt worden (vgl. Abbildung 5.24).

Um die App als User gut nutzen zu können, ist auf einen angemessenen Ressourcenverbrauch zu achten. Dieser angemessene Ressourcenverbrauch soll durch die Indikatoren Internetverkehr, Nutzung von Speicherplatz und Akkuverbrauch geprüft werden. Zeitgleich sei auf eine verständliche und intuitive Menüführung zu achten. Es wird geprüft, ob die Bedienelemente angemessen groß und sinnvoll platziert sind, ob das Design in der App einheitlich und gut wahrnehmbar ist und ob der Text in der App einfach gehalten und präzise ist. Die Metrik Sicherheit wird einerseits aus Perspektive des Datenschutzes und andererseits aus Perspektive Zugriff von Unautorisierten begutachtet. Ob Datenschutzbestimmungen berücksichtigt wurden, ist insbesondere mittels dieser drei Fragen zu bewerten: Sind Angaben zu Zweck, Nutzen, Art und Umfang der Datenspeicherung gemacht worden? Sind die Datenschutzbestimmungen

Abbildung 5.24: Qualitätsmodell für den Messenger

leicht auffindbar? Besteht die Möglichkeit bereits vergebene Berechtigungen zu korrigieren? Ob ein unautorisierter Zugang zur App möglich ist, ist durch Integrität, Vertrauenswürdigkeit und Authentizität indiziert. Bei dem Indikator Integrität sind Beschränkungen der Zugänge durch ein Rollen-, und Rechtesystem vorzunehmen. Bei dem Indikator Vertrauenswürdigkeit gilt es Erläuterung zu Funktionsänderungen und Zugriffsrechten einzubinden. Und schließlich steckt hinter dem Indikator Authentizität, die Einsehbarkeit und Korrigierbarkeit erhobener Daten. Zuverlässigkeit wird durch die Fehlerfrequenz in der App gemessen. Das heißt, es ist untersucht worden, ob offensichtliche bugs in der App eliminiert worden sind, ob geringe oder keine Zeitverzögerungen vorhanden sind und ob wenige Abstürze sichergestellt werden können.

Wie sieht ein Prozessmodell für den Messenger aus?

Die folgende Abbildung zeigt den prozessualen Ablauf zwischen einer Person A und einer Person B bei der Nutzung des Messengers (vgl. Abbildung 5.25). Dabei ist zunächst davon auszugehen, dass Person A die Messenger-App auswählt und dann nach einer Person zum Chatten (Person B) sucht. Es wird eine Synchronisierung in der Datenbank angestoßen. Wird die Person nicht gefunden, so endet der Prozess. Gilt die Person als gefunden, so erhält Person B eine Benachrichtigung über eine Chat-Einladung. Sofern Person B die Chat-Einladung bestätigt, wird Person B hierüber benachrichtigt. Person A kann nun eine Chatnachricht an Person B verfassen. Person B kann die Chatnachricht empfangen. Person B verschickt nun ebenfalls eine Chatnachricht an Person A. Schließt einer der Personen den Chat, so gilt der Prozess als beendet.

5.2.5.3.1 Zusammenfassung und Ableitung von Herausforderungen zur Stärkung der digitalen Souveränität mit Open Source (für die Projekte Informationssteckbrief und Messenger)

Tabelle 5.5 stellt wesentliche Herausforderungen aus den beiden Retrospektiven dar.

Anhand der vorangegangenen Ist-Analyse wird deutlich, dass bei der Entwicklung des Messengers, Standards und Richtlinien, die von externen Stellen wie der Matrix Foundation vorgegeben werden, die Autonomie des Projekts einschränken. Darüber hinaus liegt das Fachwissen in den Bereichen Kryptografie und Penetrationstests bei Drittanbietern. Folglich führt auch die Auswahl von

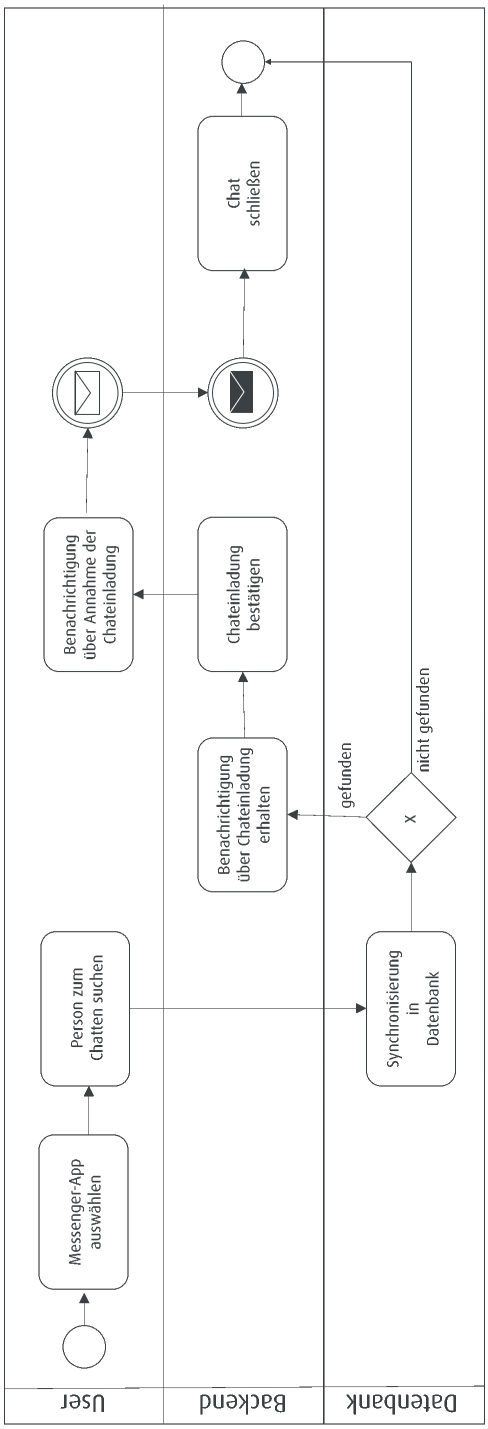


Abbildung 5.25: Prozessmodell für den Messenger

H1	Niemand aus dem Projekt ist Teil der Matrix Foundation. Damit hat das Projektteam keinen Einfluss auf das Matrix-Ökosystem.
H2	Es fehlt an Fachwissen in Kernbereichen wie Kryptografie. Aus diesem Grund wird das Thema an Externe ausgelagert.
H3	Die Verwendung bestimmter proprietärer Tools ist problematisch.
H4	Die Verwendung von Open Source sollte nicht auf Kosten der Sicherheit gehen.
H5	Es liegt eine Abhängigkeit bei der Entwicklung von Marktmonopolisten wie Amazon oder Microsoft vor.
H6	Es liegt die Erwartung vor, 100 prozentige Sicherheit zu gewährleisten.
H7	Es gibt kaum gute Alternativen zu den englischen NLP-Modellen.

Tabelle 5.5: Zitate aus den Retrospektiven mit den Projektteams

Prüfsoftware und Projektmanagement-Software zu Abhängigkeiten. Sicherheitsschwächen wurden bei der Front-End-Lösung, dem Betriebssystem, der Datenbank und der Datenbankverwaltungslösung für den Informationsauftrag festgestellt. Die im Projekt verwendete Cloud führt zu Abhängigkeiten und Lock-in-Effekten, die auch die Autonomie des Projektteams einschränken. Eine weitere Herausforderung besteht darin, dass automatisierte Extraktionen zum Missbrauch oder zur Offenlegung sensibler Informationen führen könnten. Es ist möglich, auf persönliche Daten zurückzugreifen und auf den Standort von Personen zu schließen. Der Einsatz von KI-Modellen verdeutlicht insbesondere die Herausforderung der Abhängigkeit von englischsprachigen NLP-Modellen.

5.2.6 Beschreibung des Soll-Zustands: Anforderungen digitaler Souveränität auf Basis der Herausforderungen

Der im nachfolgenden Kapitel beschriebene Zustand zeigt strategische Ziele digitaler Souveränität auf Basis der oben genannten Herausforderungen.

Wie in der Tabelle 5.5 dargestellt, ist die Autonomie der Projektteams aufgrund verschiedener Abhängigkeiten zu eingeschränkt. Unsere Literaturrecherche zeigt, dass Autonomie im digitalen Raum, im Sinne von digitaler Souveränität, den Erwerb der notwendigen Fähigkeiten und Fertigkeiten erfordert (Pohle, 2020). Pohle (2020) weist darauf hin, dass Regelungen getroffen werden sollten, die zu mehr Sicherheit und Unabhängigkeit führen, und dass dafür technologische und ökonomische Fähigkeiten notwendig sind. Eine weitere Forderung im Sinne digitaler Souveränität ist es, Abhängigkeiten

zu reduzieren (Avila Pinto, 2018; Glasze et al., 2022; Moerel & Timmers, 2021; Pohle, 2020). Diese Forderung leitet sich aus den Herausforderungen H1 und H5 ab, in denen die Abhängigkeiten von externen Stiftungen und Unternehmen hervorgehoben werden. Nach Moerel und Timmers (2021) ist die Abhängigkeit von wenigen Lieferanten und Monopolisten besonders problematisch. Dies spiegelt sich auch in der Herausforderung H5 wider, die die Abhängigkeit von Monopolisten wie Amazon und Microsoft in der Entwicklungstätigkeit aufzeigt. Glasze et al. (2022) fordern die Prüfung von sicheren, europäischen, souveränen Cloud-Alternativen, um dem Ziel der technischen Souveränität näher zu kommen. Eine weitere Voraussetzung für die Stärkung von digitaler Souveränität ist mehr Produkthoheit (Couture & Toupin, 2019; Floridi, 2020).

Die Online-Retrospektiven (siehe Herausforderung H3) zeigten, dass der Einsatz einer proprietären Software in den Projekten zu Lock-In-Effekten führte. Couture und Toupin (2019) kritisieren den Umgang von Unternehmen mit digitalen Diensten von Google, Facebook und anderen Giganten und fordern die Überprüfung von digitalen Diensten für mehr digitale Souveränität. In diesem Zusammenhang wird deutlich, dass durch mehr digitale Souveränität die Reduzierung von Lock-in-Effekten möglich ist (Fries et al., 2022; Moerel & Timmers, 2021). Fries et al. (2022) schlagen vor, Strategien zur Reduzierung von Lock-Ins zu entwickeln. Darüber hinaus weist H4 darauf hin, dass es eine Herausforderung ist, Sicherheitsschwächen zu verhindern, die zum Missbrauch oder zur Offenlegung sensibler Informationen führen. Die damit verbundene Forderung von Hummel et al. (2021), Floridi (2020), Couture und Toupin (2019) lautet: mehr Datensouveränität. Hummel et al. (2021) versteht darunter einen gänzlich selbstbestimmteren Umgang mit Daten. Das kann den Missbrauch und die Offenlegung von Informationen umfassen. Glasze et al. (2022), Pohle (2020), Moerel und Timmers (2021) sehen einen Beitrag zu mehr Datensouveränität in der Reduzierung von Sicherheitslücken. Das adressiert damit genau die Herausforderung, die in der Ist-Analyse ermittelbar war. Moerel und Timmers (2021) und Glasze et al. (2022) fordern vertrauenswürdige IT. Dies geht mit der Reduzierung von Sicherheitsschwachstellen einher. Schließlich sehen Broeders et al. (2023) und Falkner et al. (2024) die Möglichkeit, Produkte unter Berücksichtigung der wirtschaftlichen Wettbewerbsfähigkeit und der Durch-

setzbarkeit zu realisieren, als eine Möglichkeit, digitale Souveränität zu stärken. Diese Forderung deckt sich mit Herausforderung H7, die darauf hinweist, dass es kaum gute Alternativen zu den gängigen englischen NLP-Modellen gibt.

5.2.7 Gap-Analyse für den Informationssteckbrief

Nachdem die Datenerhebung im Rahmen der Retrospektive mit den Projektteams erfolgt ist, konnte ein Ist-Abbildung gestaltet werden. Der Soll-Zustand wurde durch Literatur zu digitaler Souveränität repräsentiert.

Ziel dieses Abschnitts ist es nun, den Ist- und Soll-Zustand gegenüberzustellen, um operative und strategische Risiken im Kontext digitaler Souveränität abzuleiten. Diese Risiken werden im Rahmen der Anforderungs-, Architektur-, Qualitäts-, und Prozessmodellierung dargestellt und anschließend in sogenannten Gaps subsummiert.

5.2.7.1 Gaps in den Anforderungsmodellen des Informationssteckbriefs

So lässt sich zunächst feststellen, dass die Kompetenzen innerhalb des Projektteams rund um das Thema digitale Souveränität nicht hinreichend ausgeprägt sind (vgl. Risiko Nr.25, Abbildung 5.26). Es bräuchte mehr Wissen über potenzielle Technologie-Partner mit Alternativen aus Deutschland oder der EU, mehr Einblick in die Lieferkettenabhängigkeiten, die es zu reduzieren gilt, und klarere Vorgaben, wie eine Gewährleistung von Datensouveränität bzw. -sicherheit in der Entwicklung erfolgen soll. Des Weiteren fehlen die Verantwortlichkeiten für die Prüfung des Quellcodes. Das Projektteam ist ressourcenseitig nicht dafür aufgestellt, um den Quellcode auf Korrektheit und das Nichtvorhandensein unerwünschter Funktionen zu prüfen (vgl. Risiko Nr.26). Es sollte innerhalb des Projektes das Thema Datensicherheit nachhaltig und effektiv Berücksichtigung finden. Eine mögliche Stelle eines Daten-Missbrauchs kann im Projekt bei der Einholung von Auskunft über Twitter erfolgen (vgl. Risiko Nr.5, Abbildung 5.27). Hierbei geht man davon aus, dass frei zugängliche Informationen über Personen des öffentlichen Lebens im Projektkontext verwendet werden dürfen. Man legt also zugrunde, dass ein öffentliches Interesse an einer derartigen Person besteht und dies das Recht einräumt, Daten über die Person verarbeiten zu dürfen. Dennoch birgt dieses Verständnis ein Risiko.

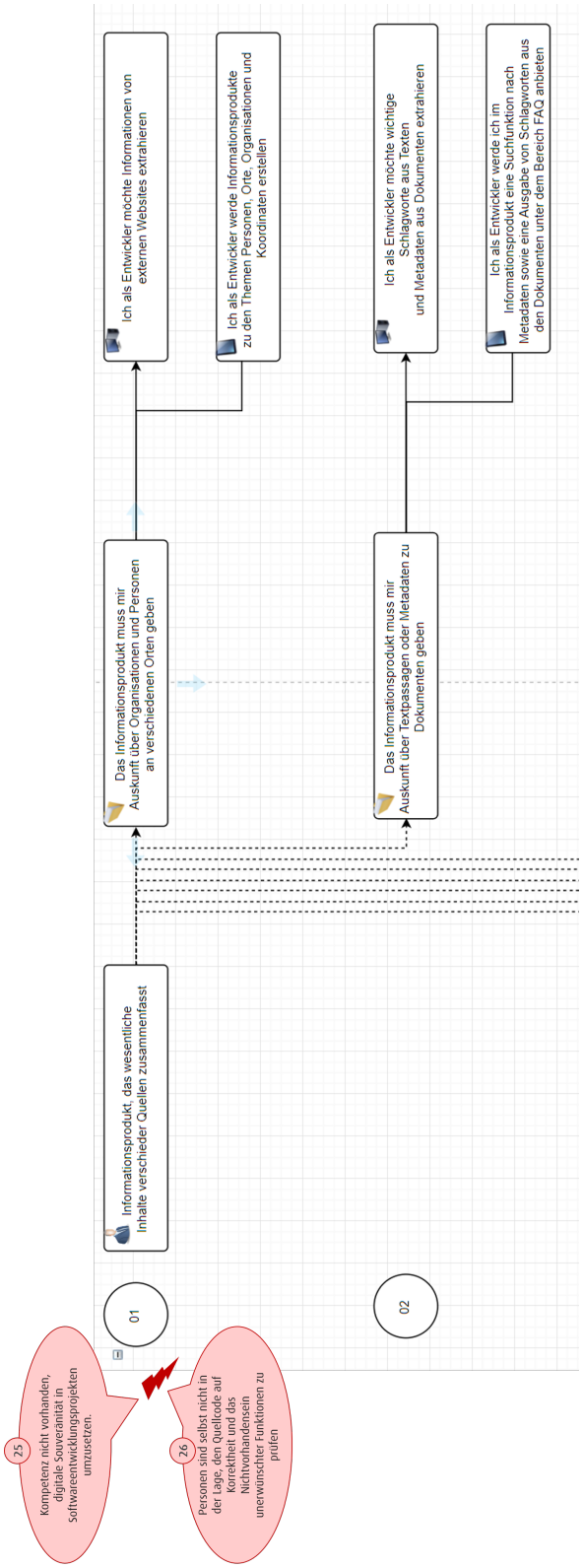


Abbildung 5.26: Identifizierte Risiken im AA-Modell für Anforderung 1 und 2 (Informationssteckbrief)

Die Verarbeitung personenbezogener Daten einer solchen Personengruppe ist nicht eineindeutig geregelt.

In Abbildung 5.29 wird deutlich, dass bei der Bereitstellung von Dokumenten die Möglichkeit eines Diebstahls von Geräten, Datenträgern oder von entsprechenden Dokumenten besteht (vgl. Risiko Nr.6, Abbildung 5.29). Auch ein Ausspähen oder ein Abhören von Informationen kann zu einem Abgreifen von Daten führen (vgl. Risiko Nr.8). Besonders kritisch ist dies im Kontext des Projekts an der Stelle, an der die Krisenprognose veröffentlicht wird. Um Datensicherheit nachhaltig und effektiv zu adressieren, sollte es das Ziel sein, diese Risiken zu mitigieren. Ferner ist es ein Risiko, dass zu wenig Awareness für das Thema Resilienz und souveräne Entscheidungsfindung bei dem Projektteam vorhanden ist (vgl. Risiko Nr.9). Dieses Verständnis ist jedoch notwendig, um Widerstandsfähigkeit und Kontrolle über die Software zu gewährleisten und zielführende Entscheidungen im Sinne der digitalen Souveränität treffen zu können. Da die Chancen und Risiken der Nutzung digitaler Dienste in der Regel durch die Product Owner oder Projektleiter festgelegt werden, in der Umsetzung aber die Entwickler die tragendere Rolle spielen, sollten sie als Experten in den Entscheidungsprozess inkludiert werden. Die Verantwortungszuteilung ist zu überdenken (vgl. Risiko Nr.10). Digitale Souveränität sieht vor, dass Datenintegrität gewährleistet wird. Regeln und Standards sind nicht in der anfänglichen Analyse-, und Designphase vom Projekt inkludieren worden (vgl. Risiko Nr.14). Dadurch, dass es keine neutrale organisatorische Instanz gibt, die eine Bewertung und Zertifizierung der IT vornehmen kann und auf die das Projektteam zurückgreifen kann, ergibt sich das Risiko, dass Eigeninteressen in Entwicklungsteams vorangetrieben werden und die eigene Arbeit - statt der Notwendigkeit nach digitaler Souveränität - in den Vordergrund gerückt wird (vgl. Risiko Nr.20, Abbildung 5.28).

5.2.7.2 Gaps im Architekturmodell des Informationssteckbriefs

Liegt kein Vertrauen zum Anbieter vor oder ergeben sich gar Gefahren hinsichtlich eines zu starken Abhängigkeitsverhältnisses, so ist das als Risiko für den Kunden anzusehen (vgl. Risiko Nr.22, Abbildung 5.30). Im Kontext Cloud ist im Projekt Informationssteckbrief auf den gängigen Hyper-Scaler Amazon

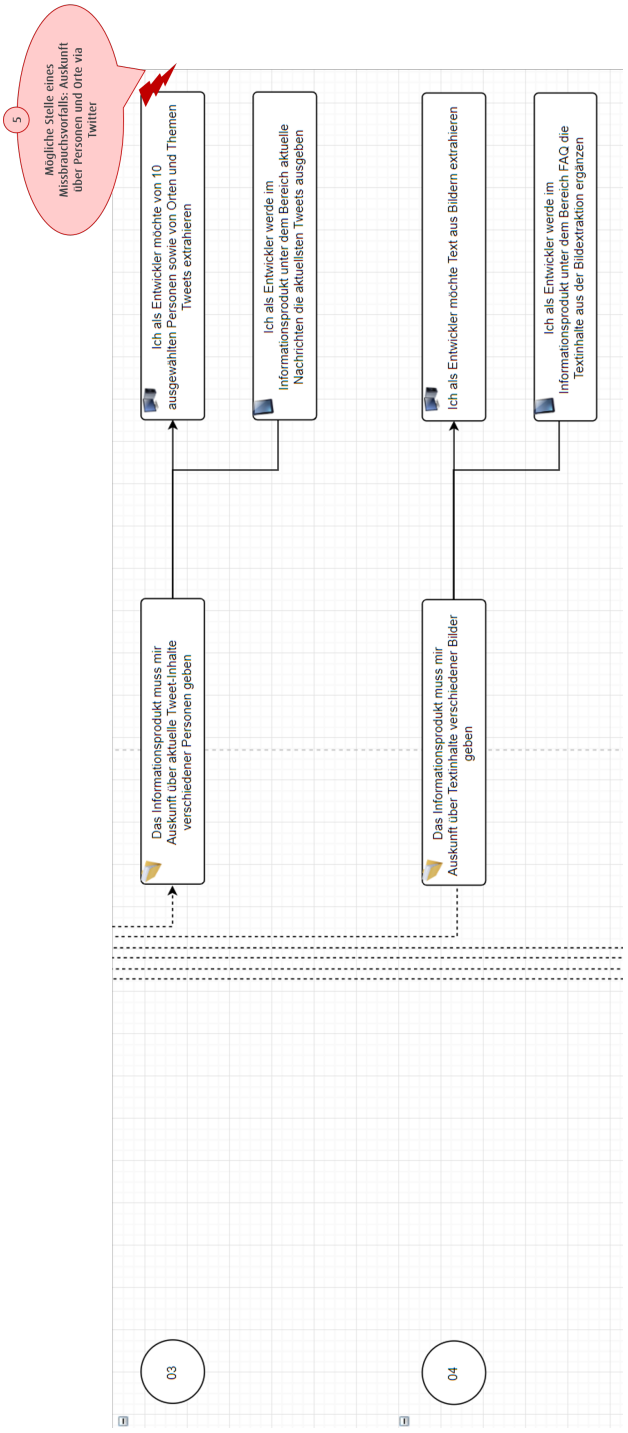


Abbildung 5.27: Identifiziertes Risiko im AA-Modell für Anforderung 3 und 4 (Informationssteckbrief)

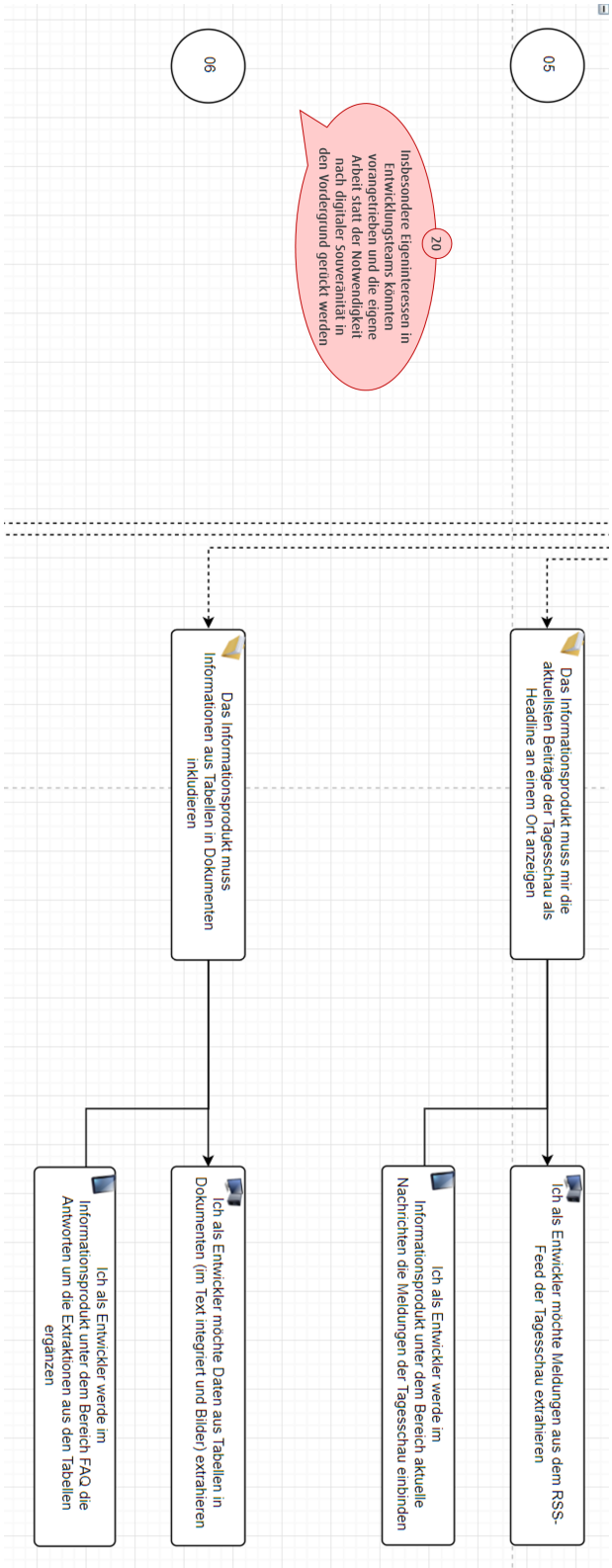


Abbildung 5.28: Identifizierte Risiken im AA-Modell für Anforderung 5 und 6 (Informationssteckbrief)

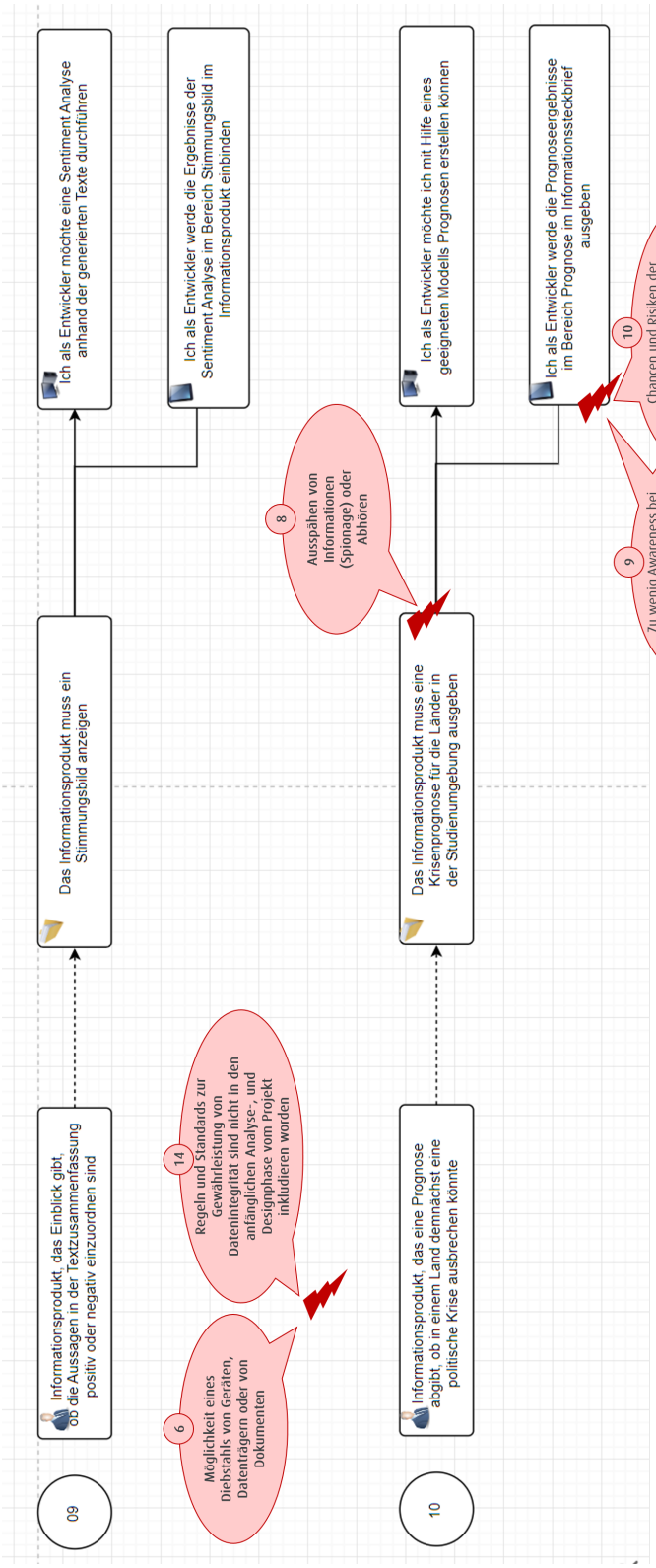


Abbildung 5.29: Identifizierte Risiken im AA-Modell für Anforderung 9 und 10 (Informationssteckbrief)

zurückgegriffen worden. Wie in den Zielen digitaler Souveränität beschrieben, sind europäische Alternativen von Cloud-Anbietern zu prüfen (vgl. Risiko Nr.12). Es ergibt sich jedoch die Herausforderung, dass die Vereinigten Staaten nicht nur zu einem führenden Experten im Cloud-Geschäft geworden sind, sondern auch zu einem der wichtigsten Zentren für die Entwicklung von künstlicher Intelligenz, mit Tech-Giganten wie Facebook, Google, Apple, Amazon und Microsoft an der Spitze der KI-getriebenen Forschung (Bal & Gill, 2020). China liegt dicht dahinter, da die Regierung massiv in die KI-Forschung und -Entwicklung investiert (Brattberg et al., 2020). Andere Länder wie Kanada, Japan und Südkorea machen ebenfalls große Fortschritte in dem Bereich (Gao et al., 2021). Europa als Ganzes hinkt bei der KI-Entwicklung hinterher (Brattberg et al., 2020).

Die vielversprechendsten NLP-Modelle für das vorliegende Projekt sind in englischer Sprache. Geht man auf ein deutsches oder europäisches NLP-Modell ergibt sich das Risiko, schlechtere Ergebnisse mit dem Modell zu erzielen (vgl. Risiko Nr.13). Im Projekt sind NLP-Experten beteiligt, sodass man davon ausgehen kann, dass sie über entsprechende Kompetenz und Fachwissen verfügen. Dennoch sei berücksichtigt, dass Alternativen zu dem Cloud-Anbieter Amazon ggf. nicht hinreichend betreiberfreundlich sind (vgl. Risiko Nr.21). Es ist zu prüfen, ob sie genügend Interoperabilität bieten und zu den Marktstandards passen, die erforderlich sind, um moderne, innovative, leistungsstarke, nachhaltige und skalierbare Produkte zu liefern. Man ist in den Optionen, die man hat, aufgrund der Tatsache, dass Europa hier in den Entwicklungen hinterher hängt, eingeschränkt (vgl. Risiko Nr.19). Darüber hinaus wurden keine Prozesse geschaffen: Es scheint nicht klar, wann man wen ansprechen und wie erreichen kann, wenn man Fragen hinsichtlich des richtigen Umgangs mit digitaler Souveränität hat (vgl. Risiko Nr.15). Ein zusätzliches Risiko sind die Sicherheitslücken im Projekt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen IT-Sicherheitshinweis für Grafana veröffentlicht (vgl. Risiko Nr.2) (BSI, 2025a). Fehlkonfigurationen in Kubernetes können laut BSI ebenfalls zu Sicherheitsrisiken führen (vgl. Risiko Nr.1) (BSI, 2025b). Die Datenbanken MongoDB und PostgreSQL weisen ebenfalls Sicherheitslücken auf (vgl. Risiko Nr.3 und 4). Beim Scraping der externen Websites

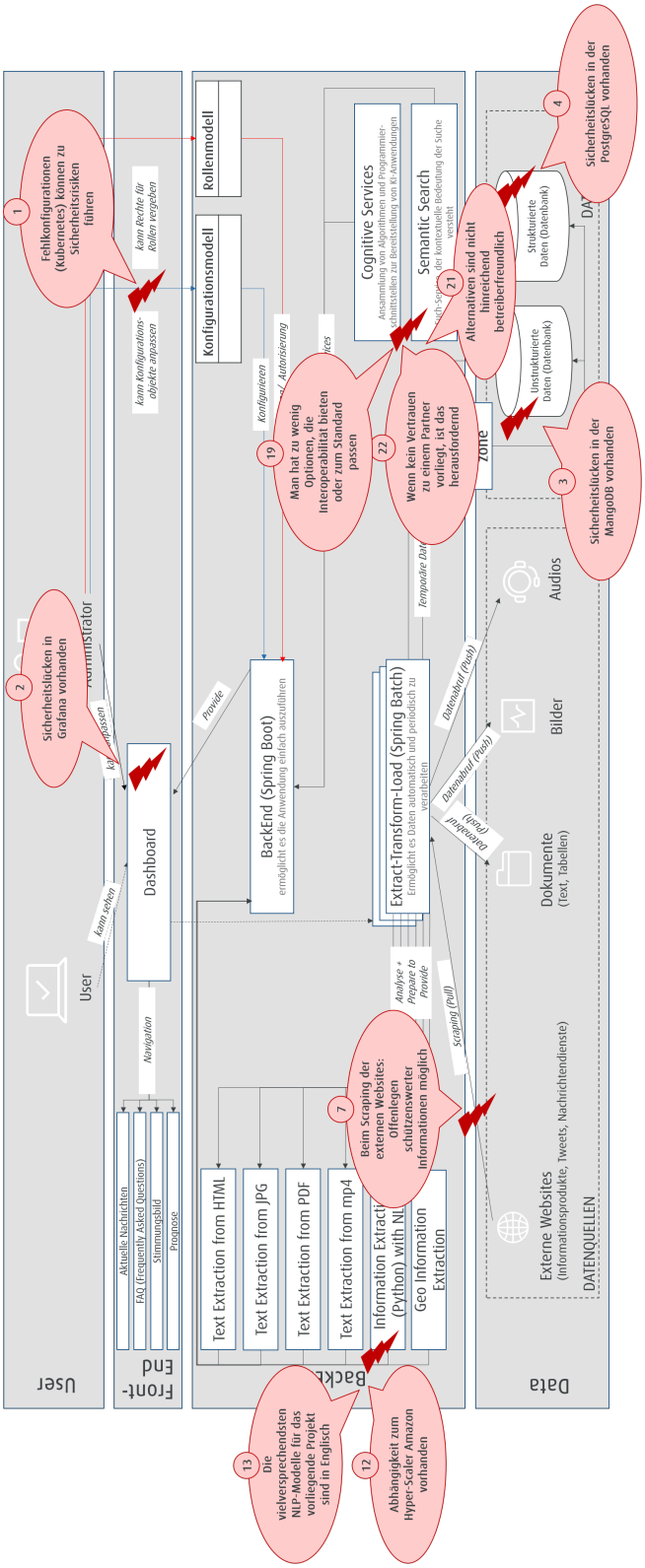


Abbildung 5.30: Identifizierte Risiken in der Projektarchitektur des Informationssteckbriefs

ist ein Offenlegen schützenswerter Informationen möglich (vgl. Risiko Nr.7).

5.2.7.3 Gaps im Qualitätsmodell des Informationssteckbriefs

Da im Rahmen der Definition von Qualitätsmerkmalen und -indikatoren im Wesentlichen technische Komponenten berücksichtigt wurden und die rechtliche Dimension marginal betrachtet wurde, ist dies eine weitere Lücke (vgl. Risiko Nr.24, Abbildung 5.31).

Die rechtliche Dimension klärt das „WAS darf das Projekt?“ bzw. was darf es innerhalb des vordefinierten Projektrahmens nicht. Insbesondere im öffentlichen Sektor ist dies eine wesentliche Dimension, da die Beschaffung von Hardware, Software und IT-Leistungen kompliziert ist (Erben & Günther, 2018). Das Risiko, das hierbei entsteht ist damit, dass keine Ausschreibungskriterien für digitale Souveränität definiert worden sind (vgl. Risiko 18). Das kann in Konsequenz dazu führen, dass das günstigste Angebot zwar genommen wird, die Sicherheit im Projekt jedoch darunter leidet. Das Projekt Informationssteckbrief sieht eine Erstellung eines Informationssicherheitskonzepts zu Beginn der Projektlaufzeit vor. Eine Aktualisierung des Konzeptes ist nicht vorgesehen. Dies birgt das Risiko, dass Verletzungsgefahren und Einbußen im Sinne der digitalen Souveränität durch das Ausbleiben der Aktualisierung des Informationssicherheitskonzeptes weiterhin bestehen (vgl. Risiko Nr.16). Dieser Effekt ist vergleichbar mit dem Erhalt des Führerscheins. Diesen erhalten Sie einmalig im Leben und dürfen dann bis zum Ende ihrer Lebensjahre damit Auto fahren. Trotz des formellen Akts kann eine unfallfreie Zeit für den Autofahrer nicht gewährleistet werden. So auch in diesem Projektkontext. Es ergibt sich das Risiko, dass man digitale Souveränität als Einheitslösung für Entwicklungsprojekte zu verkaufen versucht, was in Anbetracht der unterschiedlichen Projekte, Nutzer, des Einsatzes von verschiedenen Systemen und damit zusammenhängend ihrer Schutzmaßnahmen so sicherlich nicht möglich ist (vgl. Risiko Nr.17).

5.2.7.4 Gaps im Prozessmodell des Informationssteckbriefs

Die organisatorische Dimension gibt das „WIE dürfen wir es machen?“ vor. Auf der organisatorischen Ebene gilt es, Rollen, Prozesse und Berechtigungen so zu gestalten, dass die digitale Souveränität mit der notwendigen Dringlichkeit vorangetrieben werden kann. Es ergibt sich das Risiko, dass bei einer lediglich

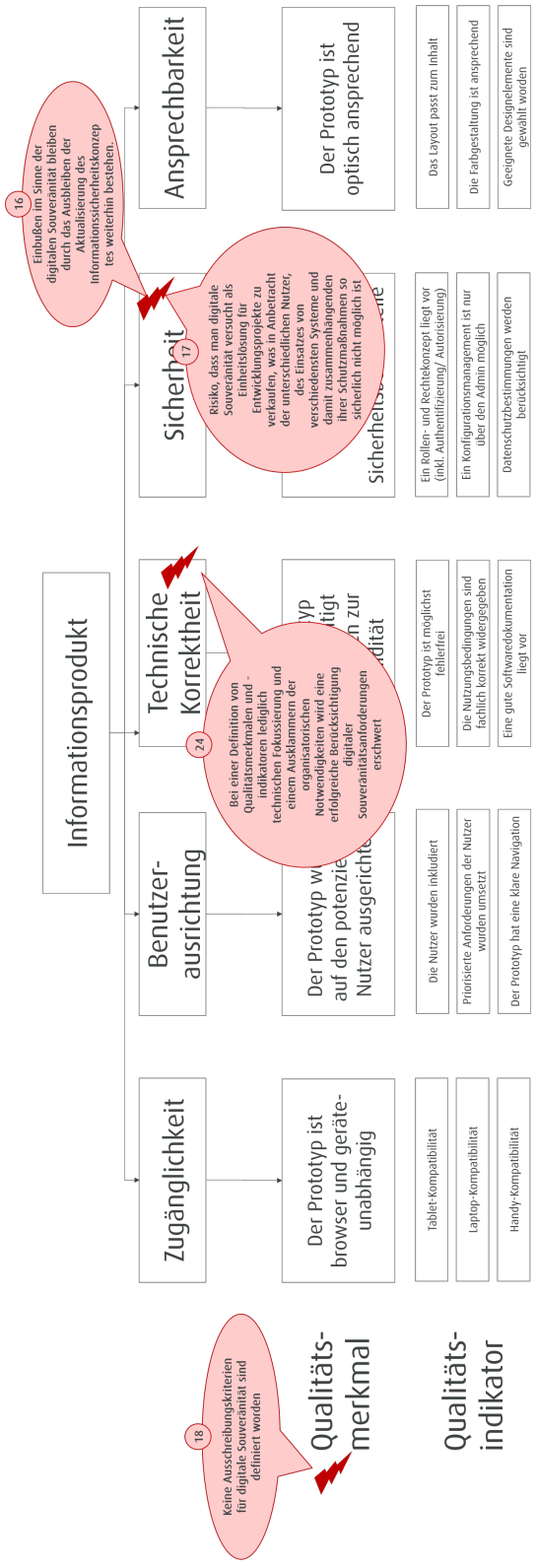


Abbildung 5.31: Identifizierte Risiken im Qualitätsmodell des Informationssteckbriefs

technischen Fokussierung und einem Ausklammern der organisatorischen Notwendigkeiten eine erfolgreiche Berücksichtigung digitaler Souveränitätsanforderungen erschwert wird (vgl. Risiko Nr.2 und 8, Abbildung 5.32).

5.2.7.5 Strategische Gaps für den Informationssteckbrief

In der Projekt-Architektur ist eine Beobachtung, dass strategische Maßnahmen zu digitaler Souveränität in der Unternehmensstrategie zwar festgelegt wurden, jedoch weder strategische noch operative Maßnahmen auf Projektebene zu finden sind (vgl. Risiko Nr.23). Das Projekt Informationssteckbrief hat gezeigt, dass der Anteil Netzwerke im Projektkontext als gegeben und resilient angenommen wird. Es gibt jedoch Ausfälle von Netzwerk-Konnektivität oder -diensten, die sich einer direkten Kontrolle des Unternehmens entziehen, z.B. Angriffe auf Dienstleister oder deren Infrastruktur im Ausland. Auch Störungen von Bereitstellungsinfrastruktur können zu einem eingedämmten Wirkungsgrad führen (Risiko Nr.29). Politische Einflüsse können z.B. dafür sorgen, dass bewusst Verschlüsselungen abgeschwächt werden und es so zu fehlerhafter Hard- und Software kommt. Derartige Risiken werden in der Regel von wenig dominanten Herstellern produziert (Risiko Nr.23) (Leyh & Bley, 2016). Auch Sanktionen haben die Eigenschaft, wenn diese zu Konkursen oder erzwungenen Stilllegungen führen, Ausfälle und fehlenden Support eines Herstellers oder Lieferanten von verbreiteten oder kritischen Produkten herbeizuführen (Risiko Nr.30) (Aksoy et al., 2022). Nicht zuletzt ist es als Risiko einzustufen, dass Ausfälle als Erpressungsinstrument genutzt werden können. So kann z.B. die Kontrolle über eine digitale Infrastruktur bei dominanten Herstellern in wenigen Ländern dazu führen, dass politische Akteure diese Sonderstellung für ihre Gegebenheiten nutzen, um politische Macht auszuüben (Risiko Nr.31). Technische Widerherstellungsverfahren können hier Abhilfe schaffen. Dennoch, das Wiederhochfahren von Logistikketten, Energie-, oder Transportnetzen ist bei einem potenziellen Angriff eine schwerwiegende Aufgabe (Risiko Nr.32). Im schlimmsten Fall müssen abgewanderte Geschäfte, Kunden oder Partner zurückgewonnen werden oder es muss auf andere Bereiche ausgewichen werden (Risiko Nr.33). Außerdem können schlecht gewählte Partner zu Abhängigkeiten, schlechten Verhandlungssituationen und erhöhten

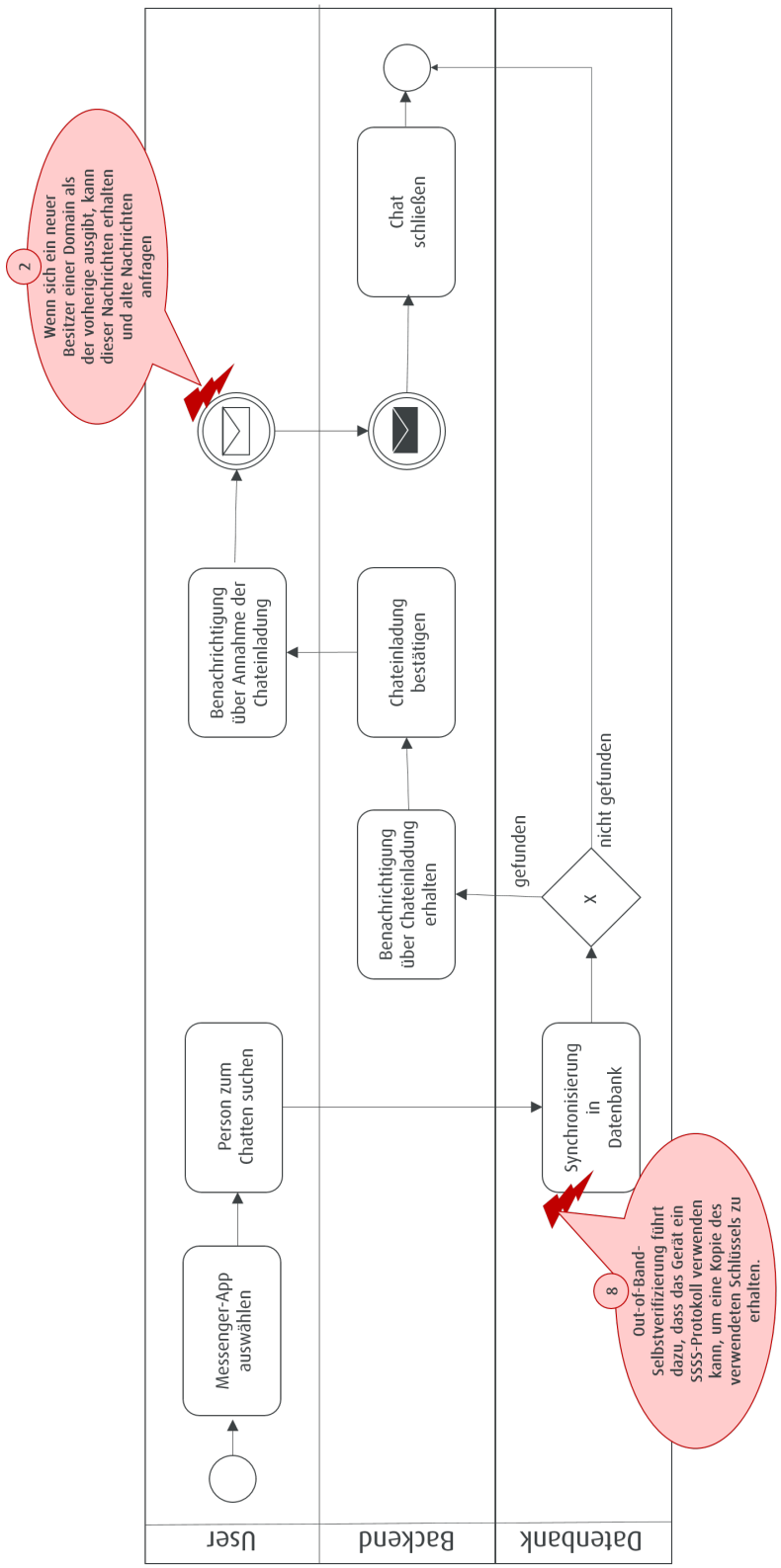


Abbildung 5.32: Identifizierte Risiken im Prozessmodell des Informationssteckbriefs

Preisen führen (BMJV, 2017). Man sollte berücksichtigen, dass das Risiko mit der Auswahl des Partners einhergeht, hohe Folgekosten zu erzeugen (Risiko Nr.34). Ebenfalls mit hohen Folgekosten verbunden sind Folgefehler, die durch Einbußen digitaler Souveränität entstehen können. So können Schäden wie z.B. der Wideraufbau von manipulierter oder zerstörter Infrastruktur derartige Kosten erzeugen (Risiko Nr.35). Sind erst die Software-Anwendungen beim Kunden mit bestimmten Anbietern im Betrieb, ergibt sich ein Lock-In-Effekt (vgl. Risiko Nr.36). Der Geschäftserfolg des Unternehmens unterliegt dann einer Abhängigkeit vom Anbieter und ist kaum mehr durch das Projekt selbst steuerbar. In den letzten Jahrzehnten haben sich die Wertschöpfungsnetze für viele Rohstoffe und Zwischenprodukte nach Asien verlagert (Huber, 2021). Neben den weit verbreiteten Gründen für diesen Trend (z.B. Kostenvorteile und günstige Transportwege) ist auch die Nähe zu den Großkunden ein entscheidender Vorteil, der die Arbeit an gemeinsamen Innovationen erleichtert (Kinkel et al., 2002). Das Risiko, das entsteht, wenn man digitale Souveränität versucht in Unternehmen zu stärken, ist, dass ein Verlust von Kostenvorteilen, der Nähe von Großkunden, und von günstigen Transportwegen die Folge sein kann (Risiko Nr.37) (Reisach, 2018). Es ist herausfordernd, Standards so zu setzen, dass man langfristig Marktführerschaften auf deutscher und europäischer Ebene unterstützt und man gleichzeitig keine Einbußen bei der Wettbewerbsfähigkeit macht (Risiko Nr. 38). Ein Management von digitaler Souveränität allein durch Inhouse-Systeme ist nur schwer möglich (Risiko Nr. 27). Es mangelt an geeigneten Managementsystemen, die hier wesentliche Unterstützung leisten können.

5.2.8 Gap-Analyse für den Messenger

5.2.8.1 Gaps in den Anforderungsmodellen des Messengers

Um im Sinne der digitalen Souveränität mehr Kontrolle über Hardware zu erhalten, muss man zunächst verstehen, wie man Vertrauenswürdigkeit von Hardware prüfen kann (Beyerer et al., 2018). Im Kontext des Kommunikationsprotokolls Matrix ist das Thema VS-NfD kritisch zu betrachten (vgl. Risiko Nr.10, Abbildung 5.33).

Das BSI hat für VS-NfD eine Bewertung des Matrix-Protokolls veröffentlicht (BSI, 2023). Es wird ersichtlich, dass in öffentlich zugänglichen Seiten behaup-

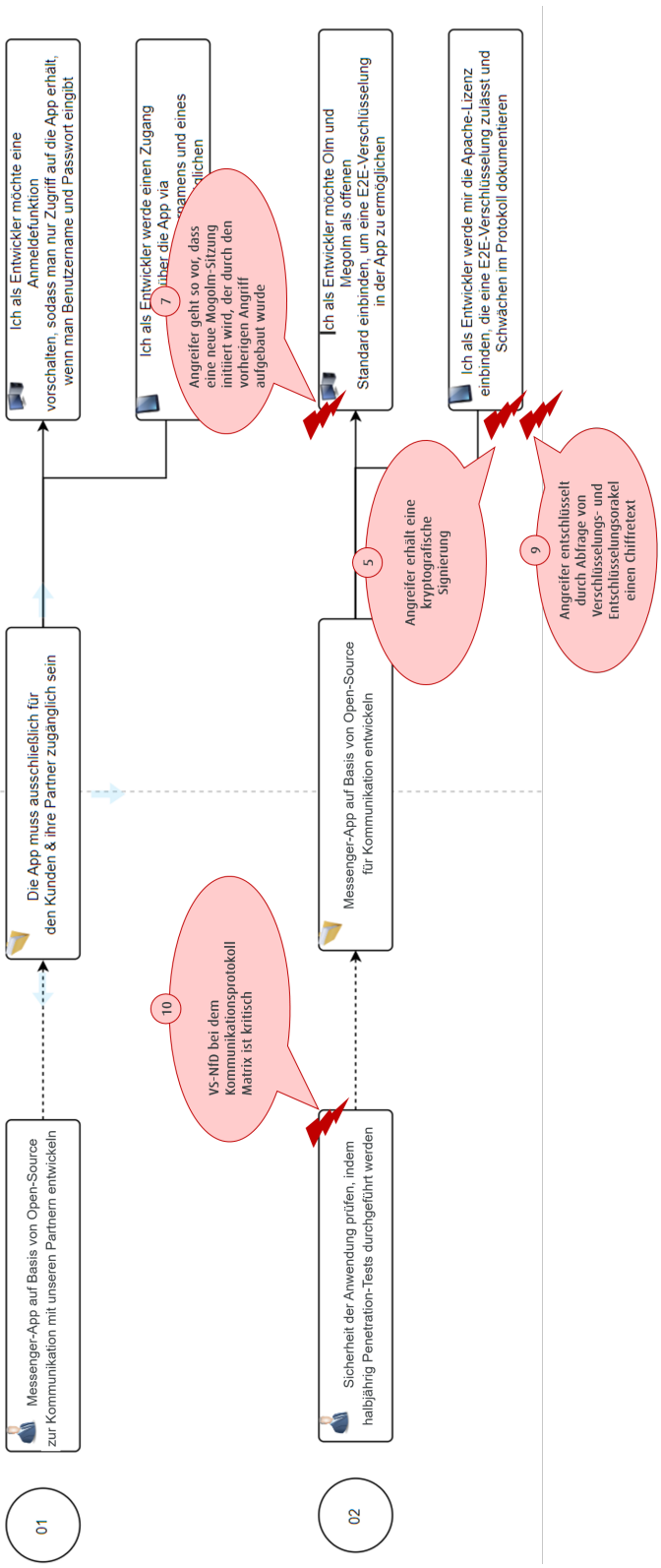


Abbildung 5.33: Identifizierte Risiken im AA-Modell für Anforderung Nr.2 (Messenger)

tet wird, dass matrix VS-NfD-tauglich sei. Die Einstufung von VS-NfD kann jedoch derzeit nur in Verbindung mit IT-Sicherheitsprodukten wie gehärteten Smartphones oder Laptops erfolgen. Im Kontext digitaler Souveränität gilt es auch Sicherheitsrisiken zu identifizieren. So kann ein Angreifer eine kryptografische Signierung erhalten und damit einen Verifikationsschlüssel (public key) anfragen oder seine Urheberschaft bestätigen (vgl. Risiko Nr.5). Im Rahmen eines anderen Vorgehens kann ein Angreifer auch eine neue Mogolm-Sitzung initiieren (vgl. Risiko Nr.7). Außerhalb der Hauptkommunikation kann ein Angreifer sich selbst verifizieren und eine Kopie des verwendeten Schlüssels erhalten (vgl. Risiko Nr.12, Abbildung 5.35). Zuletzt, kann der Angreifer auch durch eigenständige Abfragen von Entschlüsselungsorakeln einen Chiffretext entschlüsseln und so unautorisierten Zugang erhalten (vgl. Risiko Nr.9). Außerdem lässt sich feststellen, dass Angreifer sich unautorisierten Zugriff verschaffen können, indem sie sich als neuer Nutzer Räumen hinzufügen lassen und in diesem Zuge die Angreifer E2E-verschlüsselte Chats von Nutzern mitlesen (vgl. Risiko Nr.1, Abbildung 5.34).

5.2.8.2 Gaps im Architektur-Modell des Messengers

Weitere Sicherheitsrisiken ergeben sich, wenn ein Angreifer sich als ein neuer Besitzer einer bereits vergebenen Domain ausgibt (vgl. Abbildung 5.35). Bestehende Facetten der Softwareentwicklung werden nicht hinreichend durchdrungen. Insbesondere der Anteil Kryptographie wurde an ein externes Unternehmen ausgelagert, was zu einem erhöhten Abhängigkeitsverhältnis führt (vgl. Risiko Nr.11). Ein Angreifer könnte sich auch als vertrauenswürdiges Gerät ausgeben, Backups anfordern und so Zugriff auf weiterführende Daten erhalten (vgl. Risiko Nr.3). Auf architektonischer Ebene ist erkennbar, dass im Messenger-Projekt ein Homeserver angebunden ist. Hat ein Angreifer Zugriff auf diesen Homeserver, so kann er Kontrolle über die Raumteilnehmer erhalten und diese dazu zwingen Schlüssel zu teilen (vgl. Risiko Nr.4). Weitere Authentifizierungen eines Angreifers könnten über das Key Request Protokoll ermöglicht werden (vgl. Risiko Nr.6).

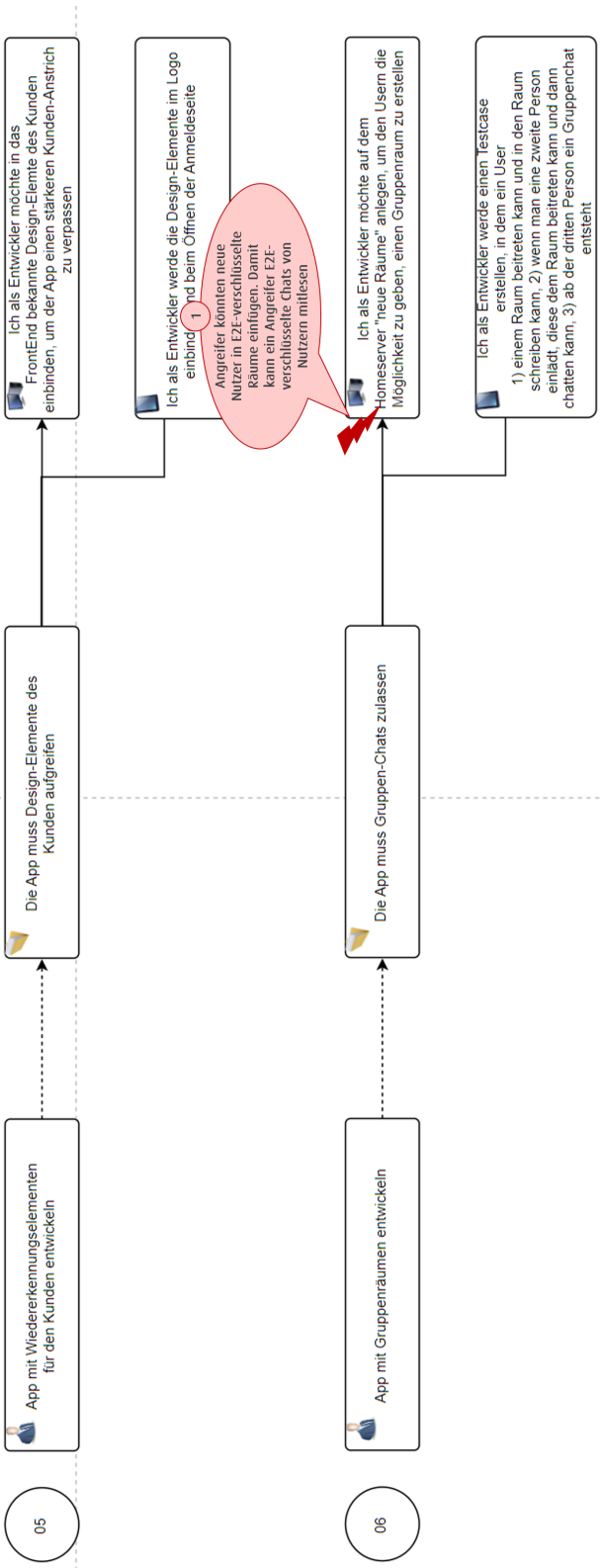


Abbildung 5.34: Identifizierte Risiken im AA-Modell für Anforderung Nr.6 (Messenger)

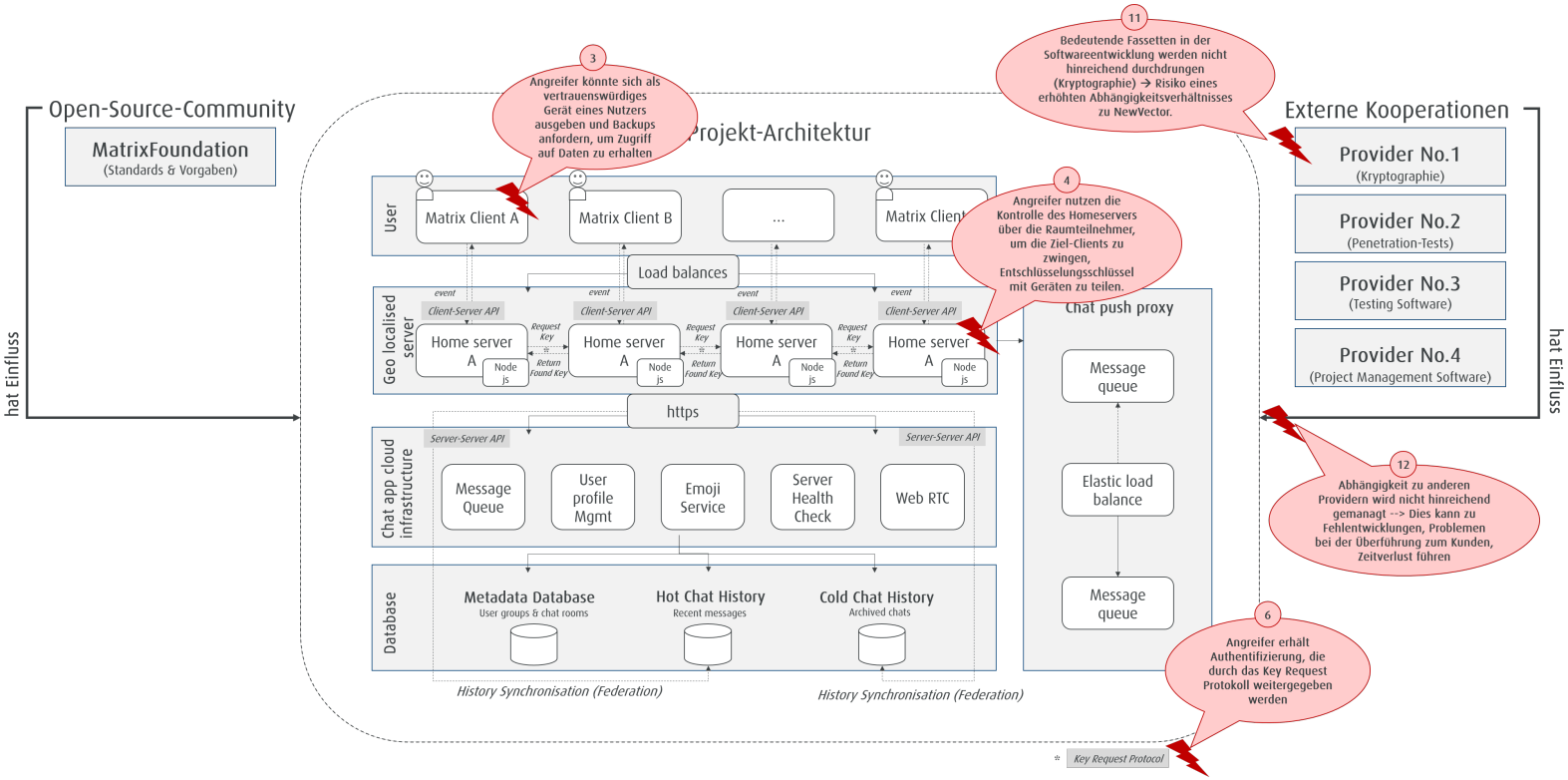


Abbildung 5.35: Identifizierte Risiken in der Projektarchitektur des Messengers

5.2.8.3 Gaps im Prozessmodell des Messengers

Eine Out-of-Band-Selbstverifizierung eines Angreifers kann dazu führen, dass das Gerät ein SSSS-Protokoll verwenden kann (vgl. Risiko Nr.8, Abbildung 5.36). Dies kann der Angreifer nutzen, um eine Kopie des verwendeten Schlüssels zu erhalten.

Wenn sich ein neuer Besitzer einer Domain als der vorherige ausgibt, kann dieser Nachrichten erhalten und alte Nachrichten anfragen (vgl. Risiko Nr.2).

5.2.9 Strategische Gaps für den Messenger

Die in dem Projekt vorhandenen Abhängigkeiten zu den anderen Providern können auf strategischer Ebene zu Fehlentwicklungen, Problemen bei der Überführung zum Kunden oder auch Zeitverlusten führen (vgl. Risiko Nr.12, Abbildung 5.35). Demnach ist das derzeit noch nicht weitreichend überdachte Management der Provider als Risiko zu sehen. Letztendlich lässt sich zusammenfassen, dass die Ergebnisse darauf hinweisen, dass digitale Souveränität ein Transformationsthema ist, das einen Mindset-Shift in Softwareentwicklungsprojekten braucht.

5.2.10 Anwendung der Affordanz-Theorie: Ableitung von Affordanzen zur Reduzierung der Gaps

Die Analyse liefert standardisierende, grundlegende, kontrollierende, organisatorische, sensibilisierende und integrierende Affordanzen. Tabelle 5.16 zeigt zunächst die ermittelten Affordanzen für das erste Projekt: den Messenger.

Wie den vorangegangenen Analysen zu entnehmen ist, werden „Standards und Richtlinien“ von der Matrix Foundation im Projekt bereitgestellt, um die ordnungsgemäße Verwendung des Matrix-Protokolls innerhalb der Open Source Gemeinschaft anzuleiten. Diese Fähigkeit wirkt sich auf die Entwicklung innerhalb des Projektes aus. „Know-How“ ist die zweite identifizierte Affordanz. Ein Drittanbieter ist für den kryptografischen Aspekt des Projekts verantwortlich. Dieser Anbieter bietet sein Know-how als Dienstleistung an. Diese Fähigkeit wirkt sich auch auf die Entwicklung und die Projektarbeit aus. Eine weitere Affordanz sind „Penetrationstests“. Hier ist ein anderer Drittanbieter für die Prüfung von Sicherheitsschwachstellen zuständig. Dies

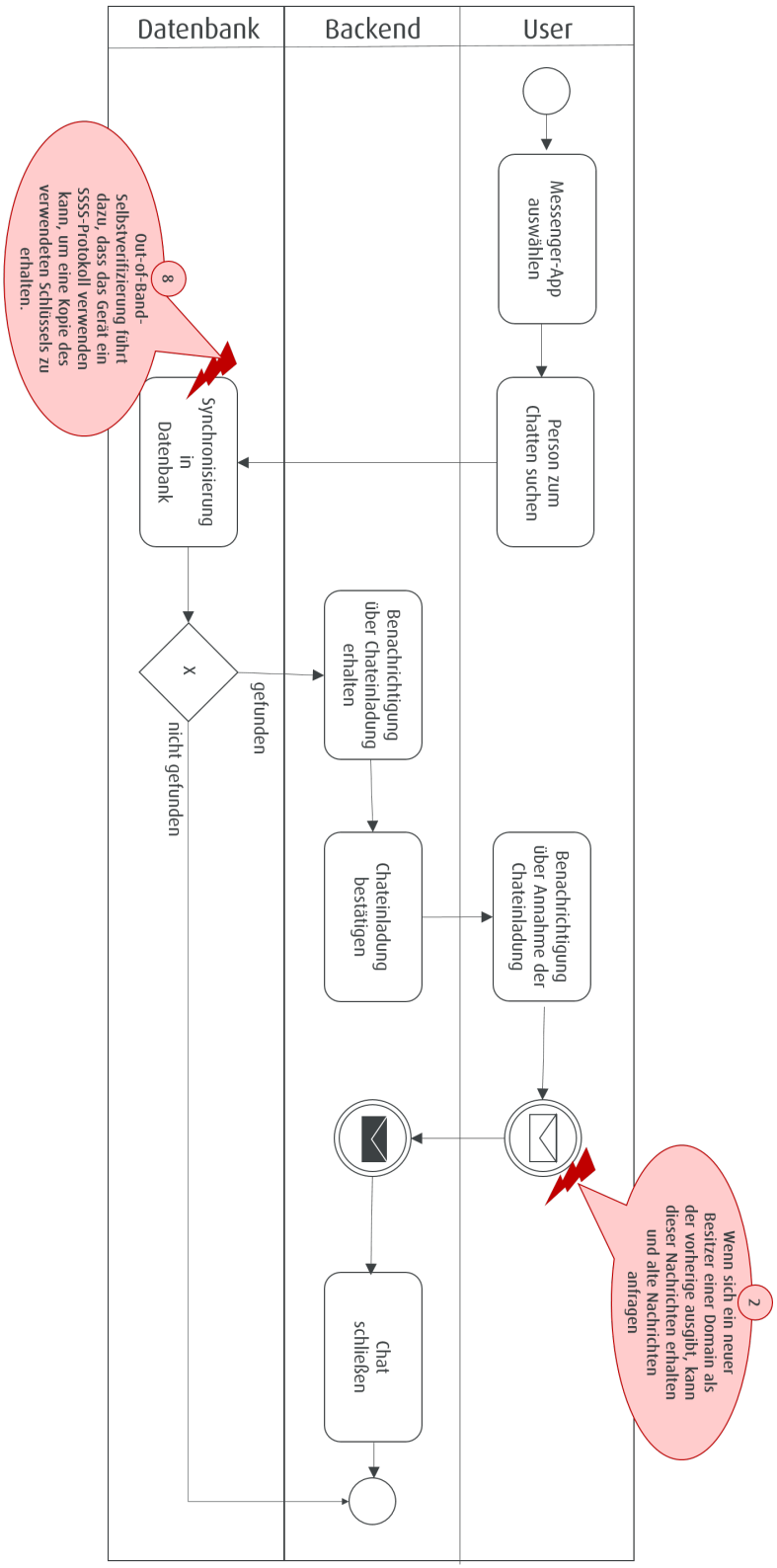


Abbildung 5.36: Identifizierte Risiken im Prozessmodell des Messengers

Open Source Project No. 1: Messenger				
Basic Affordances	Know How	Cryptography Know-How provided by provider 1	Provider 1 commissioned for the cryptography part of the project. This means that they are working on how the messenger can be made resistant to manipulation and how critical information can be securely encrypted.	Project work (development)
Controlling Affordances	Penetration Test	Penetration tests provided by provider 2	Provider 2 is responsible for penetration tests within the project. The six-monthly test is intended to ensure that security vulnerabilities in Messenger are detected quickly. SecuSmart is also responsible for proposing mitigation measures, which the project team will then implement.	Project work (speed)
	Testing Software	Eggplant provided by provider 3	Provider 3 offers testing software that provides test cases identified by AI analysis and uses a twin approach to allow developers to navigate through the system under test as a user. As a testing software, Eggplant offers a fast way to check whether the messenger is doing what it is supposed to do.	Project work (development)
Organizational Sensemaking Affordances	Project Management Tools	Jira provided by provider 4	With Jira, Provider 4 offers a web application that is used to track project processes. Jira has established itself as a monopolist for task management in software development projects for small and medium-sized development teams.	Project work (project management - quality, speed, budget)
		Confluence provided by provider 4	Provider 4 offers Confluence as software to support knowledge sharing, document management and the creation of wikis in companies. It is used as a documentation platform in this project.	Project work (project management - quality, speed, budget)
Standardizing Affordances	Standards and Guidelines	Standards and guidelines for matrix (Matrix Foundation)	Matrix Foundation is an open source community that sets standards for the use of the Matrix communication protocol and promotes the development of Matrix.	Project work (development)

Tabelle 5.6: Affordanzanalyse Open Source Projekt Nr.1: Messenger

wirkt sich auf die Geschwindigkeit des Projektes aus. Der letzte Anbieter bietet Testsoftware an. Die „Testsoftware“ ist eine Affordanz, da sie den Entwicklern als technische Dienstleistung angeboten wird und sich auf die Projektarbeit auswirkt. Die Testsoftware wird verwendet, um zu überprüfen, ob die Entwicklung des Messengers wie erwartet funktioniert. Bei den letzten beiden Möglichkeiten handelt es sich um „Projektverwaltungswerkzeuge“. Jira ist eine beliebte Webanwendung für die Projektverfolgung. Confluence bietet Software für die Dokumentenverwaltung und den Wissensaustausch. Diese beiden Affordanzen wirken sich auf die Verwaltung der Projektarbeit aus. Tabelle 5.7 zeigt die Ergebnisse der Affordanzanalyse für das zweite Open Source Projekt: den Informationssteckbrief.

Die erste identifzierte Affordanz hier ist „Front-End-Lösung“. Die im Projekt verwendete Front-End-Lösung basiert auf Open Source und wird am Ende an den Kunden geliefert. Das Front-End wirkt sich auf die Projektarbeit aus. Es wirkt sich auch auf die Kundenzufriedenheit aus, da es die Benutzerfreundlichkeit des Systems erheblich beeinflusst. Die nächste Affordanz ist das „Open Source System“. Die im Projekt verwendete Betriebssystemlösung ist Kubernetes, ein bei Entwicklern beliebtes System zur Verwaltung von containerisierten Anwendungen. Die Entscheidung, Kubernetes zu verwenden, wirkt sich auf die Projektarbeit aus, insbesondere auf das finale Produkt, das an den Kunden zu liefern ist. Außerdem konnte anhand der Projektarchitektur die Art der Dokumentenverwaltung erläutert werden. Die entsprechende Affordanz ist „Datenbankmanagementsystem“. Das Datenbankmanagementsystem hat Auswirkungen auf die Entwicklung und damit auf die Projektarbeit. Neben dem Datenbankverwaltungssystem ist eine weitere Affordanz die „Datenbank“. Die in diesem Projekt verwendete Open Source Datenbank wirkt sich ebenfalls auf die Entwicklung aus. Auch Cloud-Kapazitäten werden genutzt. Die verwendete Cloud-Computing-Plattform ist AWS (Amazon Web Services). Die Entscheidung für AWS wirkt sich auf die Entwicklungsarbeit aus. Daher ist „Cloud-Kapazitäten“ eine weitere Affordanz. „Automatisierte Extraktionen“ werden im Projekt verwendet, um Texte, Informationen und Ortsnamen zu extrahieren. Automatisierte Extraktionen wirken sich auf die Geschwindigkeit und Entwicklung des Projektteams aus. Auch „KI-Modelle“ ist eine

Cluster	Affordance	Exact solution	Explanation	Impact
Open Source Project No. 2: Information Brief				
Integrating Affordances	Front end solution	Grafana	Grafana is an open source application used in the project as a front-end solution for data analysis	Project work (customer provision), customer satisfaction (usability)
	Open source system	Kubernetes	Kubernetes is an open source system for developers. It was developed by Google to provide, manage and automate container-based applications.	Project work (customer provision), multi-provider management
Organizational Sensemaking Affordances	Database management solution	MongoDB	MangoDB is a modern database management solution from MangoDB, Inc. that enables developers to make their data queryable and quickly identifiable through a collection of JSON documents.	Project work (development)
Basic Affordances	Database	PostgreSQL	PostGreSQL is an open source database. It was developed in the 1980s by POSTGRES and is now being further developed by an open source community. It has been meticulously and continuously improved by a worldwide team of developers, making PostGreSQL one of the most convenient databases (for both relational and non-relational databases). Developers value the database for its flexibility (open standards) and reliability (largely compliant with the SQL standard SQL:2011).	Project work (development)
Integrating Affordances	Cloud Capacity	AWS (Amazon Cloud)	AWS is more than just the provision of cloud capacity. Compared to other market players, AWS scores points with developers thanks to its extensive density of functions (over 200 services). These services make it relatively easy to work with artificial intelligence (AI), machine learning, big data analytics and internet of things	Project work (development), multi-provider management,
	Automated extractions	Text extraction	Text Extraction is a text tool for extracting JSON into a TXT file.	Project work (development, speed)
		Extraction of information	Information Extraction aims to automatically extract structured information from unstructured text using Spark NLP. Spark NLP offers several ways to extract, analyze and use entities from text data.	Project work (development, speed)
		Extraction of geoinformation	Geo Information Extraction is a way to extract place names from text. With feedback to Open-Street-Map, the Python geoparsing library enables the analysis of large amounts of data. This approach is an alternative to the use of third-party APIs (e.g. Google Geocoding API).	Project work (development, speed)
	AI models	Natural language processing (NLP) model	The NLP model used in the project is called paraphrase-multilingual-MiniLM-L12-v2 and is an already pre-trained open source product that was used for this use case. While it achieves very good results in English, it should be noted that the developers are supposed to perform a prediction of the political situation in a country from the study environment. The output should be in German language.	Result at the customer (forecast results political situation in study environment)
	Open source product	Spring Boot	A Spring Boot is an open source product that developers use to develop microservices or web apps based on Java frameworks. Java Spring Boot allows to create stand-alone applications quickly and easily.	Project work (development)
	Collection of algorithms and APIs	Cognitive service	Cognitive Service is a collection of algorithms and programming interfaces for AI applications. The market monopolist in the field of cognitive services is Microsoft. Microsoft offers tools in cognitive services to design AI services and enable natural language understanding.	Project work (development), multi-provider management
	Search technology	Semantic search	Semantic Search enables contextual searches in the dashboard. To enable contextual searches, developers have to develop them on an open-source basis. Alternatively, they can use elasticsearch and Kibana to create a semantic search. In this project, the focus was on in-house development.	Project work (development)

Tabelle 5.7: Affordanzanalyse Open Source Projekt Nr.2: Informationsbrief

Affordanz, da sie im Projekt verwendet werden, um Vorhersagen zu treffen. KI-Modelle wirken sich auf das Kundenergebnis aus. Die letzten Affordanzen sind „Open Source Produkt“, „Sammlung von Algorithmen und APIs“ und „Suchtechnologie“. Alle drei Affordanzen beeinflussen die Entwicklungsarbeit.

5.2.10.1 Ergebnisse aus dem Vergleich zwischen dem Ist-Zustand und dem Soll-Zustand

Gap Nr. 1 Die Analyseergebnisse zeigen, dass die Affordanzen „Standards und Richtlinien“ und „Know-how“ die Entwicklungsarbeit der Projektteams beeinflussen, während „Penetrationstests“ die Entwicklungsgeschwindigkeit beeinflussen (siehe Abschnitt 5.2.11). Die Autonomie der Projektteams wird durch externe Stiftungen und Unternehmen eingeschränkt (siehe Abschnitt 5.2.5 und 5.2.6). Das Konzept der digitalen Souveränität erfordert den Erwerb der notwendigen Ressourcen und Fähigkeiten, um mehr Autonomie im digitalen Raum zu erlangen (siehe Abschnitt 5.2.7).

Identifizierte Lücke: Es liegt eine Lücke vor, die einen Balance zwischen der Einhaltung von Standards und Richtlinien sowie der Förderung von Fähigkeiten zur Erhöhung der Autonomie im digitalen Raum erfordert.

Gap Nr. 2 Die Affordanzen „Testsoftware“, „Projektmanagement-Tools“ und „Cloud-Kapazität“ haben einen erheblichen Einfluss auf die Arbeit der Entwickler und das Management von Open Source Projekten (siehe Abschnitt 5.2.11). Ein Vergleich des aktuellen und des gewünschten Zustands zeigt, dass Projektteams auf externe Partner für Fachwissen, Softwarelösungen und Infrastruktur angewiesen sind (siehe Abschnitt 5.2.5 und 5.2.6). Allerdings zielt das Konzept der digitalen Souveränität darauf ab, starke Abhängigkeiten zu reduzieren (siehe Abschnitt 5.2.7).

Identifizierte Lücke: Dies zeigt eine Lücke zwischen externen Angeboten, die zu Anbieterabhängigkeiten führen, und der Notwendigkeit größerer Unabhängigkeit. Unternehmen, die nachhaltigere Geschäftsmodelle durch digitale Souveränität anstreben, müssen diese Lücke sorgfältig berücksichtigen.

Gap Nr. 3 Die Analyse der Affordanzen „Front-End-Lösung“, „OS-System“, „Datenbank“ und „Datenbankmanagementlösung“ zeigt, dass sie sowohl die Kundenzufriedenheit als auch die Projektarbeit in Open Source Projekten

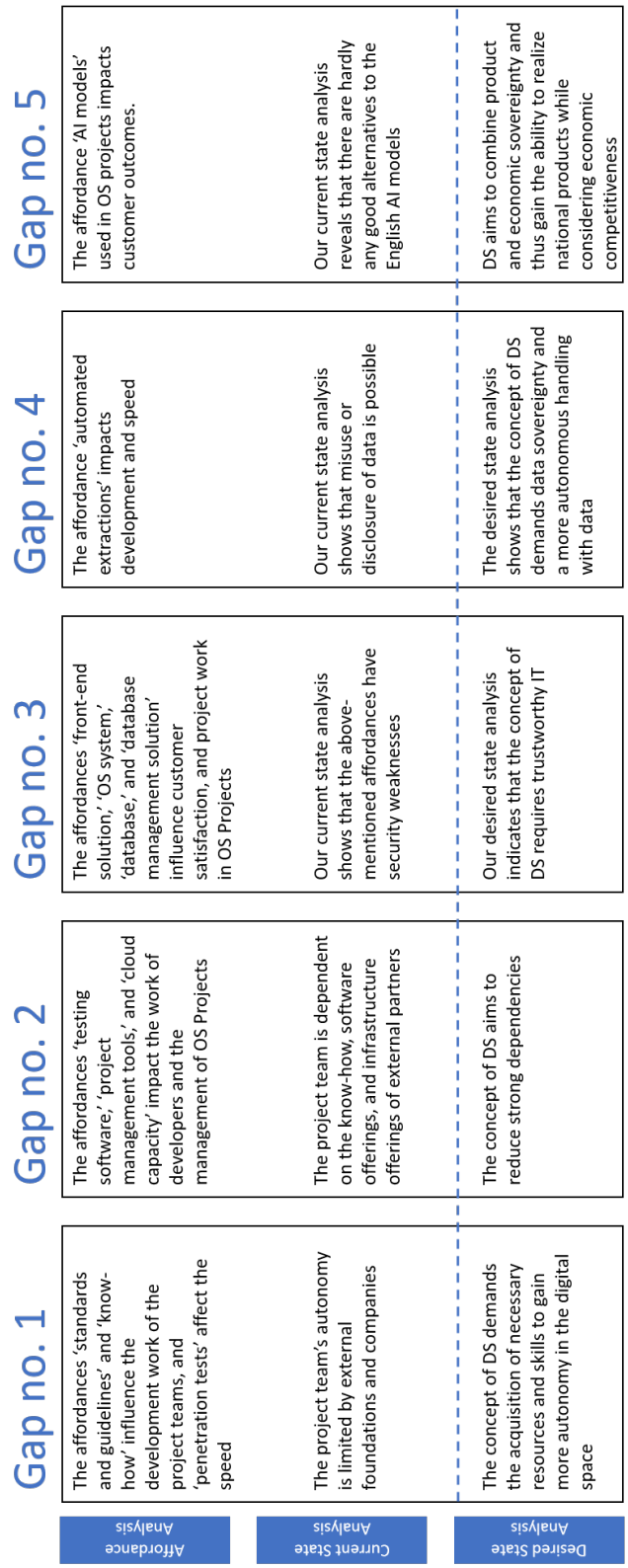


Abbildung 5.37: Übersicht über den Vergleich von Ist- und Soll-Zustand

beeinflussen (siehe Abschnitt 5.2.11).

Identifizierte Lücke: Die Analyse des aktuellen Zustands zeigt Sicherheitslücken bei diesen Affordanzen (siehe Abschnitt 5.2.5 und 5.2.6). Im Gegensatz dazu deutet die Analyse des gewünschten Zustands darauf hin, dass digitale Souveränität vertrauenswürdige IT erfordert, um eine sichere und souveräne digitale Umgebung zu gewährleisten (siehe Abschnitt 5.2.7).

Gap Nr. 4 Die Affordanz „automatisierte Extraktionen" beeinflusst sowohl den Entwicklungsprozess als auch die Geschwindigkeit des Projekts (siehe Abschnitt 5.2.11).

Identifizierte Lücke: Die zugrundeliegende Analyse des aktuellen Zustands zeigt das Risiko von Datenmissbrauch oder unbefugter Offenlegung (siehe Abschnitt 5.2.5 und 5.2.6). Der gewünschte Zustand hingegen betont die Bedeutung von Datensouveränität und einem selbstbestimmten Umgang mit Daten (siehe Abschnitt 5.2.7).

Gap Nr. 5 Es wurde auch die Affordanz „KI-Modelle" in Open Source Projekten untersucht und festgestellt, dass sie einen erheblichen Einfluss auf die Kundenergebnisse haben.

Identifizierte Lücke: Die Analyseergebnisse weisen darauf hin, dass im aktuellen Zustand ein Mangel an guten Alternativen zu den weit verbreiteten englischsprachigen KI-Modellen vorliegt (siehe Abschnitt 5.2.5 und 5.2.6). Allerdings zielt digitale Souveränität darauf ab, Produkt- und Wirtschaftssouveränität zu vereinen, indem sie die Entwicklung nationaler KI-Modelle ermöglicht, während gleichzeitig die wirtschaftliche Wettbewerbsfähigkeit gewahrt bleibt (siehe Abschnitt 5.2.7).

Gap Nr. 6 Die Analyse der Affordanzen „Sammlung von Algorithmen und APIs" sowie „Suchtechnologie" zeigten einen wesentlichen Einfluss auf die Entwicklungsprozesse (siehe Abschnitt 5.2.11). Den Daten nach haben die Projektteams positive Erfahrungen mit Open Source Lösungen gemacht, insbesondere mit den Komponenten, die für die Entwicklung von Microservices und Webanwendungen genutzt werden. Dies steht im Einklang mit dem Prinzip, dass technologische Unabhängigkeit durch Open Source gefördert werden kann (siehe Abschnitt 5.2.7).

Wie können die Affordanzen angepasst werden, um mehr digitale

Souveränität zu erreichen?

Balance zwischen Standards, Richtlinien und Know-how Um digitale Souveränität zu stärken, müssen die Affordanzen „Standards und Richtlinien" sowie „Know-how" sorgfältig vereint werden (siehe Gap Nr. 1). Dies bedeutet:

- Kompetenzentwicklung durch Schulungen und Weiterbildung ist entscheidend.
- Gleichzeitig sind klare politische und unternehmerische Regelungen zur Einhaltung von Standards zu gewährleisten.

Diese Ergebnisse stimmen mit Pohle (2020) überein, die ebenfalls betont, dass Kompetenzentwicklung und regulatorische Vorgaben für digitale Souveränität von zentraler Bedeutung sind. Außerdem bestätigt der erste Punkt die Ergebnisse aus der letzten Studie, in denen das Thema Kompentenz als Herausforderung digitale Souveränität umzusetzen, aufgedeckt wurde (vgl. Kapitel 5.1).

Reduzierung der Abhängigkeit von externen Anbietern Die Affordanzen „Testsoftware", „Projektmanagement-Tools" und „Cloud-Kapazität" weisen starke Abhängigkeiten von Drittanbietern auf (siehe Gap Nr. 2). Die Ergebnisse führen zu folgenden Empfehlungen für Unternehmen:

- Alternative digitale Partner in Betracht ziehen, um ihre Abhängigkeit von einzelnen Anbietern zu verringern.
- Multi-Provider-Strategien verfolgen, um die Flexibilität in der Software-, Tool- und Infrastrukturwahl zu erhöhen.

Diese Sichtweise steht im Kontrast zu Floridi (2020), der sich für politisch motivierte Alternativen ausspricht. Die Ergebnisse unterstreichen, was bereits im DISO-A-Modell vermutetet wurde: dass digitale Souveränität nicht nur durch politische Initiativen, sondern auch durch strategische Unternehmensentscheidungen vorangetrieben werden sollte. Softwareentwicklung mit Open Source sollte neu gedacht werden, souveräner.

Stärkung der Cybersicherheit und IT-Sicherheit Die Einführung von digitaler Souveränität erfordert einen starken Fokus auf Cybersicherheit in Open Source Projekten, insbesondere in Bezug auf die Affordanzen „Front-End-Lösung",

„Open Source System“, „Datenbank“ und „Datenbankmanagementlösung“ (siehe Gap Nr. 3). Zur Risikominderung sollten Unternehmen:

- Sicherheitslücken in diesen Affordanzen systematisch bewerten.
- Risikominimierungsmaßnahmen ergreifen, die auf Daten- und Produktsouveränität ausgerichtet sind.

Erste Vermutungen zu der Notwendigkeit einer Risikobewertung für digitale Souveränität, sind dem DISO-A-Modell zu entnehmen. Die vorliegenden Ergebnisse bestärken nicht nur die Ergebnisse aus Kapitel 4.3, sondern liefern ein tiefergehendes Verständnis dazu, an welchen Stellen Sicherheitslücken vorliegen können und wo Risiken sinnvoller Weise im Kontext digitaler Souveränität zu mitigieren sind.

Förderung der Datensouveränität durch automatisierte Extraktionen Die Affordanz „automatisierte Extraktionen“ sollte mit den Prinzipien der Datensouveränität in Einklang gebracht werden. Um die Herausforderungen von Gap Nr. 4 zu bewältigen, empfiehlt sich die Entwicklung einer umfassenden Strategie für die Themen Datenmanagement und Datensouveränität in Unternehmen. Diese Ergebnisse decken sich mit den Ergebnissen von Hummel et al. (2021), die technische, organisatorische und rechtliche Rahmenbedingungen zur Erreichung der Datensouveränität beschreiben. Im DISO-A-Modell wurden die Themen Datensouveränität und Strategie entkoppelt voneinader betrachtet. Die hier vorliegenden Ergebnisse weisen darauf hin, dass eine Kopplung sinnstiftender ist.

Förderung der KI-Souveränität durch strategische Allianzen Die Affordanz „KI-Modelle“ sollte auf eine strategische Ebene gehoben werden (siehe Gap Nr. 5). Unsere Analyse zeigt eine kritische Lücke bei nicht-englischen KI-Modellen, die die Stärkung digitaler Souveränität einschränkt. Daher sollten Unternehmen:

- Strategische Allianzen bilden, um Synergien in der KI- und NLP-Forschung zu nutzen.
- In nationale KI-Entwicklung investieren, um Abhängigkeiten von ausländischen Modellen zu reduzieren.

Das bestätigt unsere Ergebnisse aus Abschnitt 4.3. Hier hatten die Professoren mehr KI-Investitionen und Forschungsföderung gefordert.

Fortsetzung der Nutzung von Open Source Lösungen

Schließlich empfiehlt es sich die Affordanzen „Sammlung von Algorithmen und APIs“ sowie „Suchtechnologie“ in ihrer derzeitigen Form beizubehalten. Projektteams haben positive Erfahrungen mit diesen Affordanzen gemacht, was die Bedeutung von Open Source Ökosystemen für die digitale Souveränität unterstreicht.

Zusammenfassung der Ergebnisse

Eine Übersicht der ermittelten Ergebnisse aus der Gap-Analyse findet sich im Anhang. Die Tabellen 14 bis 16 zeigen, welches operative oder strategische Risiko auf Basis des Vergleichs zwischen der Ist-, und Soll-Situation abgeleitet wurde und die Empfehlungen zum Umgang mit dem Risiko.

5.2.11 Fazit, Limitationen, Ausblick

Dieses Kapitel zeigt die Möglichkeiten und Herausforderungen einer Einbettung von digitaler Souveränität in Open Source Projekten.

Die Ergebnisse bestätigen, dass das Konzept von digitaler Souveränität genutzt werden kann, um mehr autonomes Handeln im digitalen Raum zu erreichen. Allerdings zeigen die Ergebnisse auch, dass es für OS-Projektteams noch einige Herausforderungen gibt, sich an digitaler Souveränität auszurichten und Affordanzen souverän zu gestalten. Die Herausforderungen, die die Projektteams bei der Umsetzung von digitaler Souveränität sehen, sind Abhängigkeiten von Stiftungen, Abhängigkeiten von spezifischer proprietärer Software und Abhängigkeiten von Monopolisten. Fehlende Expertise, hohe Sicherheitsanforderungen und fehlende Alternativen zu englischen NLP-Modellen verstärken die Herausforderungen.

Die Daten zeigen, dass die Affordanzen aus den beiden analysierten Projekten wie folgt angepasst werden sollten: Erstens: „Standards und Richtlinien“ mit „Know-How“ kombinieren. Zweitens sollten alternative, sichere Partner für die Affordanzen „Penetrationstests“, „Testsoftware“, „Cloud-Kapazität“ und „Projektmanagement-Tools“ in zukünftigen Projekten in Betracht gezogen werden. Drittens: Die Affordanzen „Front-End-Lösung“, „Open Source System“,

„Datenbank“ und „Datenbankmanagementlösung“ sind auf Vertrauenswürdigkeit und Produkthoheit ausrichten. Viertens: „Automatisierte Extraktionen“ mit Datenhoheit in Einklang bringen. Fünftens: Berücksichtigung wirtschaftlicher und wettbewerblicher Herausforderungen und Bilden strategischer Allianzen, um KI-Modelle souveräner zu gestalten. Damit trägt die Forschung zu neuen Ergebnissen in zwei unterschiedlichen Forschungsbereichen bei: der Affordanz-Forschung und die Digitale-Souveränitäts-Forschung.

Künftige Forschung kann sich mit der Bewertung und Messung der hier aufgezeigten Maßnahmen beschäftigen. So kann geprüft werden, welche Maßnahmen konkret einen positiven Einfluss auf souveräne Softwareentwicklung haben. Auch eine Analyse von weiteren Projekten ist interessant, um ein noch besseres Bild darüber zu erhalten, wie sich Unternehmen aufstellen müssen, um digital souverän zu werden.

Als Limitation ist aufzuführen, dass hier digitale Souveränität lediglich auf Arbeitsebene betrachtet wird. Es liegt keine Vollständigkeit bei den betrachteten Mechanismen vor. So kann davon ausgegangen werden, dass es noch andere Gestaltungselemente als die Untersuchten gibt, um digitale Souveränität zu stärken.

Jetzt, wo ein besseres Verständnis darüber erlangt werden konnte, welche Möglichkeiten und Herausforderungen es gibt, mit Open Source digitale Souveränität zu stärken, sollen im nächsten Forschungsschritt nun die Lieferketten von Unternehmen genauer betrachtet werden. Es wird der Frage nachgegangen, wie der Softwareeinführungsprozess von Unternehmen digital souveräner gestaltet werden kann. Souveränere Lieferketten sind auch ein Faktor des DISO-A-Modells.

5.3 Werkzeug Beschaffungsstrategie: Soft Design Science Studie zu Softwareeinführung im Kontext digitaler Souveränität

In einer ersten Version wurden die Ergebnisse, die hier vorgestellt werden, hier veröffentlicht: *Klare, M., Hrestic, R., Stelter, A., and Lechner, U. (2025). Digital Sovereignty and Digital Transformation Practice Recommendation for the Software Life Cycle Process. International Conference on Digital Sovereignty, Procedia Computer Science, 254, 221–229. /https://doi.org/10.1016/j.procs.2025.02.081* und *Stelter, A., Klare, M., Lechner, U. (2025). Digital Sovereignty and Digital Transformation Extension for the Software Life Cycle Process in ISO/IEC/IEEE 12207:2017. Artificial Intelligence in Context of Digital Sovereignty. -> **to appear***. Dieses Papier wurde in Zusammenarbeit mit Razvan Hrestic und Aida Stelter geschrieben. Während Razvan Hrestic den Fokus auf die Themen Softwareeinführung/Softwarelebenszyklus legte und Aida Stelter auf das Thema digitale Transformation, habe ich die Ergebnisse für das Thema digitale Souveränität erhoben, analysiert, ausgewertet und die Evaluation der der ISO/IEC/IEEE 12207:2017-Erweiterung alleinig durchgeführt. Die Entwicklung der ISO/IEC/IEEE 12207:2017-Erweiterung erfolgte als Beitrag zu gleichen Teilen durch Aida Stelter und mich.

5.3.1 Einleitung

Die Frage, wo digitale Souveränität in Unternehmen eine Rolle spielt, lässt Mörl (2024) auf die Lieferketten stoßen. Gerade die Softwareeinführung der Zukunft im Rahmen der Lieferketten von Unternehmen muss sich zunehmend strategisch positionieren, indem sie den Anforderungen nach mehr Selbstbestimmung, Sicherheit und Unabhängigkeit im Sinne der digitalen Souveränität gerecht wird (Andenmatten, 2023; Rehm & Schulz, 2020). Unternehmen sollten sich zunehmend mit den Anforderungen der digitalen Transformation auseinandersetzen und stehen damit vor vielfältigen Herausforderungen bei der Einführung und Verwaltung von Softwaresystemen (Appelfeller & Feldmann, 2023; Schuh et al., 2017). So wird der Zusammenhang digitaler Transformation und digitaler Souveränität deutlich. Es bleibt jedoch unklar, welche Maßnahmen ergriffen werden können und wie die Anforderungen im Softwareeinführungsprozess unter Berücksichtigung dieser Konzepte zu

managen sind. In der Projektmanagement-Literatur dreht sich die Diskussion häufig um kritische Erfolgsfaktoren (Chow & Cao, 2008; Müller & Jugdev, 2012). Dies führt zu der Frage, wie Softwaresysteme unter Berücksichtigung der Anforderungen im Kontext von digitaler Transformation und digitaler Souveränität erfolgreich implementiert werden können. Ziel dieser Studie ist die Entwicklung praxisorientierter Leitlinien in Form einer ISO-Erweiterung unter Berücksichtigung sowohl der Management- als auch der Praxissicht. In diesem Kapitel sind die folgenden Forschungsfragen zu beantworten:

- Was sind die Anforderungen im Kontext der digitalen Transformation und der digitalen Souveränität bei der Einführung von Software in Unternehmen?
- Wie sieht eine Architekturperspektive zur Integration von Anforderungen der digitalen Souveränität und der digitalen Transformation in ein bestehendes Framework aus?

Kapitel 5.3.2 umfasst das Forschungsdesign und Kapitel 5.3.3 die Analyseergebnisse. Hier werden die Ergebnisse der Online-Umfrage zu den Themen Software-Einführung, digitale Transformation und digitale Souveränität aufgeführt. Auch das Mapping der digitalen Souveränitätserweiterung und der digitalen Transformationserweiterungen zum ISO/IEC/IEEE 12207:2017 Standard ist hier zu finden. Schließlich sind die Schlussfolgerungen und die Einschränkungen sowie ein Ausblick im Kapitel 5.3.4 aufgeführt.

5.3.2 Forschungsdesign

Als Forschungsdesign dient die in dieser Arbeit bereits vorgestellte Soft Design Science Methodology (SDSM), die von Pries-Heje et al. (2014) geleitet wird. Wie in Tabelle 5.8 dargestellt, liefert die Methode acht Forschungsaktivitäten.

Der erste Forschungsschritt besteht in diesem Kapitel darin, das spezifische Problem - Anforderungen im Softwarelebenszyklus im Kontext der digitalen Transformation und der digitalen Souveränität - zu beschreiben und besser zu verstehen.

Im zweiten Forschungsschritt werden konkrete Anforderungen aus der realen Problemstellung extrahiert. Zu diesem Zweck wurde eine Online-Umfrage

Forschungsaktivitäten	Reale Welt oder Design-Thinking-Welt?
1. Das spezifische Problem verstehen	Real
2. Generelles Problem und generelle Anforderungen kreieren	Design Thinking
3. Generelle Lösung intuitiv erfassen und ableiten	Design Thinking
4. Ex Ante Evaluation (generell)	Design Thinking
5. Spezifische Lösung für das spezifische Probelm entwickeln	Design Thinking
6. Ex Ante Evaluation (spezifisch)	Real
7. Spezifische Lösung konstruieren	Real
8. Ex Post Evaluation	Real

Tabelle 5.8: Soft Design Science Methode (Quelle: Pries-Heje et al. (2014))

konzipiert und durchgeführt. Die Umfrage war von August bis Oktober 2024 online. Teilnehmende waren ausgewählte Unternehmen, die einen Einladungslink via LinkedIn oder E-Mail zugeschickt bekommen haben. Die Umfrage ist in drei Bereiche geteilt: 1) Fragen zur Softwareeinführung, 2) Fragen zu digitaler Transformation und 3) Fragen zu digitaler Souveränität (siehe Anhang). Aufgrund der Tatsache, dass in diesem Kapitel digitale Souveränität als Transformationsversuch verstanden wird, sind für die Anteile 2) und 3) die gleichen Fragen formuliert worden. Das ermöglicht eine Überprüfung, ob sich die Herausforderungen im Kontext digitaler Transformation und digitaler Souveränität wesentlich voneinander unterscheiden. Die Umfrage konzentriert sich auf Anforderungen von Unternehmen in Deutschland, sowohl im öffentlichen als auch im privaten Sektor.

Im dritten Forschungsschritt werden die Anforderungen abstrahiert, um sie auf eine allgemeine Problemklasse zuzuschneiden. Auf Basis der Umfrageergebnisse zeigen sich Herausforderungen und Maßnahmen, die für eine Einführung von Software unter Berücksichtigung von digitaler Souveränität und digitaler Transformation wesentlich sind.

Im vierten Forschungsschritt wird das allgemeine Lösungsdesign intuitiv abgeleitet und als allgemeine Anforderungen formuliert. Hierfür sind für die Anteile digitale Transformation und digitale Souveränität Cluster zu bilden und die Beziehungen zwischen diesen Clustern zu analysieren. In diesem Schritt wird kritisch reflektiert, ob digitale Souveränität als Transformationsversuch verstanden werden könnte.

Der fünfte Forschungsschritt sieht vor, dass die allgemeinen Anforderungen an das Lösungsdesign mit dem spezifischen Problem verglichen werden, um dann im sechsten Schritt Lösungskomponenten auf Basis von Handlungsbausteinen zu identifizieren, die die allgemeinen Anforderungen erfüllen.

Im siebten Forschungsschritt folgt die Vorstellung des neuen Artefakts: die ISO/IEC/IEEE 12207:2017 Erweiterung, die einen Leitfaden für einen souveräneren Softwarelebenszyklus in Unternehmen darstellen soll. Hier finden sich Empfehlungen für den Umgang mit den Anforderungen zur digitalen Transformation und der digitalen Souveränität im Kontext des Softwarelebenszyklus wieder. Ausgangspunkt sind damit die Daten auf Basis der Umfrage.

Der achte und damit letzte SDSM-Schritt ist die Evaluation. Vor dem Hintergrund der Frage, ob die ISO-Erweiterung einen wesentlichen Beitrag für die Praxis liefern kann, fällt die Entscheidung auf die Evaluation der Ergebnisse auf Basis praxisnaher Literatur. Hier folgt eine Einbeziehung von Studien mit hohem Praxisbezug und konkreten Branchendaten. Letzter Analyseschritt ist eine Überprüfung, ob sich die Prozessbestandteile aus dem neu entworfenen Artefakt (die ISO/IEC/IEEE 12207:2017) auch in industrienaher Literatur wiederfinden.

5.3.3 Ergebnisse

Der identifizierte Datensatz besteht aus N1 = 23 gültigen Datensätzen für digitale Souveränität, N2 = 24 Datensätzen für digitale Transformation und N = 38 gültigen Datensätzen für Softwareeinführung. Abbildung 5.38 zeigt die Branchenzugehörigkeit der Umfrageteilnehmer und stellt eine ausgewogene Mischung aus dem privaten und öffentlichen Sektor dar. Die meisten der Teilnehmer der Umfrage arbeiten in der IT-Branche. Die zweitgrößte Branche ist der Dienstleistungssektor, gefolgt von der öffentlichen Verwaltung, dem Logistiksektor, der Automobilindustrie, der Telekommunikationsindustrie und der Luft- und Raumfahrtindustrie.

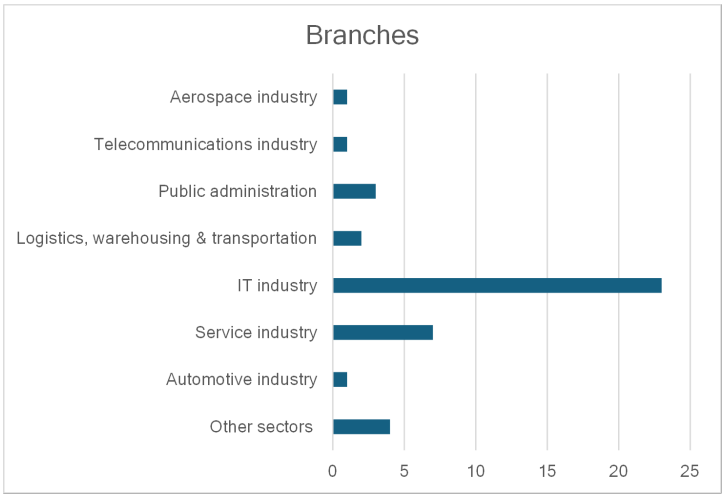


Abbildung 5.38: Branchenübersicht

5.3.3.1 Ergebnisse aus der Online-Umfrage: Zusammenhang zwischen Software-Einführung, digitaler Transformation und digitaler Souveränität in Unternehmen

SDSM-Aktivität 1: Stand der Softwareeinführung in Unternehmen Auf der Grundlage der Umfrage können Einblicke in die derzeitige Praxis der Softwareeinführung in Unternehmen gewonnen und eine Reihe von Problemen in dieser Phase identifiziert werden. Die Umfrageteilnehmer wurden aufgefordert, die Praxis der Softwareeinführung in ihrem Unternehmen zu bewerten. Wie in Abbildung 5.39 dargestellt, ist das Ergebnis, dass im öffentlichen Sektor die Anzahl der Organisationen, die eine systematische Einführung ($n = 11$) auf der Grundlage von Strategie und Anforderungen praktiziert, sogar etwas höher ist als im privaten Sektor ($n = 9$).

SDSM-Aktivität 2: Anforderungen an digitale Souveränität und digitale Transformation Die Daten zeigen Maßnahmen, die Unternehmen empfehlen zu ergreifen, um digitale Souveränität zu meistern (vgl. Abbildung 5.40). Drei besonders oft ausgewählte Maßnahmen sind: Backups, Verschlüsselung und Risikoanalysen. Interessanterweise werden entgegen vorangegangener Ergebnisse (vgl. Kapitel 5.1) regelmäßige Schulungen für digitale Souveränität als weniger wichtig angesehen. Dies kann auf die Tatsache zurückgeführt werden, dass die ersten Ergebnisse aus dieser Dissertationsschrift im Jahr 2022

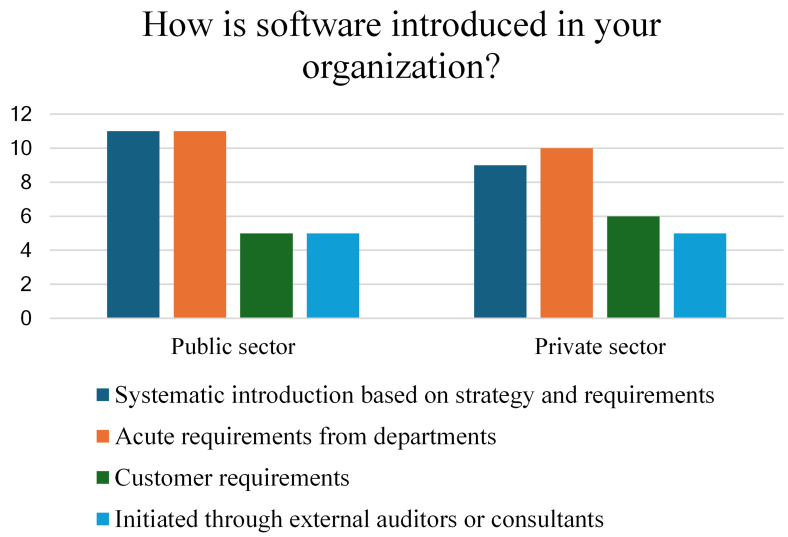


Abbildung 5.39: Softwareeinführung im öffentlichen und privaten Sektor

erhoben wurden, diese hier im Jahr 2024. Die genauen Gründe für die Diskrepanz sind nicht genauer aufschlüsselbar; es könnte aber eine Verschiebung der Prioritäten im Laufe der Zeit gegeben haben.

Abbildung 5.40 zeigt, dass im Hinblick auf die digitale Transformation insbesondere die Einführung eines Sicherheitsmanagementsystems empfohlen wird. Sicherheit ist nach Weyer (2018) einer der wichtigsten Schlüsselfaktoren im Hinblick auf eine erfolgreiche digitale Transformation. Deutlich wurde auch, dass Daten einerseits geschützt werden müssen, aber andererseits, den Befragten nach, auch nutzbar für Entwickler und Entscheider in Unternehmen sein müssen. Die Herausforderungen, die bei digitaler Souveränität erhoben worden sind, unterscheiden sich von denen digitaler Transformation. Das führt zur Interpretation, dass digitale Souveränität und digitale Transformation nicht das Gleiche sind. Dennoch kann argumentiert werden, dass digitale Souveränität im Kontext von Softwareeinführung ein Transformationsversuch innerhalb von Lieferketten in Unternehmen sein kann. Die Ergebnisse dieser Arbeit eröffnen neue Perspektiven, die in der bisherigen Forschungsliteratur zu digitaler Souveränität kaum berücksichtigt wurden. Pohle (2020) unterstreicht, dass sich durch digitale Transformation Herausforderungen für die digitale Souveränität ergeben können. Glasze et al. (2023) stellen die Entwicklungen

digitaler Souveränität seit den 2010ern, den Entwicklungen der digitalen Transformation seit den 1990ern entgegen. Damit scheinen die Konzepte aus seiner Perspektive für sich alleinstehend zu sein. In dieser Arbeit sehen wir jedoch die Notwendigkeit, dass Unternehmen sich im Zuge der Anforderungen digitaler Souveränität digital transformieren müssen. Dieses Verständnis wird weiter unten noch einmal im Rahmen des Clusterings genauer aufgegriffen.

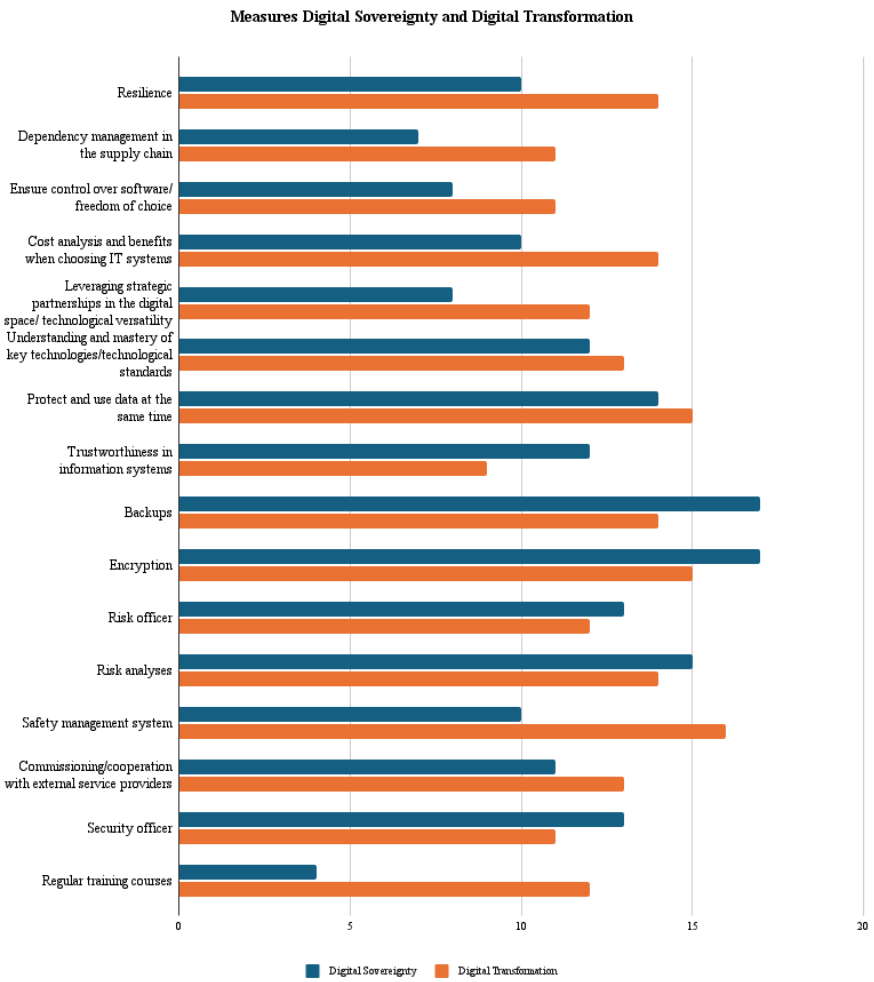


Abbildung 5.40: Maßnahmen, um digitale Transformation und digitale Souveränität zu meistern

Laut den Umfrageteilnehmern sind die drei größten Herausforderungen im

Rahmen der digitalen Transformation: hohe Komplexität bei der Umstellung bestehender Systeme und Prozesse, Technologieakzeptanz bei den Mitarbeitern und hohe Kosten (vgl. Abbildung 5.41). Im Vergleich dazu sind die drei am wenigsten bewerteten Herausforderungen in Bezug auf die digitale Transformation: Kontrolle über Daten, Regulierung und Transparenz. Im direkten Vergleich bewerteten die Teilnehmer der Umfrage die größten Herausforderungen für die digitale Souveränität: mangelnde Wahlfreiheit bei der Auswahl von IT-Produkten, personelle Ressourcen und Abhängigkeit von externen Lösungen. Die drei am schlechtesten bewerteten Herausforderungen für die digitale Souveränität sind: viele Risiken, fehlende digitale Fähigkeiten und hohe Kosten.

Im direkten Vergleich zeigen die Ergebnisse, dass sich die Herausforderungen für die digitale Transformation und die digitale Souveränität deutlich unterscheiden. Es ist auch zu sehen, dass viele Herausforderungen in Bezug auf die digitale Transformation stark bewertet wurden, aber im Vergleich zur digitalen Souveränität eher schwach. Ein Beispiel hierfür sind die hohen Kosten, die bei der digitalen Transformation zu den drei größten Herausforderungen gehören, bei der digitalen Souveränität jedoch schlecht bewertet wurden.

Um herauszufinden, welche realen Probleme deutschsprachige Unternehmen in den Bereichen digitale Souveränität und digitale Transformation haben, wurden die Teilnehmer der Umfrage gebeten, die drei größten Herausforderungen zu priorisieren. Die größten Herausforderungen in Bezug auf die digitale Souveränität, die von den Umfrageteilnehmern genannt wurden, sind: Kosten, Komplexität und zu wenig Entscheidungsfreiheit. Es wird auch erwähnt, dass die Unternehmen mit unzureichenden digitalen Fähigkeiten zu kämpfen haben. Zu viele Abhängigkeiten und zu wenig Technologieakzeptanz sind weitere Herausforderungen. Top-Herausforderungen der digitalen Transformation sind in absteigender Reihenfolge zu wenig Personal, keine Strategie und zu wenig Transparenz in den Unternehmen. Darüber hinaus sehen die Umfrageteilnehmer zu wenig Schulungen, fehlende Entscheidungskonzepte und keine Vorschriften als weitere Herausforderungen im Umgang mit dem Thema digitale Transformation.

SDSM-Aktivität 3 und 4: Abstraktion der Anforderungen zu digitaler Transformation und digitaler Souveränität und Evaluation Im

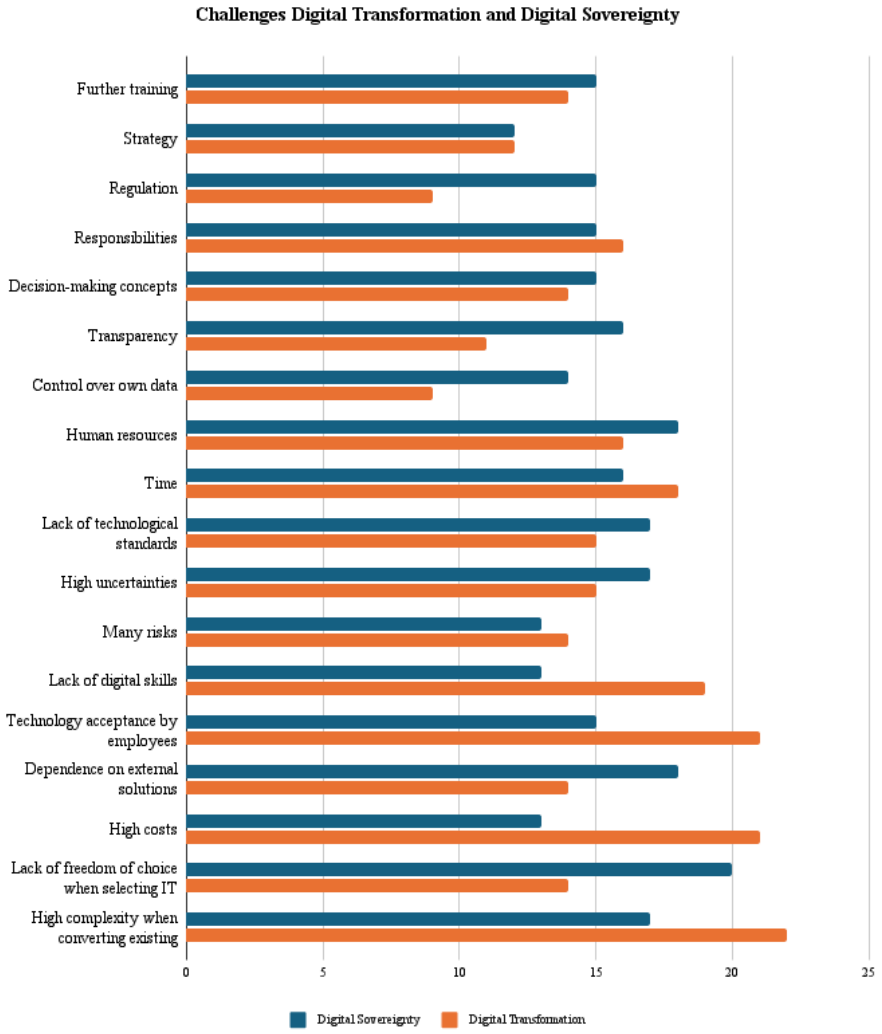


Abbildung 5.41: Herausforderungen, digitale Transformation und digitale Souveränität zu meistern

Rahmen der SDSM-Aktivität 3 ist eine Ableitung von Anforderungen möglich, die für eine Lösung der oben genannten realen Probleme in den beiden Bereichen digitale Souveränität und digitale Transformation gelten. Um diese Anforderungen zu erhalten, wird ein erstes Clustering nach den genannten Herausforderungen und Maßnahmen vorgenommen. Während der Analyse sind die Beziehungen zwischen den Clustern isoliert betrachtet worden. In

dem oben erwähnten Workshop mit den Autoren wurden die Maßnahmen und Herausforderungen für digitale Souveränität und digitale Transformation aus der Online-Umfrage geclustert und anschließend ausgewertet. Dazu wurden sie zunächst nach der Anzahl der Nennungen als Top-Antwort sortiert. Jede Antwortmöglichkeit entspricht einem Cluster. Die von den Umfrageteilnehmern als am wichtigsten eingestuften Antworten stehen an erster Stelle, die als am wenigsten wichtig eingestuften an letzter Stelle. Die Einflussfaktoren werden dann aus der Sortierung herausgenommen und einzeln aufgelistet. Daraus ergibt sich für die digitale Transformation folgende Reihenfolge: (1) personelle Ressourcen, (2) Strategie, (3) Transparenz, (4) Weiterbildung, (5) Regulierung. Die personellen Ressourcen werden als Einflussfaktor ausgewiesen. Für die digitale Souveränität ist die Reihenfolge wie folgt: (1) Kosten, (2) Komplexität, (3) Wahlfreiheit/ digitale Kompetenzen, (4) Abhängigkeit, (5) Technologieakzeptanz. Kosten und Komplexität werden als Einflussfaktoren extrahiert.

Diese Art von Analyse ergibt zwei Cluster für die digitale Transformation (vgl. Abbildung 5.42): strategische Ausrichtung und IT-Fähigkeiten.

Im Rahmen der Evaluation kristallisierte sich als Einflussfaktor *interne und externe Personalressourcen* heraus. Dem Cluster *strategische Ausrichtung* werden die folgenden Faktoren zugeordnet: Strategie, Vorschriften, Transparenz und Entscheidungsfindung. Die Analyse der Beziehung zwischen dem Cluster *strategische Ausrichtung* und seinen Faktoren in Bezug auf den Unabhängigkeitsfaktor *interne und externe personelle Ressourcen* hat gezeigt, dass eine unternehmerische Vision in Bezug auf Strategie, Vorschriften, Transparenz und Entscheidungskonzepte realistisch entwickelt werden muss, um die erforderlichen personellen Ressourcen entsprechend einsetzen zu können. Im konkreten Fall der Entwicklung von Softwaresystemen müssen Unternehmen die Geschäftsvision kontinuierlich mit der IT-Vision abgleichen, um die notwendigen personellen Ressourcen rekrutieren oder adäquat ausbilden zu können. Ansonsten muss klar sein: desto mehr Maßnahmen entwickelt und umgesetzt werden, desto mehr Zeit und Personal mit entsprechendem Fachwissen werden benötigt. Es besteht die Gefahr, dass die gesetzten Fristen nicht eingehalten werden können. Die Korrelation zwischen dem Cluster *IT-Kenntnisse* und dem Faktor *Weiterbildung* in Bezug auf den Unabhängigkeitsfaktor *Interne*

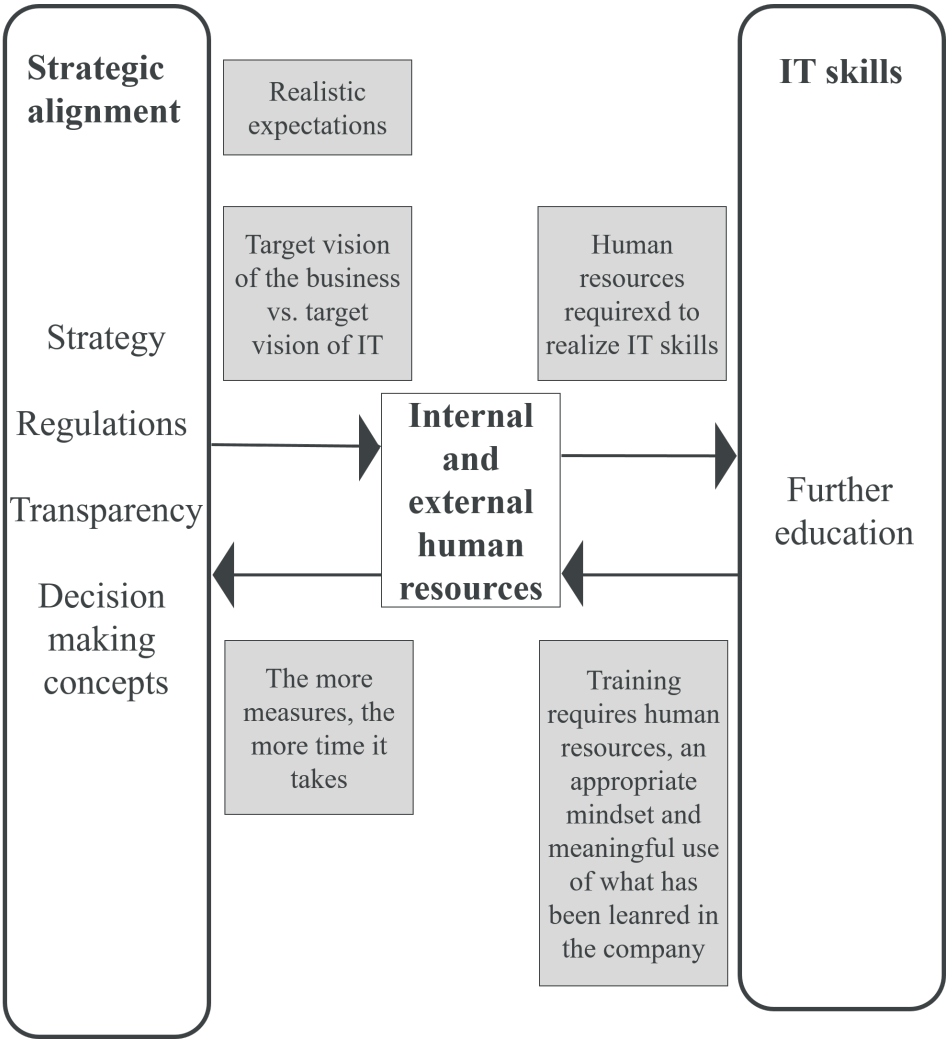


Abbildung 5.42: Darstellung des Zusammenhangs zwischen den Clustern digitaler Transformation

und externe Personalressourcen deckt die personelle Lücke auf, die notwendig ist, um die erforderlichen IT-Kenntnisse zu erfüllen. In diesem Zusammenhang zeigen die Ergebnisse auch, dass Mitarbeiter und Partner für den Erwerb der geforderten IT-Kenntnisse an Schulungen teilnehmen müssen und eine entsprechende Einstellung benötigen, um Zeit und Mühe in das Erlernen neuen Wissens zu investieren. Die Unternehmen müssen sich überlegen, welcher Ansatz ihnen einen größeren Mehrwert verspricht. Mehr Fachwissen mit wenigen eigenen Mitarbeitern aufzubauen oder externes Personal einzustellen

und nur vorübergehend über das Fachwissen zu verfügen.

Für digitale Souveränität wurden zwei Cluster identifiziert (vgl. Abbildung 5.43): erstens *Unabhängigkeit* und zweitens *IT-Kompetenzen*. *Abhängigkeit* und *Wahlfreiheit* wurden dem ersten Cluster zugeordnet, während *Technologieakzeptanz* und *digitale Kompetenzen* im zweiten Cluster zu finden sind. Die Faktoren *Kosten* und *Komplexität* werden als Unabhängigkeitsfaktoren aufgeführt.

Die bidirektionale Beziehung zwischen Unabhängigkeit und Kosten leitet sich aus der Annahme ab, dass eine Erhöhung des Kosten-Nutzen-Verhältnisses für eine zunehmende Unabhängigkeit erforderlich ist. Es sollte das Ziel der Unternehmen sein, dies zu quantifizieren. Bei der Betrachtung des Verhältnisses zwischen Kosten und Unabhängigkeit besteht die Gefahr, dass zu utopische Erwartungen geweckt werden. Wenn Unternehmen versuchen die Unabhängigkeit zu maximieren, würde das signifikant steigende Kosten verursachen (Cook et al., 2020). Aus dieser Herausforderung leitet sich der Komplexitätsfaktor ab. Es ist festzustellen, dass man, wenn man die Wahl zwischen IT-Produkten unterschiedlicher Komplexität hat, eher das Produkt mit der geringsten Komplexität wählen würde. Außerdem wird die IT-Landschaft im Unternehmen komplexer, wenn mehr technologische oder strategische Unabhängigkeit erforderlich ist. Daraus lässt sich schließen, dass Komplexität und Kosten überschaubar bleiben müssen, um die digitale Souveränität zu erhöhen. Für Unternehmen ist es ratsam, Kosten und Komplexität voneinander zu entkoppeln.

Fertigkeiten und Technologieakzeptanz können z.B. durch Schulungen verbessert werden. Das Ziel in Bezug auf die IT-Fähigkeiten sollte sein, auf dem neuesten Stand zu bleiben und zu diversifizieren. Dennoch wäre das Kosten-Nutzen-Verhältnis auch für den Erwerb von IT-Kenntnissen hilfreich, da die Produktivität mit zunehmender Schulung abnimmt (Colombo & Stanca, 2014; Klare & Lechner, 2024b). Moderne, komplexe Arbeitsumgebungen erfordern IT-Fähigkeiten, einschließlich Spezialwissen. Gleichzeitig kann die Einführung neuer Fähigkeiten zu einer vorübergehenden Überlastung führen.

SDSM-Aktivität 5: Vergleich der Anforderungen an das Lösungsdesign, um souveränere Softwareeinführung zu unterstützen Für die digitale Transformation werden die folgenden allgemeinen Anforderungen aus

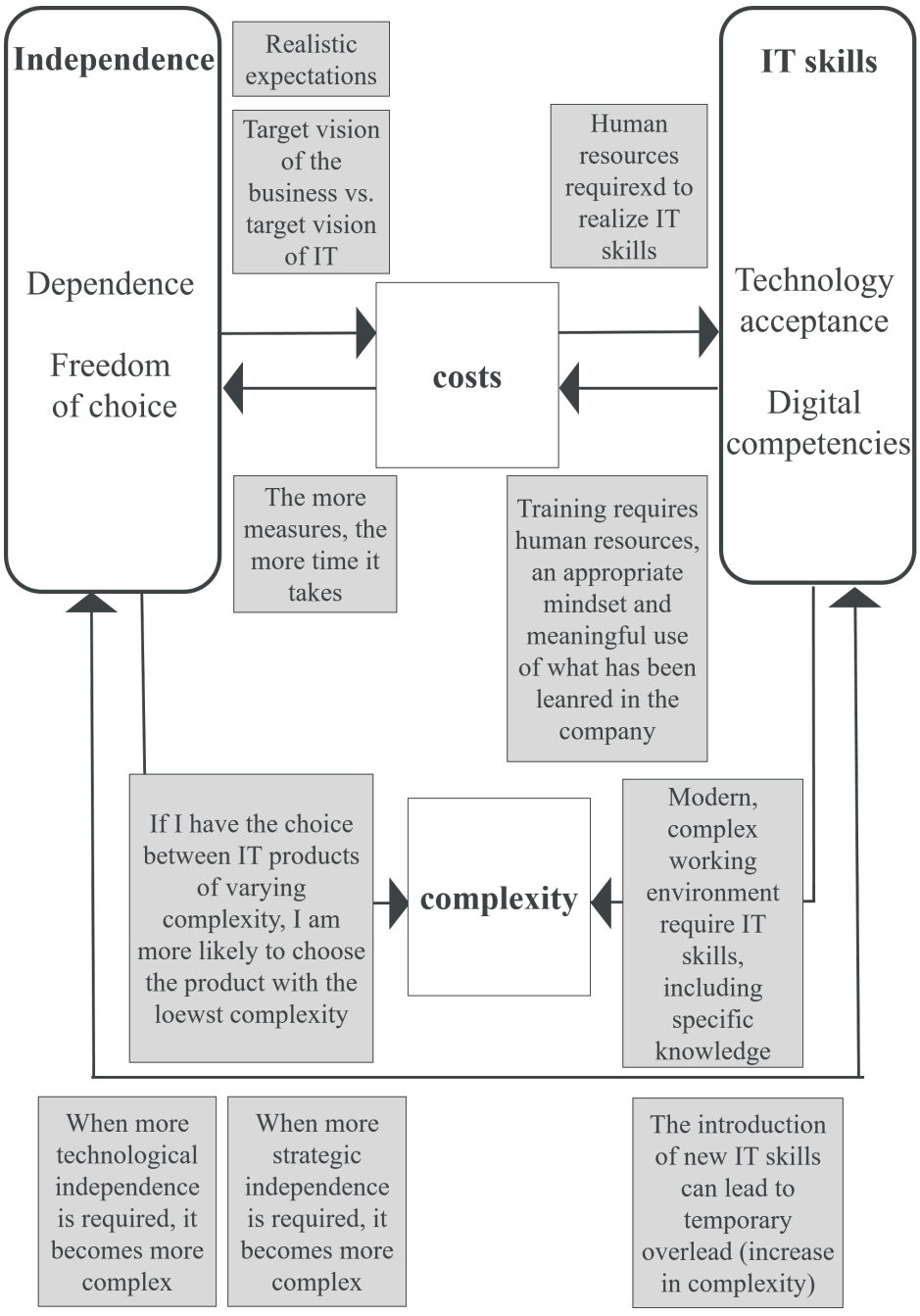


Abbildung 5.43: Darstellung des Zusammenhangs zwischen den Clustern digitaler Souveränität

den Analyseergebnissen abgeleitet:

- Es muss eine realistische unternehmerische Vision in Bezug auf Vor-

schriften und Transparenz entwickelt werden. Diese Vision muss durch die Entwicklung und Verbesserung expliziter Strategien und durch Entscheidungskonzepte untermauert werden.

- Es muss sichergestellt werden, dass ausreichend qualifizierte interne und externe personelle Ressourcen in ausreichender Zahl zur Verfügung stehen, da dieser Faktor in der durchgeführten Umfrage nicht nur als höchste Priorität, sondern auch als größte Herausforderung angesehen wurde.

Für die digitale Souveränität werden folgende allgemeine Anforderungen abgeleitet:

- Um die Unabhängigkeit von Unternehmen zu erhöhen, muss ein gutes Kosten-Nutzen-Verhältnis hergestellt werden. Darüber hinaus müssen die Unternehmen in der Lage sein, den tatsächlichen Gradienten dieses Verhältnisses zu quantifizieren, um eine rationale Entscheidungsfindung zu unterstützen.

- Kosten und Komplexität müssen so weit wie möglich voneinander entkoppelt werden, damit Unternehmen in der Lage sind, ihre Unabhängigkeit in Wettbewerbsszenarien zu maximieren.

- Der aktive Erwerb von IT-Fähigkeiten muss im unternehmerischen Kontext kostengünstig gefördert werden - sowohl im Tagesgeschäft als auch in der Projektarbeit.

- Der Erwerb von IT-Kenntnissen muss besser gesteuert werden, um vorübergehende Überlastungen zu vermeiden und das Risiko von Verzögerungen zu verringern.

Mit Hilfe des Clustering- und Ordnungsworkshops konnte außerdem sichergestellt werden, dass jede allgemeine Anforderung entweder im Abschnitt Maßnahmen oder Herausforderungen der Umfrageergebnisse gemäß SDSM-Forschungsaktivität 5 vertreten ist.

Als nächstes ist es das Ziel, allgemeine Komponenten für eine Lösung zu finden. In einem zweiten Workshop wenden die Autoren die Clustering-

Technik erneut auf alle Maßnahmen an, die sich aus der Umfrage ergaben. Als Ergebnis resultieren Handlungsempfehlungsblöcke.

SDSM-Aktivität 6: Lösungskomponenten auf Basis von Handlungsblöcken Jede Empfehlung ist in einer oder mehreren Maßnahmen aus den vorherigen Ergebnissen verankert.

IT-Kenntnisse Unternehmen sollten den Schulungsbedarf für den Einsatz und die sinnvolle Nutzung von Software erkennen. Um die Anforderungen der digitalen Transformation und der digitalen Souveränität bei der Einführung von Software zu meistern, können technologische Standards Unternehmen helfen, effizient und effektiv zu arbeiten. Dies bestätigt die Sinnhaftigkeit des Faktors Standardisierung im DISO-A-Modell. Um die Akzeptanz bei den Mitarbeitern zu erhöhen, muss Vertrauen in Informationssysteme geschaffen werden. Zu beachten ist aber auch, dass die Teilnahme der Mitarbeiter an Schulungen sinnvoll umgesetzt werden muss.

Strategische Ausrichtung Strategische Entscheidungen auf der Grundlage von Kosten-Nutzen-Analysen sind wichtig, um die Anforderungen an die digitale Souveränität und die digitale Transformation zu erfüllen. Die hier gewonnen Ergebnisse untermauern die Bedeutung des Kosten-Nutzen-Verhältnisses im Kontext digitaler Souveränität, die im Rahmen der Interviews zur Erstellung des DISO-A-Modells noch divergent diskutiert wurden. Unternehmen sollten strategische Partner für Software auf der Grundlage ihrer Anforderungen und der vorgenannten Analyse auswählen. Um erfolgreich digitale Souveränität zu adressieren, sollten Unternehmen die Sicherheit, Zuverlässigkeit und Widerstandsfähigkeit ihrer Lieferketten, aber auch gebauten IT-Systeme berücksichtigen. Im Hinblick auf digitale Transformation sind Nachhaltigkeit und Vertrauen wichtig.

Unabhängigkeit Die Zusammenarbeit mit externen Dienstleistern muss besser gesteuert werden, um als Unternehmen zukunftsfähig zu sein. Diese Notwendigkeit eines besseren Managements von Dienstleistern ging auch aus der letzten Studie hervor (vgl. Kapitel 5.2). Dabei müssen die Unternehmensziele im Fokus bleiben und das Vertrauen in die Kooperationen sowie in die Technologie muss gegeben sein. Die Ergebnisse der Umfrage unterstreichen, dass Kontrolle über die Softwarelieferketten und Wahlfreiheit bei der

Softwareauswahl notwendig sind. Diese Art der Kontrolle kann durch die Förderung von Open Source und die Einbeziehung in den Entwicklungs- und Überprüfungsprozess unterstützt werden. Den Daten nach ist es notwendig, die Abhängigkeit in den Lieferketten zu verringern.

Resilienz Basierend auf den Umfrageergebnisse ist es für Unternehmen empfehlenswert in Anlehnung an das BSI, technische Risiken frühzeitig zu erkennen und zu reduzieren. Damit lassen sich die Ergebnisse hier mit den Themen Resilienz und IT-Sicherheit (insbesondere Sicherheitsrisiken und -lücken) aus dem DISO-A-Modell koppeln. Die Ergebnisse gehen Hand in Hand mit denen aus dem vorherigen Kapitel (vgl. Kapitel 5.2): hier werden konkrete BSI-Warnungen vorgestellt, die im Kontext der OS-Arbeit Risiken für eine Stärkung digitaler Souveränität mit sich bringen. Um eine höhere Resilienz zu erreichen, ist ein Basisschutz notwendig. Konkret können Backups und Verschlüsselung helfen. Unternehmen sollten sich mit unternehmensspezifischen Risiken auseinandersetzen und Risikoanalysen durchführen. Insbesondere im Kontext von souveräneren Lieferketten ist es wichtig, zu wissen, was das übergreifende Ziel ist, das erreicht werden soll. Um digitale Souveränität und digitale Transformation erfolgreich umzusetzen, empfiehlt es sich, personelle und technische Ressourcen zu nutzen. Sinnvolle Maßnahmen sind aus Sicht der Umfrageteilnehmer die Einführung eines Sicherheitsbeauftragten, eines Risikobeauftragten und der Einsatz von Sicherheitsmanagementsystemen. Abschließend ist wichtig darauf hinzuweisen, wie bedeutsam es ist, das Geschäftspotenzial von Daten zu nutzen, indem die Strategie und die Geschäftsebene synchronisiert werden. Es muss ein Gleichgewicht zwischen dem Schutz und der gleichzeitigen Nutzung von Daten gefunden werden.

SDSM-Aktivität 7: Die ISO/IEC/IEEE 12207:2017 Erweiterung

Nun reiht sich mit der SDSM-Aktivität 7 der Versuch an, die Lösung in bestehende Enterprise Architecture (EA)-Frameworks wie z.B. TOGAF zu integrieren oder sie in einen übergreifenden architektur- und geschäftsorientierten Kontext einzubinden. Im Ergebnis wurde die letzte Option bevorzugt, da Überlegungen zur Beschaffungs- und Geschäftsstrategie integriert wurden. Bei der Untersuchung möglicher Rahmenwerke wurde die ISO/IEC/IEEE-Norm 12207:2017 ausgewählt, da sie sowohl technische, architektonische als auch

geschäftliche Belange berücksichtigt und den Praktiken der Industrie als Best Practice Standard sehr nahe kommt. Diese wurde somit als Grundlage für die Integration der Empfehlungsblöcke verwendet. Tabelle 5.9 stellt die Prozessgruppen und Prozesse aus der ISO/IEC/IEEE-Norm 12207:2017 dar und zeigt die Zuordnung der Handlungsblöcke zu den jeweiligen Prozessen (Stelter et al., 2025). Die Erklärung wurde auf der rechten Seite als Erweiterung der Norm hinzugefügt.

SDSM-Aktivität 8: Evaluation der Prozessgruppen auf Basis praxisnaher Literatur

Im Rahmen der Evaluation finden sich konkrete Hinweise in der Literatur, wo die Prozessgruppen aus der ISO-Erweiterung Anknüpfung finden können.

Aus der ISO-Norm geht zunächst hervor, dass digitale Unabhängigkeit ein wesentlicher Teil der Prozessgruppe *Agreement* ist (vgl. Abschnitt 5.3.3.1). Brüesch et al. (2022) stellt in seinem Artikel dar, wie mit Hilfe von auf digitale Souveränität ausgerichtete Cloud-Beschaffung mehr Informationssicherheit und so eine stärkere Form digitaler Unabhängigkeit erreicht werden kann. Brüesch et al. (2022) gehen damit in ihren Ausführungen besonders auf den ISO-Prozess *Supply* ein, der eine stärkere Form der Unabhängigkeit durch die Entwicklung einer Lieferkettenstrategie vorsieht.

Einer Bitkom-Studie aus dem Jahr 2019 nach, ist es wichtig, Marktverzerrungen in der Lieferkette zu reduzieren. Wie bereits bei Brüesch et al. (2022) beschrieben, scheint es empfehlenswert, diese Anstrengung im Rahmen einer neuen Lieferkettenmanagement-Strategie anzugehen (vgl. Prozess *Supply* und Prozessgruppe *Agreement* aus Abschnitt 5.3.3.1). Aber auch die Prozessgruppe *Technical* kann wegen den Schlüsseltechnologien, die als Empfehlung geliefert werden, genannt werden (siehe Prozess *Business or Mission Analysis* unter Abschnitt 5.3.3.1).

Ebenfalls der Prozessgruppe *Agreement* zuzuordnen, sind die Ausführungen von Wirnsperger et al. (2021). Sie schneiden aufgrund ihrer umsetzungsorientierten Natur auch die Prozessgruppe *Organizational Project-Enabling* an. Wirnsperger et al. (2021) schlägt konkret die Schaffung einer Datenökonomie in Unternehmen bei gleichzeitiger Berücksichtigung von Robustheit, IT-Sicherheit und KI-Entwicklungen vor. Diese Datenökonomie sollte unter

Process Group	Process	Explanation
Agreement	Acquisition	Considering the four recommendation blocks when preparing requests for supply and agreements raises awareness and established clear links to strategic objectives. Explicit expectations for suppliers e.g. recommendation block ”independence”.
	Supply	Independence and Resilience considerations should be applied in the creation of a supply strategy. This is an explicit acceptance criteria.
Organizational project-enabling	Life Cycle Model Management	Policies can be defined here e.g. Human Resource Management and requirements for training and specific skills for necessary software or how to embed.
	Human Resource Management	Requirements for training and the buildup/acquisition of specific skills for necessary software can be considered in all activities of the process.
	Portfolio Management	Requirements from recommendation blocks ”strategic alignment”, ”independence” and ”resilience” can be integrated in the defined and authorized projects activity.
	Quality Management	Risk management considerations can serve as input to evaluate and perform corrective and preventive action activities.
	Knowledge Management	The recommendation blocks ”IT skills” and ”resilience” (technical risk reduction) are mainly relevant.
Technical Management	Project Planning	Input from all recommendation blocks to the project definition activity - specifically objectives and constraints and planning the acquisition of materials and enabling systems.
	Risk Management	Input from the recommendation block ”resilience” mainly relevant in defining and monitoring risk.
	Quality Assurance	Recommendation blocks provide input for the task of evaluating products and services conformance to defined project and organization-specific criteria.
Technical	Business or Mission Analysis	Concerns from the recommendation block ”independence” and specifically regarding Digital Sovereignty can enhance the evaluation of alternative solution classes task.
	Stakeholder Needs and Requirements Definition	Recommendation blocks can serve as sources for defining non-functional requirements at organization or project levels.
	Architecture Definition	Specifically the recommendation blocks ”independence” and ”resilience” can be used to develop alternative architectures with focus on e.g. easily replaceable or open source components.

Tabelle 5.9: Zuordnung der ermittelten Handlungsempfehlungen zu bestimmten Prozessgruppen und Prozessen (Stelter et al., 2025)

anderem auf die Lieferkette von Unternehmen und deren Dienstleister ausgerichtet sein. Die Überlegungen von Wirnsperger et al. (2021) gehen aber noch weiter darüber hinaus. Der Handlungsempfehlungsblock *Resilienz* findet sich in der Prozessgruppe *Portfolio Management* wieder und sieht die Anpassung des Portfolios sowie das Überdenken des Managements dieses Portfolios vor (vgl. Abschnitt 5.3.3.1).

Glohr et al. (2022) schneidet in seiner Publikation gleich drei der Prozessgruppen aus der ISO-Erweiterung an: *Agreement*, *Organizational Project-Enabling* und *Technical Management*. Sie machen deutlich, dass ein Agreement für digitale Souveränität, Schulungen für Personal (unternehmerische Projektbefähigung) und Projektmanagement (technisches Management) notwendig ist. Insgesamt sprechen sie von einer Ende-zu-Ende-Digitalisierung, die notwendig wäre, um digitale Souveränität zu stärken. Die ISO-Erweiterung ist nicht auf eine Ende-zu-Ende-Digitalisierung ausgerichtet, da sie sich eher auf die Lieferkette, die Beschaffung und den Softwarelebenszyklus von Unternehmen konzentriert. Damit lässt sich an dieser Stelle ein weiteres Mal feststellen, dass teilweise die Überlegungen der Autoren über die vorgeschlagenen Prozessgruppen hinausgehen. Auffällig ist zudem, dass bei Glohr et al. (2022) die Prozessgruppe *Technical* nicht in den Ausführungen wiederzufinden ist.

Technical als Prozessgruppe findet sich jedoch in der Studie von McKinsey aus dem Jahr 2022 wieder, und so auch *Organizational project-enabling* (Smit et al., 2022). *Technical* wegen des Fokus auf digitale Infrastrukturen unter der Linse von Beschaffung. In dem Prozess *Business or Mission Analysis* ist verankert, dass Unabhängigkeit in Bezug auf digitale Souveränität vor dem Hintergrund alternativer Lösungen zu beleuchten ist. *Organizational project-enabling* wurde gewählt, weil der Studie nach Unternehmen durch Forschung und Politik befähigt werden müssen, was widerrum in der ISO-Erweiterung mit einer strategischen Ausrichtung, mehr Resilienz und Abhängigkeit einhergeht (vgl. Abschnitt 5.3.3.1).

Die unabhängige Datenschutzaufsichtsbehörde von Bund und Ländern (2020) greift genau so, wie die McKinsey-Studie, die Prozessgruppen *Agreement* und *Organizational Project-Enabling* auf. Agreement, weil mehr Unabhängigkeit in der Lieferkette gefordert wird, wie in der Empfehlung unter dem

Prozess Acquistion. Organizational project-enabling, weil hier Richtlinien beim Prozess Life Cycle Model Management eine bedeutende Rolle spielen, wie auch im Artikel (DSB, 2020).

Madiega (2020) nennt konkrete Beispiele, wie man Innovation unter Vorbehalt digitaler Souveränität stiften kann. Diese Publikation ist der Prozessgruppe *Technical* zuzuordnen, weil eine Abwägung von Risken wesentlich in den Beispielen Cybersicherheit, ethische KI, Datenschutz, europäische Werte und Regulierungsinstrumente diskutiert wird. Diese Risikoabwägungsperspektive ist vor dem Hintergrund von Lieferkettenmanagement in den Prozessen *Risk Management* und *Quality Management* ebenfalls als Perspektive in die ISO-Erweiterung eingeflossen (vgl. Abschnitt 5.3.3.1).

Zuletzt teilen Seifried und Bertschek (2021) konkrete Maßnahmen zur Meisterung digitaler Souveränität, darunter der Aufbau von Digitalkompetenzen, die Stärkung von Technologiesouveräniät, die Risikoabwägung, Datensouveränität und Agilität. Diese Maßnahmen schneiden folgende Prozesse an: die Risikoanalyse, *Quality Management* als Teilbereich der Prozessgruppe *Organizational Project Enabling* und digitale Kompetenzen, *Human Resource Management*, ebenfalls als Teilbereich von *Organizational Project Enabling*. Technologie-, Datensouveränität und Agilität ist der Prozessgruppe *Technical* zuzuordnen. Zu unterstreichen ist, dass diese Prozessgruppen in der Publikation aber nur in Teilen angeschnitten wurden. Die Ausführung in Seifried und Bertschek (2021) gehen wie auch schon bei zwei zuvor genannten Publikationen über die ISO-Norm hinaus.

Insgesamt stellt man fest, dass sich alle Prozessgruppen in der Literatur wiederspiegeln, wobei ein starker Fokus auf die Prozessgruppen *Agreement*, *Organzational Project-Enablement* und *Technical* feststellbar ist. Das Thema *Technical Management* wird in den Publikationen eher untergraben.

5.3.4 Zusammenfassung, Limitationen und Ausblick

Dieser Beitrag zeigt, dass viele der an der Umfrage teilgenommenen Unternehmen sich nicht im Klaren darüber sind, wie souveränere Softwareeinführung gelingen kann. Insbesondere im Wandel und unter Berücksichtigung von digitalen Transformations-, und digitalen Souveränitätsanforderungen, ist es

für Unternehmen fraglich, wie sie dies umsetzen können. Eine Möglichkeit, Unternehmen Leitlinien zu geben, wie sie souveränere Softwareeinführung meistern können, ist die in dieser Studie neu entwickelte ISO/IEC/IEEE 12207:2017 Erweiterung.

Die ISO-Erweiterung enthält die Prozesse: 1) Agreement, 2) Organizational Project Enabling, 3) Technical Managemenet und 4) Technical und umfasst Erklärungen, wie die erhobenen Handlungsblöcke aus der Umfrage umgesetzt werden könnten.

Die Herausforderungen bei der Stärkung der digitalen Souveränität in Unternehmen liegen laut der Online-Umfrage insbesondere in der mangelnden Wahlfreiheit bei der Auswahl von IT-Produkten und der Abhängigkeit von externen Lösungen. Es wird auch deutlich, dass die Einführung von digitaler Souveränität komplex und kostenintensiv ist. Für die Interviewpartner bedeutet digitale Souveränität im Kontext von Softwareeinführung innerhalb des Unternehmens vor allem eine stärkere Form der Unabhängigkeit, die mit dem Bedarf an IT-Kompetenz einhergeht. Das ist ein eingeschränkteres Verständnis, als das, was in dieser Arbeit von digitaler Souveränität im Kontext von Softwareeinführung angenommen wird. Bei dem Verständnis von Souveränität in dieser Arbeit geht auch um Erhaltung von Handlungsoptionen, die ich nur entstehen, wenn man auf Augenhöhe mit anderen interagieren kann. Als Unternehmen begibt man sich teils bewusst in Abhängigkeiten zu Kunden und Lieferanten, um ökonomisch handeln zu können. Schließlich führen die vorangegangenen Ergebnisse zur Empfehlung für Unternehmen, Abhängigkeiten auf drei verschiedenen Ebenen zu prüfen: (1) in Lieferketten, (2) bei der Auswahl von Software und (3) bei der Zusammenarbeit, z.B. mit Software-Anbietern.

Um die digitale Transformation gut zu meistern, sind nach Ansicht der Interviewpartner interne und externe Personalressourcen, ein strategischer Fokus und IT-Kompetenzen erforderlich. Als Top-Herausforderungen für die Bewältigung der digitalen Transformation in Unternehmen werden hohe Komplexität bei der Umstellung bestehender Systeme und Prozesse, hohe Kosten und Technologieakzeptanz bei den Mitarbeitern genannt. Unternehmen sollten den Schulungsbedarf erkennen, technologische Standards implementieren und Kosten-Nutzen-Analysen für strategische Entscheidungen nutzen.

Zwar geht der Umfrage nach digitale Souveränität mit anderen Herausforderungen einher, als digitale Transformation, dennoch konnte aufgezeigt werden, dass man im Kontext von Softwareeinführung digitale Souveränität als Transformationsvorhaben verstehen kann. Diese Auffassung bestätigt die ursprüngliche Vermutung, dass digitale Souveränität je nach Perspektive neu definiert werden sollte.

Für diesen Beitrag wurden Teamleiter, Abteilungsleiter und Mitarbeiter der C-Ebene gebeten, an einer Online-Umfrage teilzunehmen. Die Wahl der Zielgruppe ist eine Einschränkung, ebenso wie die relativ geringe Anzahl von Teilnehmern an der Umfrage. Zukünftige Forscher sollten mehr Daten sammeln. Eine weitere Limitation ist, dass die Integration der Empfehlungen auf ISO/IEC/IEEE 12207:2017 basiert. Die Wahl eines anderen Standards oder Rahmenwerks (z.B. TOGAF) führt zu anderen Ergebnissen. Forscher könnten sich auch der Überführung der Ergebnisse in Rahmenwerke wie TOGAF annehmen.

Der nächste Forschungsschritt sieht die Analyse von Konzepten vor, die bereits versprechen, dass sie eine Stärkung digitaler Souveränität gewährleisten: souveräne Clouds. Ziel ist es, besser zu verstehen, ob verschiedene souveräne Cloud-Konzepte tatsächlich zu einer Stärkung oder einem besseren Management von digitaler Souveränität beitragen können. Insbesondere das Thema Management scheint dieser Studie nach eine Facette zu sein, die es im Kontext digitaler Souveränität genauer zu beleuchten gilt.

5.4 Werkzeug IT-Infrastruktur: Interviewstudie zu souveränen Clouds im Kontext digitaler Souveränität

Die vierte Interviewstudie ist in einer Erstversion hier erschienen: *Klare,M., Lechner, U., and Fritzsche, A. (2025). Digital Sovereignty through Sovereign Clouds? International Conference on AI and the Digital Economy. -> **to appear***

5.4.1 Einleitung

Souveräne Clouds erfreuen sich zunehmender Beliebtheit im öffentlichen Diskurs (Holfelder et al., 2022; Rath et al., 2023; Urban, 2024). Dabei versprechen sie, digitale Souveränität stärken zu können (Adler-Nissen & Eggeling, 2024). Aber können diese Konzepte dieses Versprechen tatsächlich halten? Können souveräne Clouds wirklich zu mehr digitaler Souveränität führen? Oder vermarkten Anbieter von Cloud-Lösungen damit lediglich eine monetär lukrative Idee? In diesem Kapitel sind konkret folgende Forschungsfragen zu beantworten:

- Können souveräne Clouds dazu beitragen, mehr digitale Souveränität zu erreichen?
- Wie müssten souveräne Cloud-Konzepte angepasst werden, damit digitale Souveränität gestärkt wird?

Die Forschungsfragen sollen auf Basis der Ergebnisse aus einer Interviewstudie mit N=20 Cloud-Experten und der Analyse von IT-Architekturen verschiedener Cloud-Konzepte beantwortet werden. Konkret sind das die Cloud-Lösungen von T-Systems, Amazon, Microsoft, Oracle und IBM sowie eine Perspektivenerweiterung durch die Analyse von GAIA-X als Cloud-Ökosystem sowie einer Private Cloud aus dem militärischen Bereich in Deutschland.

Mit den Ergebnissen aus der Interview-Studie wird ein Beitrag zu einem Aspekt der Debatte geleistet. Das Ziel ist es, das Bewusstsein hinsichtlich digitaler Souveränität und die Einstellung gegenüber souveränen Clouds zu veranschaulichen. Drei Perspektiven werden gegenübergestellt, um neue Erkenntnisse abzuleiten: Management-, Architektur- und die User-Perspektive.

Dieser Beitrag ist wie folgt aufgebaut: In Kapitel 5.4.2 findet sich die Vorstellung des Forschungsdesigns. Im darauffolgenden Unterkapitel zeigen sich die Analyseergebnisse aus den Experteninterviews (siehe Kapitel 5.4.3). In Kapitel 5.4.4 sind die abgeleiteten Implikationen für Management, Architektur und Nutzer zu finden, was zur Eröffnung einer Diskussion in Kapitel 5.4.5 über Anpassungsmöglichkeiten souveräner Clouds führt. Das Kapitel schließt mit einer Abstraktion der Ergebnisse für das im nächsten Kapitel zu designende Referenzmodell, einer Zusammenfassung, einem Überblick über die bestehenden Limitationen und einem Ausblick (siehe Kapitel 5.4.6 und 5.4.7).

5.4.2 Forschungsdesign

Das Forschungsdesign besteht aus vier Forschungsschritten (vgl. Abbildung 5.44).

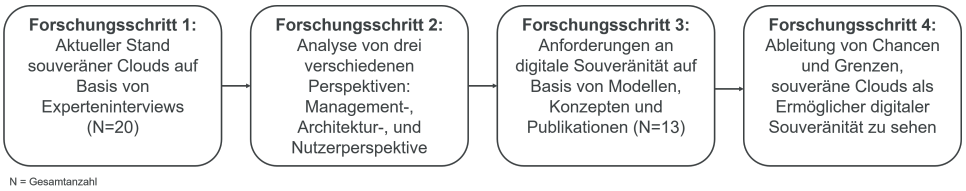


Abbildung 5.44: Forschungsdesign für die vorliegende Studie

Forschungsschritt 1 Im ersten Forschungsschritt stellt sich das aktuelle Verständnis souveräner Clouds anhand von N=20 Experteninterviews dar. Die Experten wurden teilweise über das eigene Netzwerk, hauptsächlich aber über LinkedIn rekrutiert. Es liegen 18 Audioaufnahmen vor, die zwischen mindestens 28 Minuten und maximal 1 Stunde und 22 Minuten dauern sowie zwei von den Experten schriftlich ausgefüllte Fragebögen. Die Fragen waren teilweise offen und halbstrukturiert, teilweise enthielten sie vordefinierte Antwortmöglichkeiten. Der Fragebogen kann dem Anhang entnommen werden (vgl. Abbildung 57 bis 58, Anhang). Es wird deutlich, dass sich im Fragebogen Fragen zu den einzelnen Faktoren des DISO-A-Modells widerfinden. Das soll eine bessere Auskunft darüber ermöglichen, ob die Cloud-Konzepte tatsächlich wesentliche Faktoren digitaler Souveränität abdecken.

Tabelle 5.10 gibt einen Überblick über die Berufsbezeichnungen und Fachgebiete der Experten. Besonderen Wert wurde darauf gelegt, die Abdeckung

verschiedener souveräner Cloud-Lösungen zu erzielen. Die Konzeptionierung der Experteninterviews orientiert sich an Meuser und Nagel (2009).

No.	Job title	Focus
1	Multi Cloud Architect	Amazon Web Services (AWS)
2	Cloud Solution Architect	Defense
3	Cloud Compliance Advisor	Product and Compliance Requirements
4	Senior IT Consultant	Cloud-Based ERP systems
5	Principle Cloud Architect	Transferring Traditional Infrastructure to the Cloud
6	Cloud Engineer	Google Cloud, Google Cloud Computing, Microsoft Azure, Oracle Cloud Infrastructure (OCI)
7	Cloud Consultant (Public Procurement Law)	Consulting on the Procurement of Cloud Services
8	Lead Architect	Responsibility for Setting up a Private Cloud, Cotainerization, Introducing Kubernetes
9	Cloud Engineer	Development of Technologies and Software
10	Technical Lead of the Project *Sovereign Cloud Stack*	Setting up a Sovereign Cloud
11	CEO und Consultant for Cloud Computing	AWS, Azure, JPS
12	Senior Cloud Engineer	Management of the entire Cloud Infrastructure
13	Senior IT Systems Engineer	Hybrid High-Security Cloud Environments
14	Freelancer Cloud Architect	Microsoft Technology
15	Process Consultant	Tenders from Public Institutions that want to move to the Cloud (mostly Private Cloud)
16	Lead Architect, Cloud Intrastructure Architect and Teamlead for the Topic *Public Cloud*	Open Telekom Cloud (European Cloud Concept)
17	IT-Sales Consultant	Running, Pptimizing and Monitoring of IT systems (mostly based on Cloud)
18	Cloud Architect	DevOps and Azure
19	Enterprise Architect	IT-Security-Critical Area
20	Business Development Architect and Public Affaires Specialist	Strategic Project Manager for the Cloud Project *National Secure Cloud*

Tabelle 5.10: Berufsbezeichnung und Schwerpunkt der Arbeit der befragten Experten

Forschungsschritt 2 Im zweiten Forschungsschritt werden drei verschiedene Analyse-Perspektiven auf Basis der Ergebnisse aus dem ersten Forschungsschritt aufgezeigt: eine Management-, eine Architektur- und eine Nutzerperspektive.

Forschungsschritt 3 Anforderungen zur Stärkung der digitalen Souveränität auf Basis einer spezifischen Auswahl von Publikationen, Konzepten und Modellen aus diesem Bereich, sind Teil von Forschungsschritt drei. Bei der systematischen Durchsicht der ausgewählten Studien half eine Anlehnung an den von Meline (2006) beschriebenen Prozessschritten: 1) Durchsicht von Abstracts und Titeln auf Basis von Ausschlusskriterien, 2) Eliminierung von Studien, die die Ausschlusskriterien erfüllen, 3) Durchsicht des Volltextes der verbliebenen Studien, 4) Bewertung hinsichtlich Ausschluss oder Einschluss eben dieser Studien, 5) Einschluss von Studien, die keine der Ausschlusskriterien erfüllen.

Letztendlich resultierte ein Überblick über N=13 Publikationen, anhand derer untersucht werden soll, welche Anforderungen an digitale Souveränität wesentlich in der Betrachtungsweise souveräner Clouds sind.

Forschungsschritt 4 Auf dieser Grundlage ist es Bestandteil von Forschungsschritt vier zu analysieren, ob souveräne Clouds eine Möglichkeit sind, mehr digitale Souveränität zu erreichen. Es ergibt sich an dieser Stelle eine Diskussion darüber, wie souveräne Clouds angepasst werden müssten, um stärker digitale Souveränitätsanforderungen zu inkludieren.

5.4.3 Ergebnisse aus den Interviews mit den Cloud-Experten

Wie in Abbildung 5.45 dargestellt, haben die meisten der Befragten viel Erfahrung mit dem Thema souveräne Clouds. Dieses Ergebnis bestätigt, dass tatsächlich Experten auf diesem Gebiet gefunden wurden. 35% haben zwischen eins und drei Jahren Erfahrung, 30% zwischen drei und sechs Jahren.

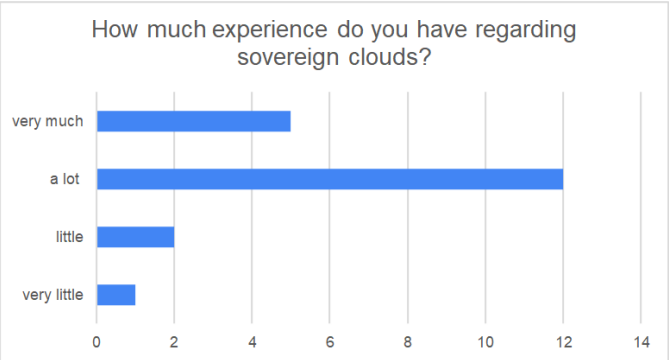


Abbildung 5.45: Erfahrung der Experten

Unterschiedliche Definitionen von souveränen Clouds

Es sind unterschiedliche Auffassungen von souveränen Clouds erkennbar. 40% sehen die Datensouveränität als Hauptziel souveräner Clouds, 30% mehr Unabhängigkeit von gewissen Partnern und 30% andere Gründe. Die Cloud-Experten sollten sich dazu äußern, was sie unter einer souveränen Cloud verstehen. Sie äußerten z.B.: „Eine spezielle Cloud mit spezifischen Compliance- und Sicherheitsrichtlinien, die von einer bestimmten Institution bereitgestellt wird, die besonders vertrauenswürdig ist“ oder „Souveränität in der Cloud ist eine Auswahl von Funktionen und Bereitstellungsmodellen, die

das erforderliche Maß an Kontrolle, Autonomie und Zuverlässigkeit erfüllen“ oder „ein Leitbild und ein zielgerichteter Begriff, der sehr interpretationsfähig ist, aber positiv wahrgenommen wird, weshalb Cloud-Anbieter diesen Begriff für ihr Marketing für sich beanspruchen - auch der Staat“. Es ist feststellbar, dass die Experten souveräne Clouds sehr unterschiedlich verstehen. Es liegt kein einheitliches Bild darüber vor, was souveräne Clouds sind. Die Verknüpfung zu digitaler Souveränität ist jedoch durch die Nennung von Themen wie IT-Sicherheit, Vertrauenswürdigkeit, Autonomie und Kontrolle erkennbar.

Hyperscaler haben Vorteile bei Skalierung, Support und Betrieb gegenüber souveränen Clouds

Hyperscaler sind Cloud-Anbieter mit einer sehr leistungsfähigen IT-Infrastruktur, die große Netzwerk-, Speicher- und Rechenressourcen bereitstellen (Bögelsack et al., 2022; Michels, 2025). Unabhängig vom jeweiligen Verständnis souveräner Clouds der Interviewten gibt es weitgehende Übereinstimmung, dass sie einen Gegenentwurf dazu darstellen.

Hyperscaler genießen besondere Vorteile gegenüber den souveränen Cloud-Konzepten von T-Systems, GAIA-X, der Bw, Microsoft, Oracle und IBM. Basierend auf 75% der Experten sind das Skalierungsoptionen, dann externe Unterstützung (50%), betriebliche Unterstützung (25%), Bereitstellung von Rechenzentren (35%), Best Practices (30%), Geschwindigkeit (20%) und 10% andere Punkte wie eine breite Palette an Plattformdiensten, auf die man zugreifen kann oder die Verfügbarkeit (vgl. Abbildung 5.46).

Die größten Herausforderungen von souveränen Clouds sind Kosten, Resilienz und Aufwand

Die größten Herausforderungen sind den Experten nach Kosten (55%), gefolgt von der Robustheit/Ausfallsicherheit der Cloud (40%) und dem zusätzlichen Aufwand für Organisation und technische Umsetzung (35%) (vgl. Abbildung 5.47). Kosten fallen ins Auge, weil es teuer ist, ein souveränes Cloud-Konzept im Markt zu implementieren. Robustheit/Ausfallsicherheit, weil es herausfordernd ist, diese Themen zu gewährleisten, ohne auf einen gängigen Hyperscaler zurückzugreifen. Und Aufwand, weil die Konzeption und Implementierung mit zeitlichem und personellem Ressourcenaufwand einhergeht. Die Experten wurden auch gefragt, wo sie die größten Hemmnisse

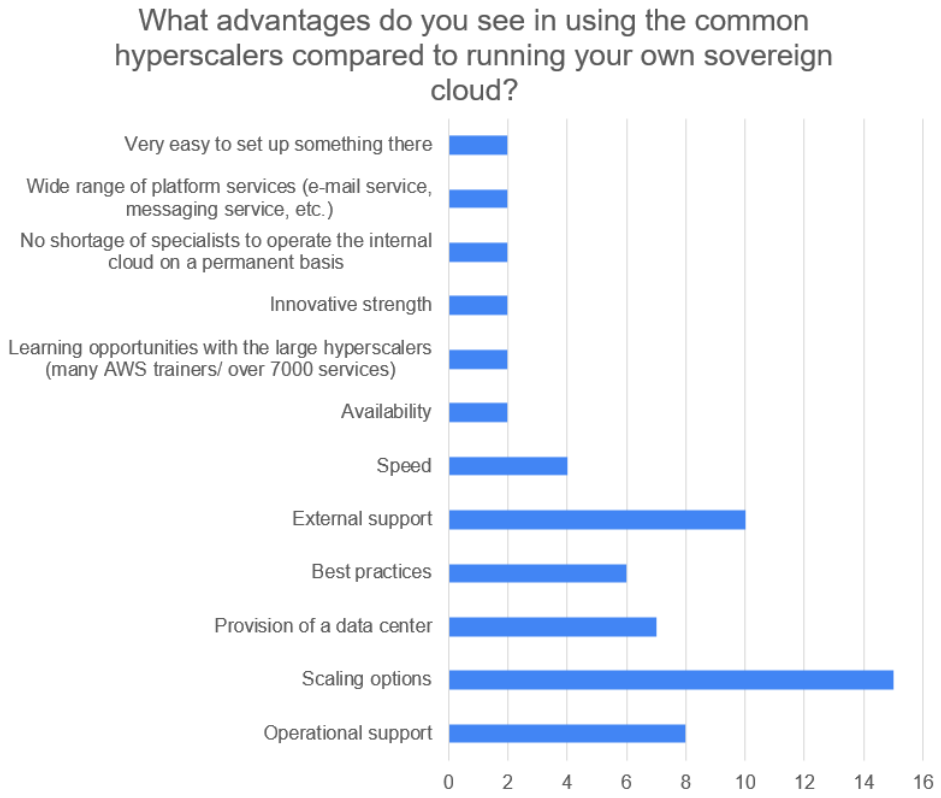


Abbildung 5.46: Vorteile beim Einsatz von Hyperscalern

für ihr Unternehmen bei der Einführung von souveränen Clouds in der Praxis sehen. 50% nannten technische Expertise und Know-how. Die gleiche Anzahl der Befragten nannte die Kosten. Hier offenbart sich, dass es auch eine Herausforderung ist, geeignete Partner und Anbieter zu finden (35%).

Nutzer fokussieren sich auf Einfachheit und Schnelligkeit bei Nutzung der Cloud

Nutzer der souveränen Cloud achten in erster Linie auf Geschwindigkeit (40%) und Benutzerfreundlichkeit (35%).

Der größte Mehrwert von souveränen Clouds ist die Einhaltung gesetzlicher Vorschriften

Anschließend sollten die Experten bewerten, worin der größte wahrgenommene Mehrwert einer souveränen Cloud für sie besteht. Die meisten Befragten nannten an erster Stelle die Einhaltung gesetzlicher Vorschriften, an zweiter

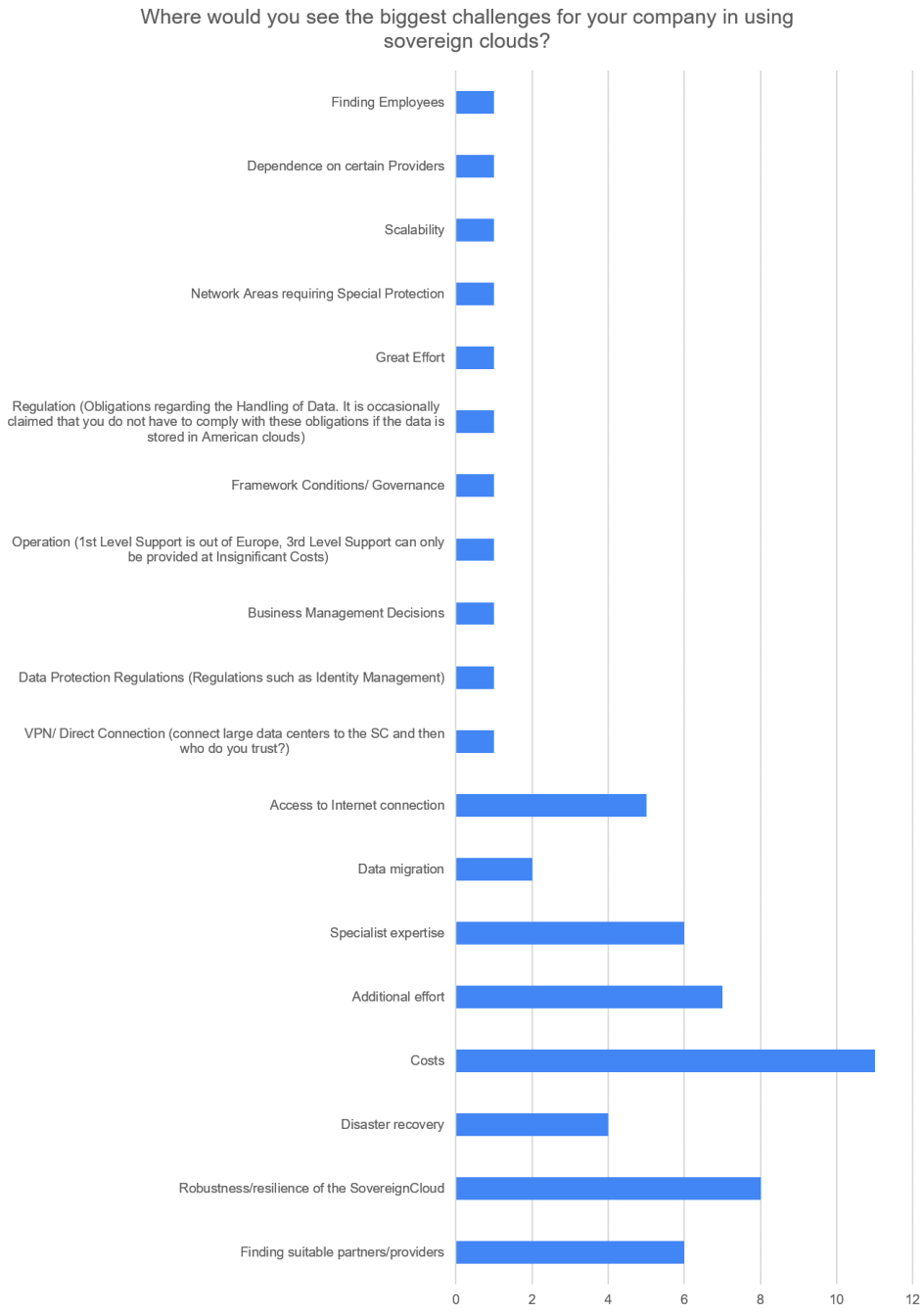


Abbildung 5.47: Größte Herausforderungen bei der Nutzung souveräner Clouds

Stelle mehr Kontrolle über die Daten und an dritter Stelle die Möglichkeit, mit Komplexität (z.B. komplexen Vorschriften) umzugehen.

Abdeckung der Faktoren digitaler Souveränität aus dem DISO-A-Modell

Als nächstes war es das Ziel, besser zu verstehen, wie gut die souveränen Cloudkonzepte einzelne Faktoren aus dem DISO-A-Modell abbilden. Hintergrund ist, dass das DISO-A-Modell ein sehr umfassendes Verständnis digitaler Souveränität aufweist. Durch die Kopplung dieser Interviewergebnisse mit den Ergebnissen aus den vorangegangenen Studien lässt sich feststellen, ob souveräne Clouds das Potenzial haben, verschiedene Facetten im Kontext digitaler Souveränität erfolgreich zu adressieren. Der Fokus fällt auf folgende Themen aus dem DISO-A-Modell: 1) IT-Sicherheit, 2) Ausfallsicherheit, 3) digitale Lieferkette, 4) Kernkompetenzen, 5) Zugang zu Kunden, 6) Umgang mit dem Wettbewerb und 7) Offenheit der Technologie.

1. IT Sicherheit wird nicht ausreichend abgebildet Es ist erkennbar, dass die souveränen Cloud-Konzepte nicht ausreichen, um eine stärkere Form von IT-Sicherheit zu gewährleisten. Denn nach Ansicht von 85% der Experten sind Unternehmen, die eine souveräne Cloud nutzen, nicht besser gegen Schwachstellen geschützt als Unternehmen, die ein Public Cloud-Angebot nutzen. 80% der Experten glauben nicht, dass Unternehmen mit einer souveränen Cloud tatsächlich besser gegen externe Hacker geschützt sind. Immerhin 80% sind der Meinung, dass die Kunden nach ihren Vorstellungen mit einer souveränen Cloud besser vor unerwünschten Funktionalitäten in der Datenverarbeitung geschützt sind als vorher.

2. Resilienz wird abgebildet Resilienz wird in vielen der souveränen Cloud-Konzepte mitgedacht. In diesem Frageblock geben 50% der Experten an, dass Unternehmen, die ihr souveränes Cloud-Konzept nutzen, nun besser in der Lage sind, sich schnell von unerwünschten Ereignissen zu erholen (z.B. wenn das Rechenzentrum abbrennt). Diese Antwort erfolgte im Vergleich zu den Konzepten, die die Unternehmen vorher nutzten. Allerdings glauben wiederum 50% nicht, dass ihre Kunden nun besser in der Lage sind, schneller auf Probleme zu reagieren, weil es dafür weiterer Maßnahmen bedarf. Die Uneindeutigkeit der Ergebnisse könnte zusätzlich darauf zurückzuführen sein,

dass ein Hyperscaler auch das Thema Resilienz gut abdecken kann und bestätigt ein Ergebnis der ersten Fallstudie: dass digitale Souveränität nicht nur aus technischer Brille betrachtet werden sollte, sondern mit zusätzlichen Maßnahmen auch aus einer strategischen.

3. Souveränere digitale Lieferketten werden nicht hinreichend abgebildet Unseren Ergebnissen nach können Lieferketten durch souveräne Clouds sicherer gestaltet werden. Viele der Experten decken dieses Thema aber noch nicht in ihren souveränen Cloud-Konzepten ab. Ihrer Meinung nach macht die Wahl vertrauenswürdiger Anbieter die digitale Lieferkette sicherer (85%). 80% der Experten sind der Meinung, dass Unternehmen mit einem der in Abschnitt 5.4 vorgestellten souveränen Cloud-Konzepte nun – im Vergleich zu den zuvor verwendeten Konzepten – mehr Kontrolle über ihre digitale Lieferkette erlangen können. Das führt zu dem Schluss, dass mehr Sicherheit in digitalen Lieferketten erreicht werden kann, aber nur, wenn diese Dimension auch im Rahmen des entsprechenden Konzeptes zu Beginn berücksichtigt wird. Dies ist im Rahmen der Cloudkonzepte derzeit noch nicht flächendeckend erkennbar.

4. Kernkompetenzen werden in unterschiedlicher Tiefe abgebildet Die Experten weisen Kernkompetenzen im Kontext souveräner Clouds und digitaler Souveränität auf. Diese unterscheiden sich jedoch gravierend in der Tiefe. Die meisten Unternehmen bieten Beratungsdienste an. Konkrete Beispiele sind Requirements Engineering, Konzeption, Architekturberatung und Cloud-Migration zu einem der großen Hyperscaler. Einige Unternehmen bieten auch Sicherheitsberatung an. Allerdings bieten nur wenige Unternehmen Softwareentwicklung an und sind in der Lage, die gesamte Wertschöpfungskette vom Vertrieb bis zum Betrieb eigenständig abzudecken. Daraus ist zu schließen, dass für die erfolgreiche Implementierung souveräner Clouds, die über die Angebote der Hyperscaler hinausgehen, mehr Expertise im selbstverwalteten Betrieb benötigt wird. Zusammenfassend lässt sich also sagen, dass Kompetenzen stärker auf eine unabhängigere Operationalisierung digitaler Souveränität auszurichten sind.

5. Im öffentlichen Sektor besserer Kundenzugang vorhanden als im privaten Sektor Den Daten dieser Studie zufolge werden souveräne Clouds überwiegend im öffentlichen Sektor (85%) eingesetzt, was angesichts der besonderen Bedeutung des Schutzes staatlicher Daten nicht überraschend ist. Überraschenderwei-

se berichten jedoch 65% der Experten auch von potenziellen Anwendungen im privaten Sektor. Den Kundenzugang gilt es jedoch weiter auszubauen. Zu den Vorteilen, die Unternehmen diesen Kunden bieten können, gehören: die Gewährleistung, dass die Daten in einem vertrauenswürdigen Land liegen (70%), die Gewährleistung der Datenhoheit (70%), eine bessere Vertrauensbildung (60%) und die Ermöglichung einer autonomeren Entscheidungsfindung (50%).

6. Umgang mit dem Wettbewerb ist schwierig Nach Ansicht von 60% der Experten ist die Expansion mit einem souveränen Cloud-Konzept eingeschränkt oder schwierig. Die Experten berichten, dass sie mit der souveränen Cloud mehr lokale Konkurrenten und Lieferanten haben und dass sich die Kooperationen verändern.

7. Geschwindigkeit, Wechselbarrieren und Verhandlungsspielraum bei souveränen Clouds 75% der Experten sind der Meinung, dass Technologien und Services bei der souveränen Cloud langsamer eingeführt werden. 65% der Teilnehmer sagen, dass es eher oder sehr schwer ist, die Entscheidung für eine souveräne Cloud rückgängig zu machen. Außerdem betonen die meisten Teilnehmer, dass sie eher wenige oder keine Möglichkeiten haben, auf Preisänderungen der Cloud-Anbieter zu reagieren (70%). Diese Erkenntnis unterstreicht die Notwendigkeit, digitale Souveränität im Zusammenhang mit technischen Cloud-Lösungen stärker zu betrachten.

Im Abschnitt Ausblick gehen 95% der Experten davon aus, dass die souveräne Cloud die Bewältigung geopolitischer Probleme in Zukunft erleichtern wird (z.B. das Fernhalten politischer Gegner, insbesondere bestimmter Länder, von bestimmten digitalen Bereichen). Das erklärt, warum als wesentlicher Kundenstamm souveräner Clouds der öffentliche Sektor gesehen wird. Immerhin 70% verweisen hier nochmals darauf, dass es in Zukunft nicht weniger Cybersicherheitsarbeit mit souveränen Clouds geben wird. Schließlich äußern 65%, dass die Einführung von souveränen Clouds die Wettbewerbsfähigkeit von Unternehmen langfristig erhöhen kann, es aber eine Frage der Strategie ist.

Zudem kristallisieren sich zwei Konzepte für eine stärkere Integration digitaler Souveränität heraus: eine souveräne Cloud open stack entwickeln oder ein Multi-Cloud-Konzept designen.

5.4.4 Analyse von drei Perspektiven: Management-, Architektur- und Nutzerperspektive

Management-Perspektive: Manager brauchen Guidelines, um besser prüfen zu können, welches souveräne Cloudkonzept am besten welche digitalen Souveränitätsanforderungen abdeckt

Die Darstellung der Management-Perspektive erfolgt vor dem Hintergrund der Frage, wie Manager unterstützt werden können, digitale Souveränität zu stärken. Es werden Herausforderungen und Möglichkeiten aus der vorangegangenen Interviewstudie dafür herangezogen.

Auf Basis der Daten ist es möglich, für Manager 25 Faktoren zu liefern, die eine wichtige Rolle bei der Entscheidung für ein passendes souveränes Cloud-Konzept (Open Stack vs. Multi-Cloud-Konzept) spielen (vgl. Tabelle 5.11).

Die folgenden 25 Faktoren können Managern, die sich mit den Herausforderungen bei der Stärkung der digitalen Souveränität durch eine souveräne Cloud-Lösung auseinandersetzen, als Orientierung dienen.

Transparenz: Manager sollten entscheiden, welchen Grad an Transparenz sie benötigen. Sollte das Unternehmen nach einem besonders hohen Grad an Transparenz streben, so sollte die Entwicklung mit Open Source und damit das Zurückgreifen auf Open Stack in Erwägung gezogen werden. **Kontrolle:** Manager sollten entscheiden, wie viel Kontrolle sie über das, was entwickelt wird, haben wollen. Mit Open Source und einem Open Stack können Sie einen besonders hohen Grad der Kontrolle erreichen. Bei einem Multi-Cloud-Konzept sind Kontrollmechanismen vertraglicher Natur möglich. **Skalierung:** Manager sollten festlegen, wie stark sie skalieren wollen. **Kosteneffizienz:** Die Manager sollten auch die Kosten für Hardware, Personal, usw. berücksichtigen. **Datenzentren:** Manager sollten bedenken, dass sie entweder Rechenzentren bauen müssen, was mit einem erheblichen Anfangsaufwand verbunden ist, oder für bestehende Rechenzentren bezahlen müssen. Im Sinne digitaler Souveränität ist die Wahrung von Datenschutz und Geschäftsgeheimnissen zu berücksichtigen. Um digitale Souveränitätsziele zu erreichen, ist aber nicht zwangsweise ein OpenStack-Ansatz notwendig (Hartmann, 2021). **API-Verbindung:** Manager sollten die Komplexität der Integration nicht unterschätzen. **Compliance:** Manager sollten ihre spezifischen Compliance-Anforderungen von

No	Factors	Explanation
1	Transparency	The advantage of open source is full transparency
2	Control	The advantage of open source is full control over what you have developed
3	Scaling	Will probably be easier with a multi cloud concept
4	Cost efficiency	You have very high initial costs with open stack in hardware, human ressources, etc. You can gain price advantages with a multi cloud concept
5	Speed (through access)	Data centers can be accessed easier with a multi cloud concept. With my own operation, I would have to set it up first
6	API connection	Open Stack: APIs are more open, it's easier to integrate or connect data here than with different companies
7	Compliance	If you have specific requirements, it might be easier to look for someone who can do it (multi cloud concept saves time, Focus on core competence simpler). You don't have to do it yourself (open stack)
8	IT security	Multiple platforms give you a larger attack surface
9	Skills	You have to look for experts for Open Stack, there are very different ecosystems for which you need experts
10	Resilience	With open stack, resilient infrastructure comes with high costs. Geographical distribution is also possible with hyperscalers or a multicloud concept. Initial multicloud is more scalable
11	Complexity	A multi-cloud can become very complex. If you have different systems that depend on each other, you have to look at whether and how you can get the systems up and running again after a disaster
12	Independence	You are not so dependent on others if you use Open Stack
13	SLAs and costs	In extreme cases, you may be able to get help faster from Open Stack, but only if you have your own staff. If you have recourse to the Hyerscaler, this can be very expensive
14	Speed	Resource availability is better with a multi-cloud concept. Hyperscalers in particular can react quickly due to their staff density
15	Innovation	Development of prototypes and innovative solutions is easier with hyperscalers
16	Digital supply chain	Open stack offers more control over your own supply chain because you know exactly what you are using
17	Disaster recovery	You can do distaster recovery on many levels yourself. These are concepts that are not necessarily feasible with Multi Cloud. It depends on the scope you need. Multi cloud as a concept carries the risk that it won't work because at some point you lose the overview and therefore control
18	Data sovereignty	Data sovereignty in both cases higher but a higher degree of data sovereignty can be achieved with open stack
19	Self-determined decisions	Easier to achieve with open stack. With a multi-cloud concept, you have to take what the providers offer you
20	Additional effort	It depends on the management of the multi-cloud. It mightl be more complex in operation with a multi cloud concept, the set-up will also be more complex because you then have to make sure that you can get different systems up and running. With Open Stack, you may have less effort here. It is much more complex to scale it (due to physical resource problems and more costly depending on how many persons you need, for example system admins)
21	Operational support	Operational support is easier with multi-cloud
22	Scaling options	Scaling can be implemented more quickly with multi-cloud
23	Provision of a data center	You have to be a big player to set something like this up or have a large funding base and time. So it's faster with a multi-cloud concept
24	Best practices	Multi-cloud is more likely to be available than open stack. Best pracitces still need to be developed for open stack
25	Support	These concepts are already in place with all the multi-cloud soultions. With Open Stack, you first have to develop concepts, which is not trivial. But again, it depends. Just because you say that it's a big company you're using doesn't automatically mean that the support is good

Tabelle 5.11: Analyseergebnis Managementperspektive

Anfang an berücksichtigen. **IT-Sicherheit:** Manager sollten beachten, dass mehrere Plattformen zu einer größeren Angriffsfläche führen können. Wenn die IT-Sicherheit intern implementiert wird, müssen die Manager Zeit und Personalressourcen dafür bereitstellen. **Fähigkeiten:** Manager sollten sich darüber im Klaren sein, dass, wenn sie auf das souveräne Cloud-Konzept angewiesen sind, spezifische Fähigkeiten erforderlich sein können, die auf dem Markt manchmal schwer zu beschaffen sind. **Komplexität:** Manager sollten bedenken, dass insbesondere bei einem Multi-Cloud-Konzept die Komplexität mit der Anzahl der Anbieter steigt. **Unabhängigkeit:** Manager sollten berücksichtigen, dass sie mit OpenStack weniger abhängig von anderen sind. Um digitale Souveränitätsziele zu erreichen, ist aber nicht zwangsweise ein OpenStack-Ansatz notwendig (Rikap et al., 2024). **Service Level Agreements (SLAs) und Kosten**: Manager sollten SLAs definieren, wenn sie eine souveräne Cloud aufbauen oder ein Multi-Cloud-Konzept einführen, und abschätzen, wie teuer es sein wird, diese SLAs einzuhalten. **Geschwindigkeit:** Die Manager sollten beachten, dass man Unternehmen bei einem Multi-Cloud-Konzept zur Einhaltung bestimmter Latenzen, Verfügbarkeiten und SLAs verpflichten kann. **Innovation:** Die Manager sollten sicherstellen, dass sowohl der konzeptionelle als auch der technische Rahmen die Entwicklung von Prototypen und innovativen Lösungen ermöglicht. **Digitale Lieferkette:** Manager sollten bewerten, inwieweit sie mehr Kontrolle über die digitale Lieferkette benötigen. **Disaster Recovery:** Manager sollten entscheiden, wie sie die Notfallwiederherstellung umsetzen wollen. **Datensouveränität:** Manager sollten berücksichtigen, dass verschiedene Konzepte die Datensouveränität verbessern können. Es ist notwendig, eine Abschätzung zu treffen, welcher Grad an Sicherheit gewünscht ist (Moerel & Timmers, 2021). **Selbstbestimmte Entscheidungen:** Manager sollten bedenken, dass selbstbestimmte Entscheidungen mit OpenStack leichter zu erreichen sind. Bei einem Multi-Cloud-Konzept ist man auf das Angebot der Provider beschränkt. Mit einer maßgeschneiderten Lösung eines Anbieters müssen Manager ihre Freiheitsgrade sorgfältiger prüfen. **Zusätzlicher Aufwand:** Der Betrieb eines Multi-Cloud-Konzepts kann komplexer sein, und auch die Einrichtung wird komplizierter, da die Funktionalität der verschiedenen Systeme sichergestellt werden muss. Mit OpenStack kann

dieser Aufwand geringer sein. Allerdings kann die Skalierung von OpenStack aufgrund der begrenzten physischen Ressourcen und der potenziell höheren Kosten deutlich komplexer sein, je nachdem, wie viele personelle Ressourcen, z.B. Systemadministratoren, benötigt werden. **Externer Support:** Die Manager sollten bedenken, dass der Support entweder mit zusätzlichen Ressourcen bereitgestellt oder extern eingekauft werden muss. **Operationale Unterstützung:** Manager sollten bedenken, dass die betriebliche Unterstützung bei einem großen Akteur einfacher ist. Um diese Unterstützung unabhängig zu leisten, ist eine sorgfältige Prüfung und Planung erforderlich. **Skalierungsoptionen:** Manager sollten bedenken, dass die Skalierung mit einem Hyperscaler schneller umgesetzt werden kann. **Bereitstellung eines Rechenzentrums:** Manager sollten berücksichtigen, dass die Kapazitätsplanung und Leistungszusicherung bei Rechenzentrumsplanungen ein Zurückgreifen auf ein großes Unternehmen oder erhebliche finanzielle und zeitliche Mittel erfordert. **Best Practices:** Manager sollten bedenken, dass Best Practices eher bei einem Multi-Cloud-Konzept verfügbar sind. Wenn eine souveräne OpenStack-Cloud unabhängig aufgebaut wird, müssen Best Practices erst noch entwickelt werden, was mit einem zeitlichen Nachteil einhergehen kann.

Den Ergebnissen nach ist es für Manager empfehlenswert, diese Faktoren zu berücksichtigen, um zu prüfen, welches souveräne Cloud-Konzept für ihre Anforderungen an digitale Souveränität geeignet ist.

Architektur-Perspektive: die Analyse der Architekturen der Cloudkonzepte zeigt einen starken Fokus auf Datensouveränität

Rückblickend ging aus dem DISO-A-Modell hervor, dass es hilfreich sein könnte, Konzepte wie GAIA-X zu validieren. In diesem Abschnitt wird dieser Forderung nachgegangen: Die IT-Architekturen von GAIA-X und den anderen Cloud-Konzepten werden gegenübergestellt und wesentliche Unterschiede herausgestellt. Die Gegenüberstellung der Unterschiede erfolgt vor dem Hintergrund der Frage, inwieweit aus der IT-Architektur des jeweiligen Cloudkonzepts ersichtlich wird, dass digitale Souveränität unterstützt werden kann.

Vergleicht man die Architekturen der Anbieter, so stellt man außerdem fest, dass die meisten souveränen Cloud-Angebote einen starken Fokus auf die Datensouveränität legen (vgl. Abbildung 5.48). Zudem wird deutlich, dass die ana-

lysierten souveränen Cloud-Konzepte in folgenden Dimensionen einen Beitrag für mehr digitale Souveränität leisten können: Datensouveränität, Softwaresouveränität, operationale Souveränität und die Schaffung von mehr Transparenz.

Nutzer-Perspektive: Schnelligkeit und einfache Handhabung vorrangig für Nutzer

Die Analyse der Nutzerperspektive erfolgt vor dem Hintergrund der Frage, inwieweit Nutzer bei der Gestaltung digitaler Souveränität inkludiert werden sollten.

Aus der Interviewstudie eröffnet sich das Ergebnis, dass es den Nutzern nach zweitrangig zu sein scheint, dass die Cloud souverän ist (vgl. Abbildung 5.49). Der Schwerpunkt liegt darauf, die Cloud schnell und einfach nutzen zu können, das ging aus den Befragungen mit den Cloud-Experten hervor (vgl. Kapitel 5.4.3). Auch bei den Interviews mit den Professoren vermuteten sie, dass Nutzer im Zweifel nicht auf Risiko, Technologie oder Ethik eines digitalen Produktes achten, sondern vielmehr den Mehrwert in den Vordergrund stellen (vgl. Kapitel 4.3). Unsere Ergebnisse hier bestätigen diese Vermutung.

5.4.5 Diskussion

5.4.5.1 Was sind Anforderungen an digitale Souveränität, die im Rahmen der souveränen Cloud-Konzepte nicht umgesetzt wurden?

Aus den Experteninterviews ging hervor, dass über 80% der Cloud-Spezialisten nicht glauben, dass die analysierten souveränen Cloudkonzepte besser gegen Schwachstellen oder externe Hacker schützen können. Das führt zu der Notwendigkeit, IT-Sicherheitsmaßnahmen vor dem Hintergrund von digitaler Unabhängigkeit, Handlungsfähigkeit und Risikoabwägung bereits bei der Konzeption der souveränen Cloud-Konzepte stärker mitdenken zu müssen. Um einen umfassenderen Grad an digitaler Souveränität zu erreichen, sollten Projektleiter und Manager stärker das Thema IT-Sicherheit in der Planungsphase berücksichtigen. Dies geht auch einher mit den Ergebnissen von Goldacker (2017). Ziel sollte es sein, mit souveränen Clouds nicht nur die technologische, sondern auch die organisationale Vertrauenswürdigkeit zu stärken (vgl. Kapitel 4.3.3.1). Die vorliegenden Ergebnisse bestätigen damit die Forderung von Beye-

T-Systems Sovereign Cloud powered by Google Cloud	Sovereign Cloud Stack for GAIA-X	pCloudBw	European digital sovereignty — Amazon Web Services	Microsoft Cloud for Sovereignty	Oracle European Union Sovereign Cloud	IBM Sovereign Cloud Capabilities
Data Sovereignty	**Eliminating data silos/ ensuring interoperability**	**Autarky**	**Data Sovereignty**	**Data Sovereignty**	**Data Sovereignty**	**Data Sovereignty**
The aim is to give the owner of the data the certainty that their data in the cloud cannot be copied, manipulated, deleted or viewed by unauthorized persons. T-Systems also includes the provider. T-Systems determines the management of the keys in an external key management system so that the operator has no access to the keys.	Gaia-X is a cloud ecosystem designed to ensure that data can be merged or shared securely, transparently and in compliance with data protection regulations of the European Union. In its early days, the aim of GAIA-X was to break down data silos and merge existing data spaces. Today, GAIA-X is an offer to share data in a decentralized and interoperable way.	Independence from providers, a single cloud agent that a) originates from Germany b) acts as a subsidiary of the Federal Ministry of Defense and c) takes over operations for the Bundeswehr in Germany.	By using the Eviden XKS service together with the AWS service, users can generate, rotate or delete their keys, giving them extensive control over their data.	With its solution, Microsoft offers greater transparency about the storage location, use of data and therefore more control over the data. Data backup during transmission and at rest. To ensure greater data resilience, the use of encryption and compliance with regulatory requirements of the European Union. The use of cloud HSMs (hardware security modules) supports the cryptographic processes.	The EU Sovereign Cloud offers OCI customers the following functions: • Data protection via service protection and data replication • Access to models via virtual networks • Security models via IAM • Auditing of compliance modeling and governance	At IBM, data sovereignty is to be guaranteed in various technical ways, for example through: • IBM Cloud Satellite Control Plane • VM to a private cloud from IBM *or* Cloud Satellite Location from AWS *or* Cloud Satellite Location on premise *or* IBM Cloud Services on own infrastructure with characteristics of a public cloud
Operational Sovereignty	**Vendor Sovereignty**	**Data Sovereignty**	**Consulting**	**Operations**		**Operations**
Within the framework of operational sovereignty, users are given transparency and control over the provider's operating activities. In this specific case, T-Systems monitors Google as the provider of the platform and ensures that adjustments to the platform do not undermine T-Systems' understanding of sovereignty. The platform's performance and future security shall be ensured with Google as strategic partner.	The aim of vendor independence is to ensure dependency on cloud providers as well as software and hardware. To this end, GAIA-X provides decentralized infrastructures that enable IT systems to work together independently of the provider or software.	• As few external APIs as possible • Ensuring that data is protected. However, data exchange should still be possible.	With Eviden, AWS offers a strategic consulting partner who, together with the customer, 1) classifies sovereignty challenges, 2) defines goals, 3) describes risks, 4) defines a suitable framework with the customer and finally 5) implements it. This is where the customer enters the build and run phase of Amazon.	Microsoft takes over the operation of the cloud. Performance and scaling options as required.		IBM takes over the operation (with providers). Fast provisioning and pay-as-you-go concept as required.
Provider Sovereignty	**Transparency**		**Operations**			**Management**
In order to achieve software sovereignty, T-Systems is adopting the concept of an open platform. This is intended to prevent users from becoming trapped in excessive vendor lock-ins. The services and applications are orchestrated in a multi-cloud landscape. This should enable customers to migrate to a different IT infrastructure as quickly as possible.	To ensure transparency, an open source approach was chosen in GAIA-X. The code is freely accessible to everyone. What happens to the respective user data is also shared.		Amazon takes over the operation of the cloud.			IBM offers the following control functions: • Internal Management • Access Management
						Transparency
						IBM increases transparency through: • Cloud services based on open source technologies • Open multi-cloud concept

Abbildung 5.48: Analyseergebnis Architektur-Perspektive

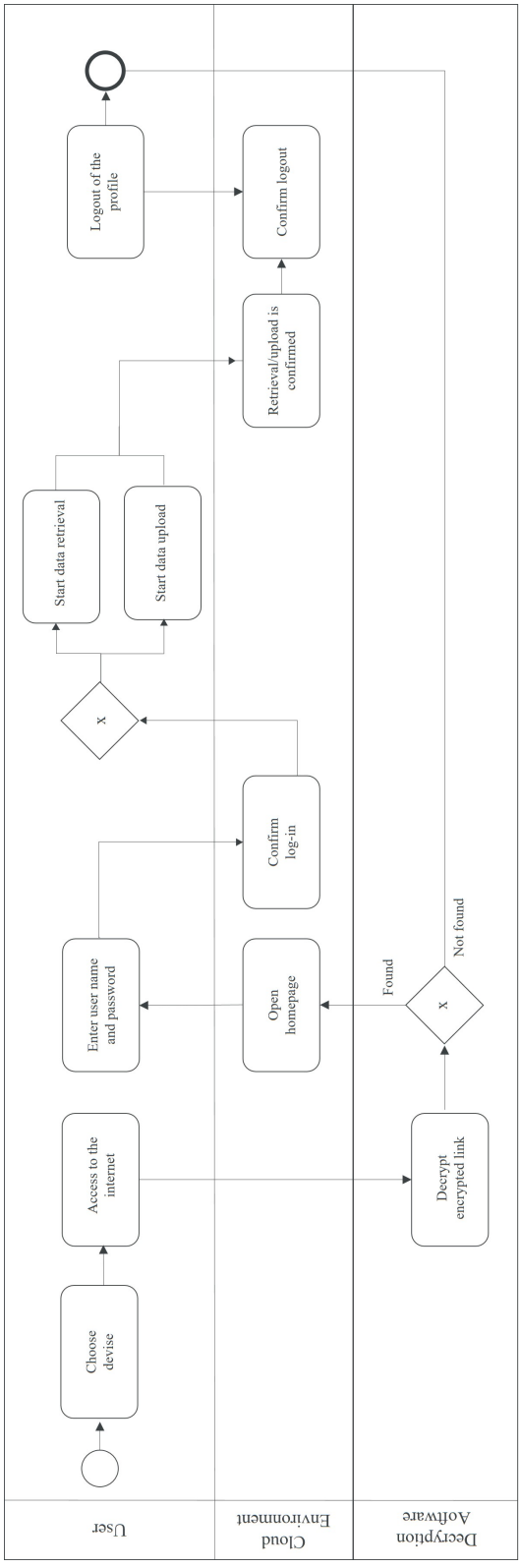


Abbildung 5.49: Analyseergebnis Nutzerperspektive

rer et al. (2018), Bogenstahl und Zinke (2017) und Vogt (2021), die ebenfalls mehr Vertrauenswürdigkeit im Kontext digitaler Souveränität fordern.

Um mehr digitale Souveränität zu erreichen, schlägt Sheikh (2022) vor, die Beschaffung von Chips, die Gestaltung von Netzfragen wie 5G, die Schaffung intelligenter, vernetzter Anwendungen und Geräte aus Europa zu berücksichtigen. Ein zentrales Ziel ist die Reduzierung von Abhängigkeiten und Schwachstellen entlang der gesamten Wertschöpfungskette von Unternehmen und die Verringerung der starken Abhängigkeit von Hard- und Software aus den USA und China (Chakhava & Hikes-Wurm, 2024). Das ging auch aus der systematischen Literaturrecherche zu digitaler Souveränität in dieser Arbeit hervor (vgl. Kapitel 4.1). Es wurde aus den Ergebnissen deutlich, dass viele souveräne Cloudkonzepte weiterhin auf amerikanische Lösungen setzen. Das scheint nicht verwunderlich, weil aus den Ergebnissen auch hervorging, dass insbesondere die amerikanischen Hyperscaler mit besseren Skalierungs-, Support- und Betreibermöglichkeiten punkten. Ebendiese Konzepte inkludieren aber keine alternative Beschaffung aus lediglich europäischen Ländern. Den Ergebnissen dieser Arbeit nach ist dieser Punkt jedoch kritisch zu betrachten, da er durch Zielkonflikte geprägt ist (vgl. Kapitel 4.1). Man begegnet hier der Herausforderung, dass man nicht für alle oben genannten Segmente gute Alternativen in der EU findet (vgl. Kapitel 5.2).

Die EU möchte mehr Kontrolle über die Fähigkeit, die Produktion, das Design, die Nutzung und den Output digitaler Technologien haben, um ein wichtiger digitaler Akteur zu werden (Davies et al., 2023). Sowohl der Staat als auch die Unternehmen haben die Möglichkeit, Regelungen zu definieren, die es den Nutzern erlauben, selbst zu entscheiden, welche persönlichen Daten sie (nicht) weitergeben wollen (Pohle, 2020). Den Ergebnissen nach ist es herausfordernd, den Nutzer zu digital souveränerem Verhalten zu akquirieren. Es war möglich, aufzuzeigen, dass Nutzer insbesondere auf eine einfache Handhabung und Schnelligkeit setzen. Um digitale Souveränitätsanforderungen stärker in souveräne Cloudkonzepte zu inkludieren, ist als Argument anzuführen, dass Manager und Projektleiter eine stärkere Ausrichtung auf digitale Souveränität brauchen. Sie brauchen eine Referenz, an der sie sich orientieren können.

5.4.5.2 Was hat sich verändert im Vergleich zu den anderen Ergebnissen der Arbeit?

Es ist zu beobachten, dass eine stärkere Auseinandersetzung mit dem Thema digitale Souveränität erfolgt und dass mit souveränen Clouds erste Konzepte der Umsetzung ihren Weg in den Markt finden. 2022 wurde innerhalb einer Umfrage-Studie gezeigt, dass zwar 79% der Befragten das Thema bekannt ist, über 60% der Unternehmen aber noch gar keine oder kaum Maßnahmen ergreifen, um diese zu erreichen. Operationalisierungsideen steckten zu dieser Zeit noch in der Planungsphase. Die Cloudexperten hier - im Jahr 2024 - weisen Kernkompetenzen im Kontext souveräner Clouds auf und teilen ein umfassenderes Verständnis digitaler Souveränität, als das im Jahr 2022 zu erkennen war. Diese unterscheiden sich jedoch in der Fokussierung und gravierend in der Tiefe (vgl. Kapitel 5.4.3).

5.4.5.3 Wie müssen nun die souveränen Cloud-Konzepte angepasst werden, damit ein höherer Grad digitaler Souveränität erreicht wird?

Vergleicht man die Ergebnisse aus den Experteninterviews und die Analyseergebnisse mit den in Publikationen, Konzepten und Modellen identifizierten Anforderungen an digitale Souveränität, so stellt man fest, dass souveräne Clouds zwar in bestimmten Segmenten zu mehr digitaler Souveränität beitragen können, für eine umfassende Form digitaler Souveränität jedoch mehr erforderlich ist.

Die Cloud-Experten sollten äußern, ob sie glauben, dass man mit souveränen Clouds eine bessere Lieferkettenkontrolle abbilden könnte. 80% der Experten sind der Meinung: ja. Die Publikationen von Andenmatten (2023), Moerel und Timmers (2021) und Skierka (2020) fordern ebenfalls die Berücksichtigung sicherer, souveränerer Lieferketten. Dies geht auch mit den Ergebnissen aus dieser Arbeit (vgl. Kapitel 5.2) einher. Aus diesem Grund scheint dieser Use-Case sinnvoll zu sein, um eine stärkere Form digitaler Souveränität mit Hilfe eines souveränen Technologie-Stacks zu erzielen. Eine Entkopplung der Cloud-Konzepte von den jetzigen Zielen (sehr starker Fokus auf Datensouveränität) und eine stärkere Ausrichtung auf einen derartigen

Use-Case, der einen höheren Grad digitaler Souveränität inkludiert, könnte damit als Anpassung in Frage kommen.

Schließlich ist zu empfehlen, sich intensiver mit dem Thema Schlüsseltechnologien und Offenheit von souveränen Cloud-Technologien zu beschäftigen. Dies geht in eine etwas andere Richtung, als bei den Forderungen von Peuker (2020), die eher die Beherrschung ebendieser Schlüsseltechnologien fordern. Oder Beyerer et al. (2018), die die Eigenentwicklung von Schlüsseltechnologien in den Vordergrund rücken. Die Forderung auf Basis dieser Studiendaten zielt eher auf eine Entscheidung in der Konzeptphase ab, auf welche Schlüsseltechnologien man setzen will, da dies tragende Auswirkungen auf die IT-Architektur des souveränen Cloudkonzepts haben wird. Es ist im Sinne digitaler Souveränität, moderne, leistungsfähige und wettbewerbsfähige Produkte zu bauen, gleichzeitig jedoch Themen wie IT-Sicherheit, mehr Vertrauenswürdigkeit und Unabhängigkeit mitzudenken (Pohle, 2020). Der Einsatz moderner Schlüsseltechnologien und das Setzen auf Open Source kann hier einen Beitrag leisten, das zeigten bereits die vorangegangenen Ergebnisse aus Kapitel 5.1 und 5.2.

5.4.6 Zusammenfassung, Limitationen und Ausblick

Es sind die Cloud-Konzepte von T-Systems mit Google, Amazon, Microsoft, Oracle und IBM, GAIA-X als Cloud-Ökosystem sowie eine Private Cloud aus dem militärischen Bereich in Deutschland analysiert worden.

Die Ergebnisse zeigen, dass sie einen Beitrag für mehr digitale Souveränität auf der Daten-, Operationalisierungs- und Software- sowie Transparenzebene leisten. Die sieben Cloudkonzepte befassen sich mit Aspekten wie Wahrung der Datenhoheit, Überdenken von Partnerschaften und Etablierung von Open Source. Souveräne Clouds werden jedoch sehr unterschiedlich definiert und der Zweck dieser unterschiedlich verstanden. Aus der Nutzerperspektive wird deutlich, dass die Nutzer in erster Linie auf die Benutzerfreundlichkeit und Geschwindigkeit der Cloud achten. Die Ergebnisse dieses Kapitels zeigen auch, dass Manager und Projektleiter eine Referenz für eine stärkere Inklusion digitaler Souveränitätsanforderungen in souveräne Cloudkonzepte benötigen. Ein griffiger Use-Case, bei dem 1) wesentliche Anforderungen digitaler Souveränität inkludiert werden, 2) auf Open-Source gesetzt wird und 3) eine

Entscheidung für eine wesentliche Schlüsseltechnologie (z.B. KI) getroffen wird, könnte hier einen Beitrag leisten. Als Leitlinie für Manager und Projektleiter wurden 25 Schlüsselfaktoren geliefert, die für Manager entscheidend sind, um Souveränitätsanforderungen im Kontext souveräner Clouds mitzudenken.

Die Ergebnisse basieren im Wesentlichen auf öffentlich zugänglichen Architekturen der sieben souveränen Clouds und Experteninterviews mit Cloud-Experten (N=20). Das ist eine Limitation. Zudem berücksichtigen die vorangegangenen Analysen nur eine Reihe von souveränen Cloud-Konzepten zum Zeitpunkt Januar 2025. Diese Angebote können sich in der Zukunft verändern. Forscher können auf den Forschungsergebnissen aufbauen, indem sie in zukünftigen Arbeiten souveräne Architekturen, Prozesse für Nutzer und weiterführende Richtlinien für Manager entwickeln.

Als Nächstes ist es der Plan, die Ergebnisse aus den vorangegangenen Studien in ein Referenzmodell zu überführen.

6

Referenzmodell für die Stärkung digitaler Souveränität in Unternehmen

Eine frühere Version eines Referenzmodells wurde bereits hier veröffentlicht: Klare, M., and Lechner, U. (2024). A Reference Model to Strengthen Digital Sovereignty in Companies. *ICSOB Companion*, 1–9. https://ceur-ws.org/Vol-3921/phd-paper3.pdf

6.1 Einleitung

Aus der Praxisperspektive besteht ein Bedarf nach einer Referenzlösung für digitale Souveränität. Das haben auch die vorangegangenen Ergebnisse aus Abschnitt 4.1 bis 5.4 gezeigt. Ziel dieses Abschnittes ist es nun, eine Referenz für Unternehmen zu finden und dabei folgende Forschungsfrage zu adressieren:

- Wie kann ein Referenzmodell zur Stärkung digitaler Souveränität in Unternehmen aussehen?

Dieses Kapitel ist wie folgt strukturiert: Theoretische Grundlagen (6.2), Forschungsdesign (6.3), Ergebnisse (6.4), Diskussion (6.5), Zusammenfassung, Limitation und Ausblick (6.6).

6.2 Theoretische Grundlagen

6.2.1 Referenzmodellierung

Mittels eines Referenzmodells kann ein Sachverhalt, so wie digitale Souveränität, repräsentativ für wiederholte Anwendungen dargestellt werden (Klare & Lechner, 2024b; Vom Brocke, 2003). Merkmale eines Referenzmodells sind, dass sie in sich konsistent, veröffentlicht und in der wissenschaftlichen Welt akzeptiert sind (Thomas, 2005). Für die Wissenschaft, aber auch die Praxis, ermöglicht die Orientierung an Merkmalen eine Weiterentwicklung des Referenzmodells (Becker & Delfmann, 2013; Becker et al., 2007).

Methodisch kann man zur Gestaltung eines Referenzmodells auf Beobachtungen oder Interviews zurückgreifen (Becker et al., 2002). Mehrere Iterationen aus Datengenerierungen und Datenauswertungen führen zu einem theoretischen Modell (Lindner, 2020). Ziel eines Referenzmodells ist die Anwendbarkeit bzw. Nutzbarkeit (Becker & Delfmann, 2013).

Zur Abgrenzung: Referenzmodelle und Referenzarchitekturen. Referenzmodelle haben ein höheres Abstraktionsniveau als unternehmensinterne Modelle (Fettke & Loos, 2002). Man grenzt Referenzmodelle und Referenzarchitekturen ab, indem man Referenzmodelle als ein Konstrukt aus vielen konzeptionellen Segmenten versteht, während eine Referenzarchitektur einen Systemaufbau visualisiert (Thomas, 2005).

Becker et al. (2002) schlagen folgendes Vorgehen für die Referenzmodellierung vor: (1) Anwendungsdomäne identifizieren, (2) Modellelemente konstruieren, (3) Modell evaluieren, (4) ein geeignetes Referenzmodell aus verschiedenen Referenzmodellen selektieren oder Ergebnisse zu einem Referenzmodell zusammenführen, (5) an den Anwendungskontext anpassen. Wesentliche Literatur zu Referenzmodellierung ist Fettke und Loos (2004), die beschreibt, wie man Referenzmodellierungsforschung in der Wirtschaftsinformatik betreiben kann. Dabei gehen Fettke und Loos (2002) besonders darauf ein, welche Methoden man für die Gestaltung von Referenzmodellen verwenden kann und wie man

eine Wiederverwendbarkeit gewährleistet. Sie empfehlen die Analyse von verschiedenen Kontexten und eine Überprüfung, wo sie in ähnlicher Form auftreten (Fettke & Loos, 2004). Becker und Delfmann (2013) liefert einen Stand zu Wissenschaft und Praxis von Referenzmodellierungen und Vom Brocke (2003) Beispiele zur Gestaltung von Konstruktionsprozessen. Abschließend definieren Schütte (2013) Grundsätze ordnungsgemäßer Referenzmodellierung, als Orientierung für die Konstruktion von anpassungsorientierten Modellen.

6.3 Forschungsdesign

Wie in Abbildung 6.1 dargestellt, besteht das Forschungsdesign für dieses Kapitel aus drei Schritten.

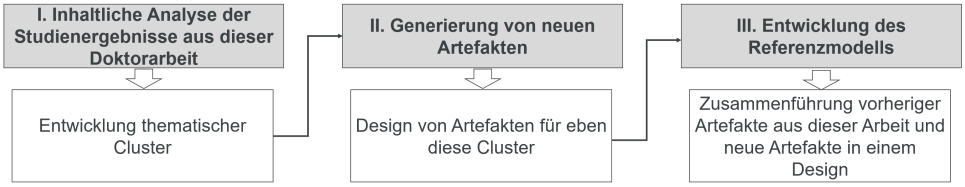


Abbildung 6.1: Forschungsdesign für die Entwicklung des Referenzmodells

Erster Schritt ist eine thematische Analyse der Studienergebnisse aus dieser Arbeit, die sich an den Grundsätzen thematischer Analysen von Clarke und Braun (2017) orientiert. Als Hilfsmittel wird auf SPSS-Software zurückgegriffen, um die Studienergebnisse, die bis jetzt in Kapitel 4 und 5 vorgestellt wurden, mit einer Two-Step-Clusteranalyse zu analysieren. Die kategorialen Variablen werden dabei klassifiziert, indem eine feste Anzahl an Clustern (n=3) vorgegeben wird.

Auf den Erkenntnissen der thematischen Analyse wird im zweiten Forschungsschritt aufgebaut. Es werden neue Oberthemen für die erhobenen thematischen Cluster vorgeschlagen. Zur Herleitung dieser Oberthemen wird *informed argument* genutzt. Das heißt, ein Zusammenspiel verschiedener Argumente hilft dabei, zur Schlussfolgerung zu kommen, warum das gewählte Oberthema gut passt. Hierbei wird kritisch evaluiert, wie andere Referenzmodelle aus anderen Domänen gestaltet sind. Mittels einer Literaturreview ist es schließlich möglich, für den Zweck passende Oberthemen zu identifizieren.

Im dritten Forschungsschritt erfolgt die Entwicklung des Referenzmodells.

Das Design des Referenzmodells basiert auf vier Design-Prozess-Iterationen (vgl. Abbildung 6.2).

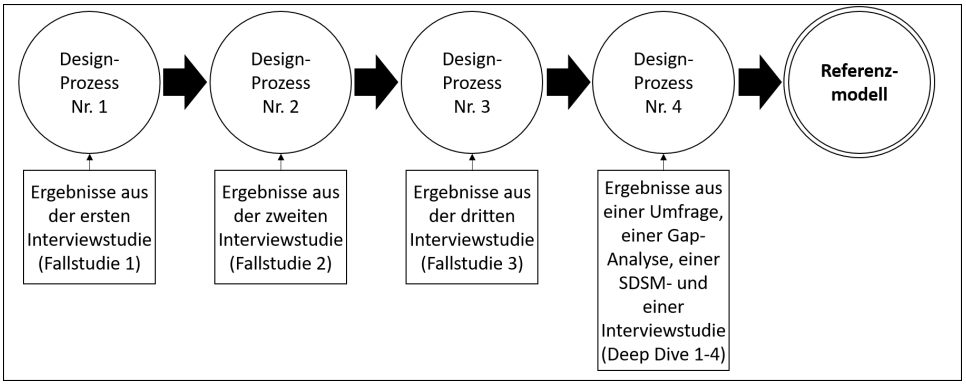


Abbildung 6.2: Design-Prozess für die Entwicklung des Referenzmodells

Die ersten drei Design-Prozess-Iterationen sind bereits in Kapitel 4.1, 4.2 und 4.3 erfolgt: Das DISO-A Modell aus Kapitel 4.3 bildet die Basis für das Design des Referenzmodells. Die Ergebnisse aus der vorangegangenen Umfrage (siehe Kapitel 5.1), der Gap-Analyse (siehe Kapitel 5.2), der Soft Design Science Studie (siehe Kapitel 5.3) und der Interviewstudie (siehe Kapitel 5.4) bilden die Datenbasis für die Analyse und die Basis für das neue Design. All diese Kapitel beschäftigten sich mit der Frage, wie digitale Souveränität umgesetzt werden soll. Da sich die Modelle DISO-C, DISO-L und DISO-A stark auf die Frage bezogen, was digitale Souveränität in dieser Arbeit meint, wird dieses Kapitel einen stärkeren Fokus darauf legen, kritisch zu reflektieren, welche Studienergebnisse Unternehmen dabei helfen können, mehr digitale Souveränität zu erreichen und wie man dies in einem Referenzmodell abbilden kann.

Das Design der Cluster erfolgt in Anlehnung an Hevner et al. (2004). So rückt die Design Science Research Methodologie ins Licht (vgl. Abbildung 6.3). Für die Erstellung eines Paradigmas für diesen Zweck leistet die Design Science Research nach Hevner (2004) einen passenden Rahmen, weil Design Science Research von einem Problem ausgeht, das anwendungsorientiert begründet ist, so wie digitale Souveränität. Basierend auf diesem Problem wird ein Artefakt als Problemlösung geschaffen (Hevner & Chatterjee, 2010). Es wird in der realen Welt analysiert, um dann zu verstehen, was diese Lösung bewirkt (Hevner et al., 2004). Dieses Verständnis kann mittels eines Design-

Prozesses unterstützt werden. Trägt die Kreation eines Artefakts zur Lösung eines Problems bei, so handelt es sich nach Hevner und Chatterjee (2010) schließlich um Design Science Research. Um ein gutes Artefakt zu erhalten, erfolgt eine Einbindung von Praxis – mittels vorangegangener Interviews und der Einbindung von Projektergebnissen; sowie Theorie – mittels bereits durchgeführter und neuer Literaturreviews.

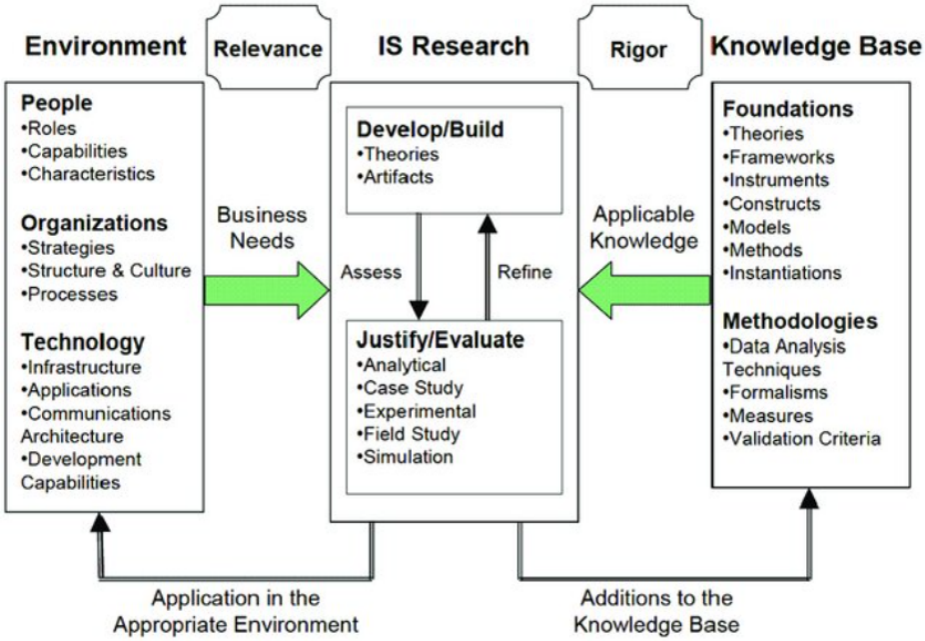


Abbildung 6.3: Design Science Research Methode (Hevner et al., 2004) als methodischer Rahmen für die Entwicklung des Referenzmodells

Der dritte Forschungsschritt ist die Entwicklung des Referenzmodells. Als Orientierung für diesen Forschungsschritt dienen Fettke und Loos (2002) und Fettke und Loos (2004). Wenn das Referenzmodell entwickelt wird, wird besonders auf die Grundsätze Nutzbarkeit und Einfachheit geachtet (Fettke & Loos, 2002, 2004). Damit ist nicht die Vollständigkeit des Referenzmodells das Ziel, sondern vielmehr die Ergebnisse aus den vorangegangenen Kapiteln zu abstrahieren und in ein Modell zu integrieren.

6.4 Ergebnisse

6.4.1 Inhaltliche Analyse der Studienergebnisse aus dieser Arbeit

Herausforderungen, das DISO-A-Modell zu verwenden Die Modellierung von Clustern digitaler Souveränität erfolgte in Kapitel 4.3. Ziel des DISO-A-Modells war es, zu beantworten, was digitale Souveränität umfasst (vgl. Abbildung 6.4).

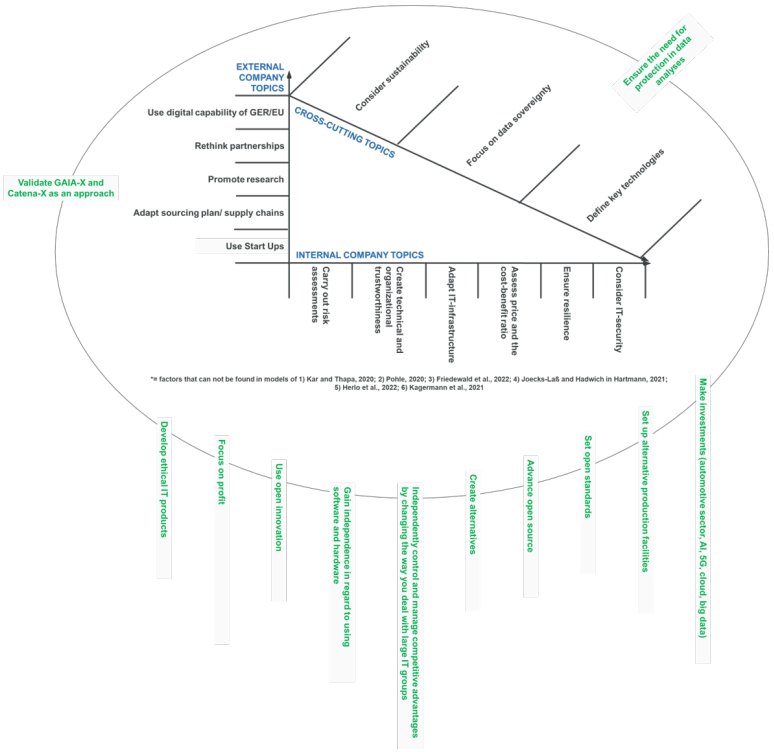


Abbildung 6.4: Ausgangspunkt DISO-A: Digitale Souveränitätsmodell-Optimierung Academia (3. Version)

Es scheint jedoch herausfordernd, das DISO-A-Modell zu verwenden, um zu beantworten, wie man digitale Souveränität erreichen kann. Bei genauerer Betrachtung der Cluster aus Abbildung 6.4 stellt man fest, dass einige Cluster zwar auch als Empfehlung verstanden werden können, wie man digitale Souveränität erreichen kann, dies aber nicht flächendeckend für alle Cluster gilt. Ein Beispiel: Partnerschaften überdenken zu müssen, kann ein wesentlicher Pfeiler sein, um zu beschreiben, was digitale Souveränität meint. Es kann aber

auch eine Handlungsempfehlung sein, wie man digitale Souveränität erreicht.

Eine starre Abbildung wie diese hier, die lediglich aufzeigt, welcher Dimension (intern, extern) ein Cluster zugeordnet wurde, scheint nicht mehr passend, um zu beantworten, wie man digitale Souveränität erreichen kann. Es braucht eine dynamischere Abbildung, die die Zusammenhänge zwischen den Clustern beschreibt.

Neues Clustering und Zusammenhänge der Cluster mit Ausrichtung auf Forschungsfrage Unter Prüfung, welche Cluster einen Aufschluss darüber geben, wie man digitale Souveränität erreichen kann, wurde das DISO-A-Modell kritisch reflektiert und neue Cluster gebildet (vgl. Abbildung 6.5).

Hierzu werden diejenigen Cluster eliminiert, die keinen Aufschluss darüber geben, wie man digitale Souveränität erreichen kann. Ähnliche Cluster werden zusammengefasst und zwei Einflussfaktoren herausgearbeitet: das ist die *Entwicklung einer Strategie* und das *Kontrollieren und Management von Maßnahmen digitaler Souveränität*. Diese beiden Einflussfaktoren unterliegen einer zeitlichen Abfolge. Während die Entwicklung einer Strategie ein Planungsschritt ist, ist das Managen der Maßnahmen als Umsetzungsschritt zu verstehen und folgt damit in zeitlicher Abfolge nach der Strategieentwicklung. Die Planung und Umsetzung sollten einer ständigen Validierung unterliegen.

Im Rahmen der Strategieentwicklung ist es, den Daten dieser Arbeit nach, sinnvoll zu prüfen, welche digitalen Alternativen es in Deutschland bzw. der EU gibt. Außerdem sollte eine Risikoabwägung vorgenommen werden, um zu entscheiden, wo Anpassungen notwendig sind (z.B. Infrastruktur, Software, etc.). Die Umsetzung der Maßnahmen sollte vor dem Hintergund einer Kosten-Nutzen-Abwägung erfolgen. Maßnahmen sollten eingepreist werden und vor dem Hintergrund des Gewinns des Unternehmens bewertet werden.

Das Unternehmen sollte dann nach eigenem Ermessen entscheiden, welche Stoßrichtung es wählen will. Auf Basis der Daten dieser Arbeit empfiehlt es sich, mehr Unabhängigkeit bei der Nutzung von Software und Hardware zu erlangen (souveräne Entwicklung von IT-Produkten), den Fokus auf mehr Datenhoheit zu legen (Sicherstellung des Schutzbedarfs bei Datenanalysen) und Investitionen in IT-Sicherheit (und gegebenenfalls auch z. B. in KI, 5G, Cloud und Big Data) vorzunehmen.

Abbildung 6.5: Zusammenhänge zwischen den Clustern aus dem DISO-A-Modell

Analyseergebnisse und Artefaktentwicklung Nun werden wichtige Ergebnisse aus den vorangegangenen Studien analysiert. Hierzu wurden die Studieninhalte aufgelistet und die Themen einem Cluster aus dem DISO-A-Modell zugeordnet (vgl. Tabelle 17 bis 24 im Anhang).

Aus den Studienergebnissen lassen sich N=2 wesentliche Schlüsseltechnologien für die Stärkung von Datensouveränität in Unternehmen herleiten: künstliche Intelligenz und Blockchain. Zudem liefern die Daten N=8 Maßnahmen (einen Maßnahmenkatalog) zur Stärkung digitaler Souveränität mit den Schlüsseltechnologien KI und Blockchain.

N=38 Risiken für die Stärkung digitaler Souveränität mit Hilfe von Open Source in Softwareentwicklungsprojekten sind ebenfalls dargestellt worden. Daraus ließen sich N=15 Affordanzen aus den Open Source-Projekten ableiten und N=5 Anpassungsvorschläge für diese Affordanzen zur Einbettung digitaler Souveränität in Softwareentwicklungsprojekten.

Weiter folgen N=4 Cluster und N=10 Zusammenhänge zwischen den Clustern, die wesentlich sind für die Einführung digitaler Souveränität im Softwarelebenszyklus von Unternehmen. Zusammen mit N=13 Prozessen und N=4 Prozessgruppen für eine souveränere Softwareeinführung können diese Prozesse und Prozessgruppen als Orientierung für Unternehmen dienen.

Um digitale Souveränitätsanforderungen im Rahmen eines passenden souveränen Cloudkonzepts zu berücksichtigen, stellen N=1 Prozess aus Nutzer-Perspektive, N=9 Faktoren aus IT-Architektur-Perspektive und schließlich N=25 Faktoren für Manager eine Entscheidungsunterstützung dar.

Kumuliert sind das N=96 Ergebnisse, die in das Referenzmodell einfließen.

Wie in Abbildung 6.6 dargestellt, werden die Cluster den folgenden Oberthemen zugeordnet: *Ermöglicher*, *Prozesse* und *Risiken*.

Reflexion vor dem Hintergrund von Literatur Ermöglicher sind Schlüsselkomponenten mit wesentlichem Einfluss auf das Erreichen der digitalen Souveränität von Unternehmen beziehungsweise kritischer Erfolgsfaktoren hinsichtlich der definierten Ziele. Auch andere Referenzmodelle verweisen auf die Bedeutung von Ermöglichern als Leitplanke für Unternehmen. Ermöglicher finden sich so beispielsweise auch in dem EFQM-Excellence Model von Rentrop (2024) oder dem strategischen Rahmenwerk von Dous (2007) wieder.

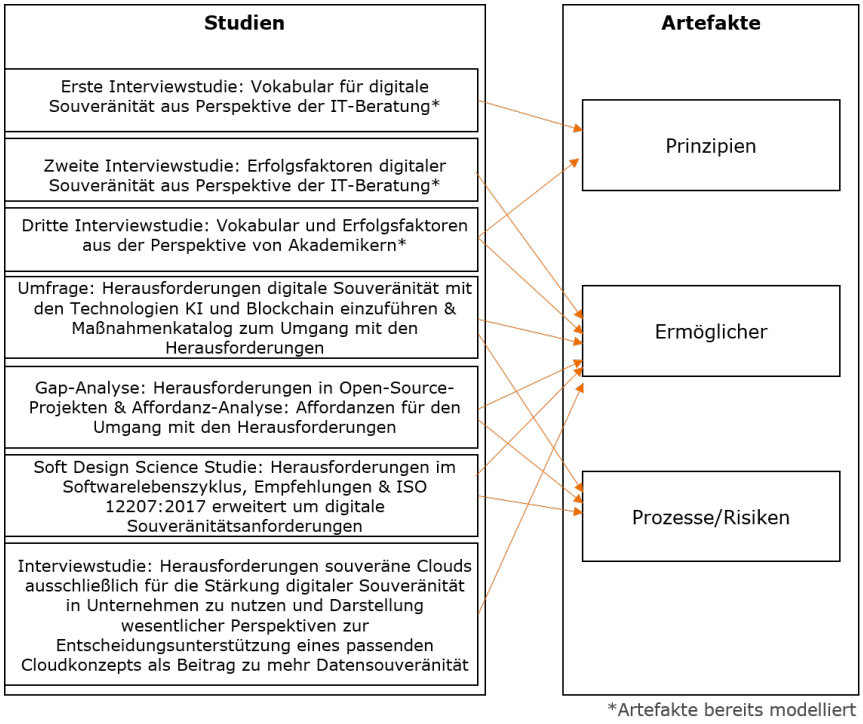


Abbildung 6.6: Zuordnung der Studienergebnissen zu den Artefakten

Für das Referenzmodell sind Schlüsseltechnologien als wesentlicher Treiber zu sehen, wie man digitale Souveränität in Unternehmen stärken kann.

Prozesse dienen als Richtlinien für Unternehmen, wie sie digitale Souveränität bei sich im Unternehmen einführen können. Prozessdefinitionen sind bei verschiedenen Frameworks Bestandteil, so bei Frameworks für Veränderungsmanagement (Price & Chahal, 2006), Unternehmensumstrukturierungen (Umar, 2023) oder Risikomanagement (Lai, 2011). Für das Referenzmodell sind Prozesse wesentliche Leitlinien für Unternehmen und bieten damit einen roten Faden, wie eine Einführung von digitaler Souveränität gelingen kann.

Risiken lassen sich am besten als fundamentale Faktoren verstehen, die einen Vorrang haben, weil sie das Erreichen digitaler Souveränität fundamental erschweren können. Ein Blick auf die Literatur zeigt, dass Risiken auch in anderen Frameworks eine Rolle spielen: so zum Beispiel bei COBIT (Rentrop, 2024). Auf Basis unserer Datenlage ist es notwendig, einige Risiken im Kontext digitaler Souveränität zu berücksichtigen, da diese einer erfolgreichen

Einführung digitaler Souveränität in Unternehmen im Wege stehen könnten.

Alle Oberthemen (Ermöglicher, Prozesse und Risiken) dienen den Unternehmen damit als Leitfaden, wie sie digitale Souveränität umsetzen können. Die ersten drei Fallstudien (siehe Kapitel 4: Faktoren digitaler Souveränität aus Perspektive der IT-Beratung (Friedensfall), Faktoren digitaler Souveränität aus Perspektive der IT-Beratung (Landesverteidigungsfall), Faktoren digitaler Souveränität aus Perspektive von INF-, WINF-, und BWL-Professoren) leisten einen Beitrag zu einem besseren Begriffsverständnis digitaler Souveränität und zeigen auf, wie digitale Souveränität verstanden werden kann. Schlüsseltechnologien wie KI und Blockchain können ein wesentlicher Ermöglicher für mehr Datensouveränität sein. Die Affordanztheorie ist hilfreich, um sich souveränerer Softwareentwicklung auf Basis von Open Source zu nähern. Die Affordanzen aus Projekten müssen jedoch angepasst werden, damit dies gelingt. Insbesondere Kosten und Komplexität hindern Unternehmen bei der Gestaltung souveränerer Softwareeinführung. Die ISO 12207:2017-Prozess-Erweiterung kann helfen, sich einer souveräneren Softwareeinführung zu nähern. Souveräne Clouds gelten zwar als Ermöglicher digitaler Souveränität, analysierte Konzepte leisten aber eher einen Beitrag für mehr Datensouveränität. Bestimmte Faktoren für Manager können dennoch dabei helfen, das passendste Konzept je nach Souveränitätsanforderung zu finden. Dies sollte jedoch unter Berücksichtigung der IT-Architektur und der entsprechenden Nutzer-Perspektive erfolgen.

6.4.2 Entwicklung des DISO!-Modells

Schließlich visualisiert Abbildung 6.7 das Referenzmodell zur Stärkung digitaler Souveränität in Unternehmen.

Der innere Bereich des Referenzmodells widmet sich der Frage, was digitale Souveränität ist. Das äußere Dreieck wiederum geht darauf ein, welche Oberthemen Unternehmen Orientierung bieten können, um mehr digitale Souveränität zu erreichen. Aus Abbildung 6.6 ging hervor, welche der N=96 Studienergebnisse sich hinter welchem Artefakt verbinden: 25,6% der Ergebnisse hinter Cluster 1: Ermöglicher (zum Beispiel Schlüsseltechnologien), 25,6% der Ergebnisse hinter Cluster 2: Prozesse (zum Beispiel für souveräne Softwareeinführung die ISO/IEC/IEEE 12207:2017-Erweiterung) und 48,8%

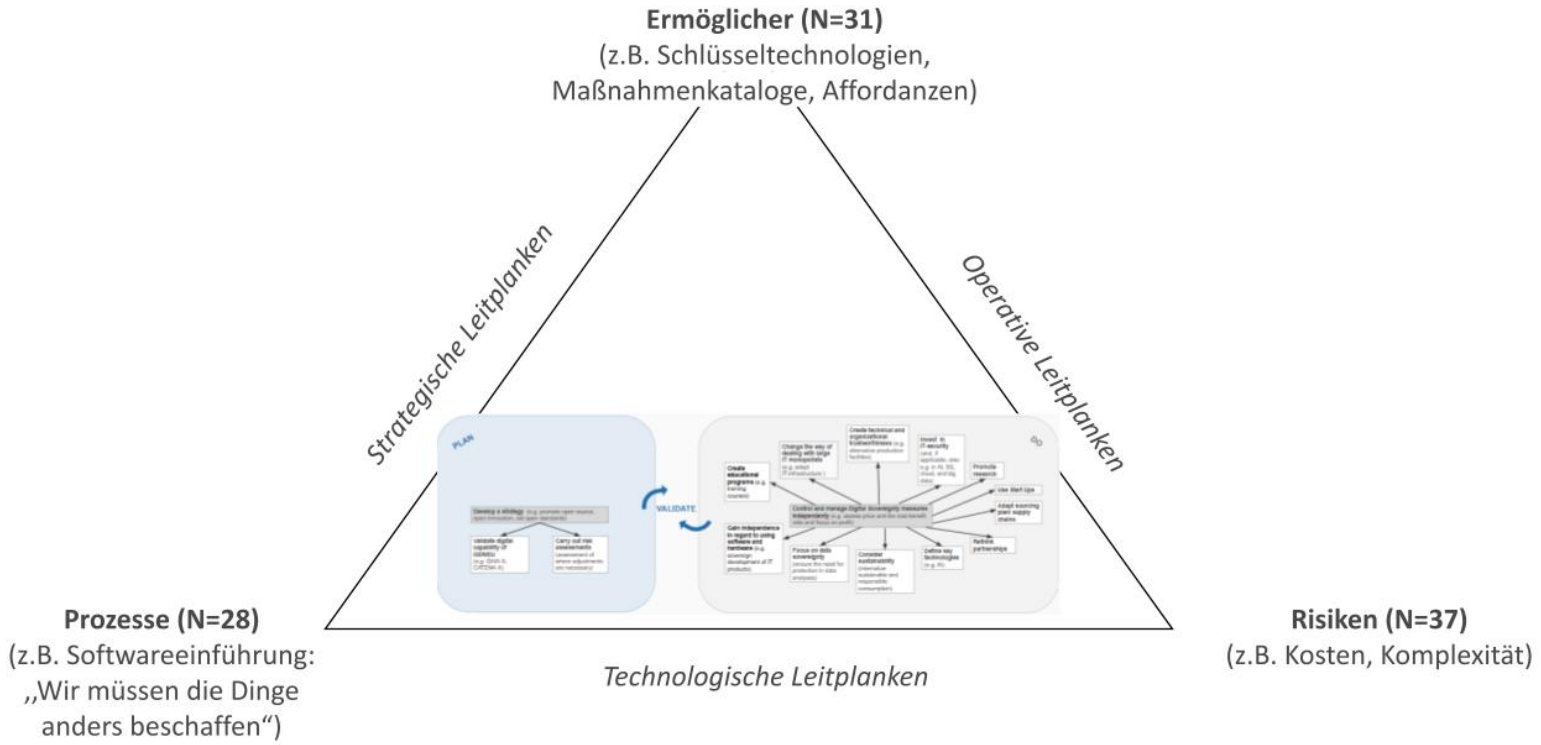


Abbildung 6.7: DISO!: Digitale Souveränitätsoptimierung - ein Referenzmodell

der Ergebnisse hinter Cluster 3: Risiken (zum Beispiel Komplexität, Kosten oder Sicherheitsrisiken in Softwareentwicklungsprojekten).

Digitale Souveränität für Unternehmen erfolgt auf strategischer, technologischer, organisationaler sowie auf operativer Ebene. Dies erfordert Leitplanken auf ebendiesen Ebenen, die das DISO!-Modell enthält.

Strategische Leitplanken. Das DISO!-Modell zeigt, dass es notwendig ist, ein Zielsystem für digitale Souveränität zu entwickeln. Neben einer Strategie für das Partnermanagement und das Thema Cloud ist es auch sinnvoll, Governance-Strukturen einzuführen (vgl. Kapitel 5.1.4). Governance-Strukturen sind für Unternehmen im Kontext digitaler Souveränität essenziell, weil sie den strategischen, organisatorischen und operativen Rahmen schaffen, um digitale Selbstbestimmung effektiv umzusetzen und aufrechtzuerhalten. Governance hilft, strategische Abhängigkeiten (z.B. von Hyperscalern wie Amazon oder Microsoft) frühzeitig zu erkennen, zu bewerten und zu steuern. Digitale Souveränität umfasst auch Datensouveränität. Governance-Strukturen regeln, wer Zugriff auf Daten hat, wo Daten gespeichert werden und wie sie verarbeitet oder geteilt werden. Governance ist notwendig, um IT-Sicherheit, Datenschutz, Audits und Umgangsregeln systematisch im Unternehmen zu verankern. Dies hilft bei der Ausrichtung auf strategische Souveränitätsziele. Im Vergleich zu Pohle (2020) zeigt sich in dieser Arbeit die Notwendigkeit von Governance-Strukturen für die Umsetzung strategischer Leitplanken für Unternehmen. Roberts et al. (2021) unterstreicht zwar die Bedeutung globaler Governance und Pohle und Santaniello (2024) Internet-Governance, doch die Notwendigkeit unternehmerischer Governance führt das DISO!-Modell neu in die Debatte rund um digitale Souveränität ein.

Technologische Leitplanken. Hier zeigt das DISO!-Modell, dass der Einsatz von Open Source sinnvoll für die Stärkung digitaler Souveränität ist. Aber auch Themen wie IT-Architekturen spielen eine wesentliche Rolle, wenn es an die Prüfung unternehmensinterner Instrukturen geht. Es gilt jedoch strategische, personelle Risiken, Sicherheitsrisiken und Lock-In-Effekte zu berücksichtigen (vgl. Kapitel 5.2). Es sind digitale Fähigkeiten im Kontext digitaler Souveränität einzuführen und Kosten für eine Umgestaltung auf souveräne Softwareeinführung abzuwägen (vgl. Kapitel 5.3). Standards können dabei hel-

fen, die Unabhängigkeit, Kontrolle und Handlungsfähigkeit von Unternehmen zu fördern, indem sie Interoperabilität schaffen und verhindern, dass Organisationen an einzelne Anbieter (z.B. Microsoft, Amazon, Google) gebunden sind. Offene Standards und Protokolle ermöglichen es, die Funktionsweise von Systemen nachzuvollziehen, was zentral für die Themen Vertrauen und Kontrolle ist. Standards, z.B. ISO/IEC-Normen oder europäische Standards, erleichtern die Einhaltung von gesetzlichen und regulatorischen Vorgaben (z.B. DSGVO, NIS2, Cyber Resilience Act). Ohne standardisierte Schnittstellen, Protokolle und Prozesse lassen sich souveräne Cloud-Infrastrukturen, datenhoheitliche Lösungen oder eigene KI-Plattformen kaum realisieren. Unsere Ergebnisse bestätigen die von Pohle (2020) und Bauer und Erixon (2020). Sie zeigen, dass technologische Leitplanken notwendig sind, um digitale Souveränität zu stärken.

Organisationale Leitplanken. Klare Zuständigkeiten und Entscheidungsstrukturen, Rollen und Verantwortlichkeiten für das Thema digitale Souveränität sind wesentlich, um Veränderungen in Unternehmen zu etablieren. Aus dem DISO!-Modell geht hervor, dass digitale Souveränität ein Transformationsversuch ist. Ein Unternehmen muss damit seine Strukturen und Kultur grundlegend neu gestalten, um sich an die veränderten Souveränitätsziele und die veränderten Marktbedingungen anzupassen. Ein Veränderungsmanagement hilft bei der Planung und Umsetzung dieses Wandels und stellt sicher, dass die Betroffenen bei der Transformation mitgenommen werden. Awareness-Kampagnen können zudem eingesetzt werden, um das Bewusstsein für diese Art der Veränderung zu schärfen und Mitarbeiter zu motivieren, sich aktiv an der Transformation zu beteiligen. Der Einsatz eines Veränderungsmanagements im Kontext digitaler Souveränität für Unternehmen weist auf einen Zusammenhang hin, der in der bisherigen Fachliteratur zu digitaler Souveränität nicht diskutiert wird.

Operative Leitplanken. Die Auswahl von Tools und Affordanzen beeinflusst den Erfolg der Transformation (vgl. Kapitel 5.2). Monitoring von Abhängigkeiten und die Generierung von Notfallplänen sind je nach Höhe des Risikos grundlegend. Zudem kann ein SLA-(Service Level Agreement) Management sinnvoll sein. Ein SLA-Management ist im Kontext digitaler Souveränität besonders sinnvoll, weil es Unternehmen hilft, Kontrolle, Transparenz und

Sicherheit über ausgelagerte digitale Dienste und Infrastrukturen zu behalten. So hilft dies, Risiken wie Systemausfälle, Datenverlust, Nichtverfügbarkeit von Services oder mangelnde Support-Reaktionszeiten zu erkennen und Vertragsstrafen oder Eskalationsprozesse abzusichern. Wer eigene Anforderungen formulieren und messen kann, hat mehr Verhandlungsspielraum mit Anbietern. Die Idee einer Verknüpfung von SLA-Management und digitaler Souveränität ist auch bei Bokolo (2025) und Esposito et al. (2018) wiederzufinden, hier aber eher im Sinne von Datensouveränität mit einem stark technologischen Ansatz.

6.5 Diskussion

Nutzen des DISO!-Modells: *Wofür wurde das Referenzmodell entwickelt? Kann es für diesen Zweck genutzt werden?*

Das Referenzmodell bietet einen konkreten, praktischen Handlungsrahmen, der Unternehmen befähigt, digitale Souveränität gezielt zu fördern. Es bietet Orientierungshilfe, Entscheidungsunterstützung, Planungsgrundlage und einen Best-Practice-Transfer.

Orientierungshilfe bietet das DISO!-Modell, weil es komplexe Themen wie Datensouveränität, IT-Sicherheit, Cloud-Strategien und Open Source strukturiert. Es hilft dabei, technologische, organisatorische und rechtliche Anforderungen zu erkennen und abzuwägen. Insbesondere durch die Inklusion der Risiken im DISO!-Modell ist eine Entscheidungsunterstützung vorhanden. Unternehmen können aus dem DISO!-Modell strategische Maßnahmen ableiten, z.B. für die Wahl ihrer Cloud-Lösung, der Entscheidung für IT-Investitionen und der Wahl von sicheren, souveränen Partnerschaften. Das schafft Planungsgrundlagen. Und letztlich ist durch die Inklusion von Best-Practice-Ansätzen der IT-Beratung das Lernen aus strukturierten Erfahrungswerten für Unternehmen möglich.

Das Referenzmodell kann von IT-Beratern als Rahmenwerk zur Steuerung und dem Management von digitaler Souveränität genutzt werden. Zusätzlich können auch Unternehmer das Referenzmodell nutzen, um eine Referenz dafür zu erhalten, was digitale Souveränität umfassen kann und wie man sie erreichen kann. Es ist empfehlenswert, selbstständig zu entscheiden, auf welche Faktoren sich Unternehmen stärker beziehen wollen.

Relevanz des DISO!-Modells: *Warum ist das relevant für Unternehmen?*

Das Referenzmodell ist relevant, weil es aktuelle Herausforderungen im Kontext digitaler Souveränität adressiert, z.B.: Wachsende Abhängigkeit von Tech-Giganten, Datenschutz und IT-Compliance (DSGVO, NIS2, etc.), nationale und europäische Strategien zu digitaler Souveränität (z.B. GAIA-X, EU-Digitalstrategie) und Technologietrends wie Cloud, KI, Blockchain, Open Source – verbunden mit Souveränitätsfragen. Zudem ist das Referenzmodell anschlussfähig, weil es Bezüge zu etablierten Modellen herstellt (z.B. ISO 12207, COBIT, Design Science Frameworks) und nicht nur politisch-normativ, sondern unternehmenspraktisch verwertbar ist. Damit ist das Referenzmodell nicht nur wissenschaftlich fundiert, sondern auch wirtschaftlich anschlussfähig.

Das Referenzmodell leistet einen Beitrag zu einem auf empirischer Forschung und Modellierung basierenden Begriffsverständnis für digitale Souveränität und bietet damit den Nutzenden eine vokabulare Unterstützung. Es bietet aber auch Leitlinien, wie Unternehmen digitale Souveränität umsetzen können. Hinter drei Clustern *Ermöglicher*, *Prozesse* und *Risiken* verstecken sich eine Vielzahl von Empfehlungen für Schlüsseltechnologien und Affordanz-Anpassungen, von Prozessempfehlungen für souveränere Lieferketten bis hin zu Faktoren und Perspektiven, die bei der Entscheidung zu einem passenden souveränen Cloud-Konzept helfen können.

Gültigkeit des DISO!-Modells: *Was wurde wie verallgemeinert?*

Die Studienergebnisse aus den Kapiteln 4.1 bis 5.4 dieser Arbeit wurden in diesem Kapitel verallgemeinert. Es konnte gezeigt werden, dass das Modell vier verschiedenen Betrachtungsweisen standhält: Das Referenzmodell ist valide und übertragbar, weil es empirisch fundiert ist (z.B. basiert es auf Interviews, Fallstudien und Literaturreviews). Es ist klar definiert und logisch konsistent. Es ist auch validierbar – etwa durch Fallstudien oder Experteninterviews. Das Referenzmodell ist skalierbar und anpassbar, je nach Branche, Unternehmensgröße und Grad der Souveränität. Hinter der Verallgemeinerung der Ergebnisse verbirgt sich eine Vielzahl an Reflexionsprozessen auf Konferenzen, Fachveranstaltungen und Diskussionen mit Forschungsgruppen.

6.6 Zusammenfassung, Limitation und Ausblick

Das hier vorliegende DISO!-Modell leistet einen Beitrag, indem es Leitlinien für Unternehmen bietet, die ihre digitale Souveränität stärken wollen. In dieser Arbeit sind drei Artefakte für die Stärkung digitaler Souveränität vorgeschlagen worden: Ermöglicher, Prozesse und Risiken. Zudem inkludiert das DISO!-Modell ein besseres Begriffsverständnis von digitaler Souveränität, mit dem die Brücke zwischen politischen Forderungen zur Umsetzung mit IT-Technologien geschlagen werden kann. Methodisch sind die Ergebnisse auf Interviews mit IT-Beratern und Professoren sowie Literaturreviews von 2014 bis 2025 zu digitaler Souveränität zurückzuführen. Die Ergebnisse weiterer Studien (zwei Interviewstudien, einer Umfrage, einer Gap-Analyse und einer Soft Design Science Studie) zeigen auf, was Unternehmen tun können, um ihre digitale Souveränität zu stärken.

Zusammenfassend lässt sich festhalten, dass das DISO!-Modell Ermöglicher liefert, die für Unternehmen als fundamentale Grundlagen dienen können, um sich dem Thema digitale Souveränität zu nähern. Ein Beispiel für Ermöglicher sind Schlüsseltechnologien. KI und Blockchain können einen Beitrag zu mehr Datensouveränität leisten, wenn man Federated Learning als Ansatz des maschinellen Lernens wählt. Zudem sind Prozesse und Risiken im DISO!-Modell inkludiert worden. Die Ergebnisse weisen darauf hin, dass erst aus einer Mischung von passenden Schlüsseltechnologien, Maßnahmen, einer Anpassung der IT-Architektur und einer Nutzereinbindung sowie durch ein entsprechendes Management, eine Stärkung digitaler Souveränität in Unternehmen erreicht werden kann. Eine konkrete Empfehlung an Unternehmen ist die Orientierung an standardisierenden, grundlegenden, kontrollierenden, organisatorischen, sensibilisierenden und integrierenden Affordanzen. Schlussendlich bietet das Modell 28 Prozesse und 37 Risiken. Diese sind Richtlinien für Unternehmen, wie sie digitale Souveränität bei sich im Unternehmen einführen können und sind als Leitfaden zu verstehen, auf was Unternehmen achten sollten, wenn sie digitale Souveränität einführen. Konkrete Beispiele für Risiken sind fehlende digitale Fähigkeiten und hohe Kosten bei der Softwareeinführung oder potenzielle Sicherheitslücken und Ressourcenengpässe zur Prüfung von Quellcode bei der Softwareentwicklung. Prozesse aus der Erweiterung von

ISO/IEC/IEEE 12207:2017 bieten Möglichkeiten des Umgangs.

Die Ergebnisse dieses Kapitels leisten einen Beitrag zu digitaler Souveränität durch Design-Science-Forschung, indem ein Artefakt entwickelt wurde, das auf empirischen sowie theoretischen Ergebnissen zu digitaler Souveränität basiert.

Eine Limitation des Referenzmodells ist, dass es keiner Vollständigkeit unterliegt. Einerseits begrenzt sich das Modell auf die Perspektive der IT-Beratung und Professoren aus den Bereichen INF, WINF, BWL. Andererseits basieren die Artefakte Ermöglicher, Prozesse und Risiken grundsätzlich nur auf den Forschungsergebnissen dieser Arbeit. Das ist eine Limitation. Digitale Souveränität in Verbindung mit anderen Technologien (z.B. Quantum Computing) und anderen Konzepten als Federated Learning zu untersuchen, sind weitere, über diese Arbeit hinausgehende Forschungsfelder. Diese Möglichkeiten sind nicht weiter in dieser Studie untersucht worden und stellen demnach eine weitere Limitation dar.

Es ist empfehlenswert für Forschende, auf den Ergebnissen dieses Referenzmodells aufzubauen. So wäre es sinnvoll, als nächstes zu evaluieren, ob das Modell tatsächlich praktische Anwendung in der realen Welt finden kann. An dieser Stelle soll die Verschriftlichung der Dissertationsschrift ein Ende finden. Über diese Arbeit hinaus ist es ein persönliches Anliegen, die Ergebnisse rund um die Affordanztheorie zu erweitern, um besser zu verstehen, ob Affordanzen als Konstrukt dabei helfen können, digitale Souveränität voranzutreiben.

7

Fazit, Zusammenfassung, Limitationen, Ausblick

Diese Dissertation ist ein Beitrag zum laufenden Diskurs über digitale Souveränität, denn Kapitel 6 zeigt ein Referenzmodell mit einem konkreten Verständnis darüber, was digitale Souveränität in dieser Arbeit meint und liefert konkrete Handlungsempfehlungen auf Basis von Risiken, Ermöglichern und Prozessen.

Die vorliegende Dissertation leistet damit drei wesentliche Beiträge: Erstens, ein besseres Verständnis für digitale Souveränität. Zweitens, praktische Ansätze, wie digitale Souveränität gesteigert werden kann. Drittens, ein übersichtliches Referenzmodell für Unternehmen, das als Leitplanke genutzt werden kann.

Als Ergebnisse präsentiert diese Dissertation:

- das DISO-A-Modell (Digital Sovereignty Model from the Perspective of IT Consultancy and Academia), das wichtige Cluster digitaler Souveränität aufzeigt.
- Einen Maßnahmenkatalog für die Stärkung digitaler Souveränität mit

KI und Blockchain, sowie Implikationen, wie Blockchain und Federated Learning bei der Umsetzung von KI zu mehr Datensouveränität beitragen können.

- Eine Übersicht über standardisierende, grundlegende, kontrollierende, organisatorische, sensibilisierende und integrierende Affordanzen und wie man sie anpassen sollte, um souveräne Softwareentwicklung zu fördern.
- Eine ISO-Erweiterung für das Management von Software-, und Hardware-Lieferketten in Unternehmen, die Unternehmern eine Übersicht an Prozessgruppen und Prozessen bietet, um den Softwarelebenszyklusprozess souveräner zu gestalten.
- Praktische Management-, Architektur-, und Userperspektiven zur Unterstützung von Unternehmensentscheidungen hinsichtlich eines passenden souveränen Cloudkonzepts unter Berücksichtigung unterschiedlicher Souveränitätsanforderungen in Unternehmen.
- Und schließlich, das DISO!-Modell zur Stärkung digitaler Souveränität in Unternehmen, um das strategische Thema der digitalen Souveränität anzugehen. Es ist ein Rahmenwerk, das eine Reihe von Forschungsergebnissen inkludiert und abstrahiert. Diese Dissertation unterbreitet damit sowohl praktikable als auch theoretische Ansätze zum Umgang mit digitaler Souveränität.

Limitationen dieser Arbeit sind einerseits, dass die durchgeführten Interviews im Wesentlichen auf der Meinung von IT-Beratern, Professoren, Entwicklern und Cloud-Experten basieren. Die Literatur, die genutzt wurde, um das Verständnis abzugleichen bzw. zu erweitern, ist eine Teilmenge der Literatur, die in dem Themenkomplex (Stand: 2025) existiert. Die systematische Literaturrecherche beginnt im Jahr 2014. Weitere empirische Daten können die Ergebnisse anreichern. Zudem ist das entwickelte DISO!-Modell nicht frei von Zielkonflikten, die teilweise nicht auflösbar sind. Unternehmen müssen demnach je nach Situation entscheiden, welche der ermittelten Faktoren für sie größere Bedeutung hat. Die Handlungsempfehlungen, wie man digitale Souveränität erreichen kann, sind darauf ausgerichtet, einen Beitrag zur Unternehmensebene zu

leisten, dabei aber insbesondere technologische Aspekte, Prozesse und Aspekte auf Projektebene in den Fokus zu nehmen. Betrachtet man Schlüsseltechnologien (wie KI und Blockchain), die Softwareentwicklung, die Lieferketten, die IT-Infrastruktur-Modelle (insbesondere souveräne Clouds), dann ist das nur ein Anteil an Bereichen, in denen digitale Souveränität für Unternehmen eine Rolle spielen kann. Schließlich wird das Referenzmodell auf Basis verschiedener Design-Iterationen entwickelt. Das heißt, das DISO!-Modell hat die Limitation, auf eine sehr spezifische Perspektive digitaler Souveränität begrenzt zu sein. Dennoch kann als Argumentation angeführt werden, dass ein nützliches Artefakt erzielt wurde, da die Einbindung von Praxis als auch Theorie eine wesentliche Rolle in dieser Dissertationsschrift spielt. Ein Zusammenspiel aus Interviews, Umfragen und systematischen Literaturrecherchen oder auch Literaturrecherchen mit dem Schneeballsystem unterstreichen dies. Die Evaluation des Modells mit IT-Beratern liefert einen Hinweis darauf, dass IT-Berater das Modell als hilfreich ansehen. Es ist deutlich geworden, dass 94% der Befragten das Verständnis digitaler Souveränität als bedarfsgerecht ansehen, um Unternehmen hinsichtlich digitaler Souveränität zu beraten. Dies ist ein vielversprechendes Ergebnis. Auch die Evaluation vor dem Hintergrund von praxisnaher Literatur lieferte das Ergebnis, dass sich alle Prozessbestandteile der ISO-Erweiterung in den Ausführungen praxisnaher Literatur wiederfinden lassen. Das kann als Referenz dafür gesehen werden, dass das entwickelte Artefakt einen sinnstiftenden Beitrag für den Umgang mit digitaler Souveränität liefert.

Für Anwender dieses Modells in Forschung und Praxis ist es empfehlenswert, einen Evaluationsprozess anzuschließen. Zudem kann das Referenzmodell um weitere Prozesse und Governance-Ansätze erweitert werden, mit dem Ziel, ein Rahmenwerk zu erhalten, das sich mit Anwendung in der Praxis und Weiterentwicklung zu einem anerkannten Modell entwickelt.

Literatur

Abrahamsson, P., Salo, O., Ronkainen, J., & Warsta, J. (2017). Agile software development methods: Review and analysis. *arXiv preprint arXiv:1709.08439*.

Adler-Nissen, R., & Eggeling, K. A. (2024). The discursive struggle for digital sovereignty: Security, economy, rights and the cloud project Gaia-X. *JCMS: Journal of Common Market Studies*, *62*(4), 993–1011.

Aksoy, C. G., Baur, A., Flach, L., & Javorcik, B. (2022). Wie reagieren Unternehmen auf Lieferkettenstörungen?-Ergebnisse einer Unternehmensbefragung. *ifo Schnelldienst digital*, *3*(7), 01–05.

Akter, S., Michael, K., Uddin, M. R., McCarthy, G., & Rahman, M. (2020). Transforming business using digital innovations: The application of AI, blockchain, cloud and data analytics. *Annals of Operations Research*, *308*, 7–39. https://doi.org/10.1007/s10479-020-03620-w

Andenmatten, M. (2023). Digitale Cloud und Datensouveränität: Illusion oder Realität? *HMD Praxis der Wirtschaftsinformatik*, *60*(5), 1016–1033.

Anding, M. (2018). Fachkräftemangel: Zur Lösung eines greifbaren Problems in digitalen Zeiten. *Wirtschaftsinformatik & Management*, *10*(1), 14–21.

Andresen, J. (2017). *Retrospektiven in agilen Projekten: Ablauf, Regeln und Methodenbausteine*. Carl Hanser Verlag GmbH Co KG.

Appelfeller, W., & Feldmann, C. (2023). *Die digitale Transformation des Unternehmens - Systematischer Leitfaden mit zehn Elementen zur Strukturierung und Reifegradmessung* (2.Auflage). Springer Gabler Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-65413-2

Avila Pinto, R. (2018). Digital sovereignty or digital colonialsim. *International Journal on Human Rights*, *15*, 1–15.

Bal, R., & Gill, I. S. (2020). Policy approaches to artificial intelligence based technologies in China, European Union and the United States. *Duke Global Working Paper Series No. 26*, 1–27. https://doi.org/http://dx.doi.org/10.2

139/ssrn.3699640

Balzert, H. (1998). *Balzert H.(1998): Lehrbuch der Software-Technik: Software-Management, Software-Qualitätssicherung, Unternehmensmodellierung.* (Bd. 2). Springer.

Balzert, H. (2009). Anforderungen modellieren. In *Lehrbuch der Softwaretechnik: Basiskonzepte und Requirements Engineering* (S. 547–564). Spektrum Akademischer Verlag. https://doi.org/10.1007/978-3-8274-2247-7_25

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., & Rossi, M. (2018). Design science research contributions: Finding a balance between artifact and theory. *Journal of the Association for Information Systems*, *19*(5), 3. https://aisel.aisnet.org/jais/vol19/iss5/3

Baskerville, R., Pries-Heje, J., & Venable, J. (2009). Soft design science methodology. *Proceedings of the 4th international conference on design science research in information systems and technology*, 1–11. https://doi.org/https://doi.org/10.1145/1555619.155563

Bauer, M., & Erixon, F. (2020). *Europe's quest for technology sovereignty: Opportunities and pitfalls* (ECIPE Occasional Paper Nr. 02/2020). ECIPE Occasional Paper. Brussels, European Centre for International Political Economy (ECIPE). https://hdl.handle.net/10419/251089

Bechara, J., & Lechner, U. (2024). Digital Sovereignty and Open-Source Software - A Discussion Paper. In F. Phillipson, G. Eichler, C. Erfurth & G. Fahrnberger (Hrsg.), *Innovations for Community Services* (S. 397–407). Springer Nature Switzerland.

Becker, J., & Delfmann, P. (2013). *Referenzmodellierung: Grundlagen, Techniken und domänenbezogene Anwendung*. Springer-Verlag.

Becker, J., Delfmann, P., Knackstedt, R., & Kuropka, D. (2002). Konfigurative Referenzmodellierung. *Wissensmanagement mit Referenzmodellen: Konzepte für die Anwendungssystem- und Organisationsgestaltung*, 25–144.

Becker, J., Delfmann, P., & Rieke, T. (2007). Referenzmodellierung — Perspektiven für die effiziente Gestaltung von Softwaresystemen. In J. Becker, P. Delfmann & T. Rieke (Hrsg.), *Effiziente Softwareentwicklung mit Referenzmodellen* (S. 1–9). Physica-Verlag HD. https://doi.org/10.1007/978-3-7908-1994-6_1

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and Europeans Security Integration: an Introduction. *European Security*, *31*(3), 337–355.

Beyerer, J., Müller-Quade, J., & Reussner, R. (2018). Karlsruher Thesen zur Digitalen Souveränität Europas. *Datenschutz und Datensicherheit-DuD*, *42*(5), 277–280.

Biström, D., Adolfsson, K. K., & Stocchetti, M. (2024). Open-Source Software and Digital Sovereignty. In M. E. Auer, R. Langmann, D. May & K. Roos (Hrsg.), *Smart Technologies for a Sustainable Future* (S. 106–113). Springer Nature Switzerland.

Blossfeld, H.-P., Bos, W., Daniel, H.-D., Hannover, B., Köller, O., Lenzen, D., McElvany, N., Roßbach, H.-G., Seidel, T., Tippelt, R., et al. (2018). *Digitale Souveränität und Bildung. Gutachten*. Münster: Waxmann. https://doi.org/10.25656/01:16569

BMI. (2023). *IT-Strategie des Bundes*. Verfügbar 9. März 2025 unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitaler-wandel/it-strategie/it-strategie-bund-leitbild-und-ziele.pdf?__blob=publicationFile&v=5

BMJV. (2017). *Digitale Souveränität*. Verfügbar 9. März 2025 unter https://www.%20bmjv.%20de/SharedDocs/Downloads/DE/PDF/SVRV%5C_Gutachten%5C_DigitaleSouveraenitaet.%20pdf

Boehm, B. (1986). A spiral model of software development and enhancement. *ACM SIGSOFT Software engineering notes*, *11*(4), 14–24.

Boehm, B. W. (1988). A spiral model of software development and enhancement. *Computer*, *21*(5), 61–72.

Bögelsack, A., Chakraborty, U., Kumar, D., Wolz, E., Rank, J., & Tischbierek, J. (2022). Einleitung und Einführung zu Hyperscaler Clouds. In *SAP S/4 HANA-Systeme in Hyperscaler Clouds: Architektur, Betrieb und Setup von S/4HANA-Systemen in Microsoft Azure, Amazon Web Services und Google Cloud* (S. 1–28). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-34475-7_1

Bogenstahl, C., & Zinke, G. (2017). Digitale Souveränität–ein mehrdimensionales Handlungskonzept für die deutsche Wirtschaft. *iit Themenband Digitale Souveränität*, 65–82. https://doi.org/10.1007/978-3-662-55788-4_1

Bokolo, A. J. (2025). Implementing Digital Sovereignty to Accelerate Smarter Mobility Solutions in Local Communities. *Smart Cities*, *8*(4), 106.

Bolloju, N., Alter, S., Gupta, A., Gupta, S., & Jain, S. (2017). Improving Scrum User Stories and Product Backlog Using Work System Snapshots. *AMCIS*,

1–10.

Brattberg, E., Rugova, V., & Csernatoni, R. (2020). Europe and AI: Leading, lagging behind, or carving its own way? *Working Paper*, *9 Edition*, 1–51. https://carnegie-production-assets.s3.amazonaws.com/static/files/BrattbergCsernatoniRugova_-_Europe_AI.pdf

Bratton, B. H. (2016). *The stack: On software and sovereignty*. MIT press.

Brock, L. (1990). „Frieden". Überlegungen zur Theoriebildung. In V. Rittberger (Hrsg.), *Theorien der Internationalen Beziehungen: Bestandsaufnahme und Forschungsperspektiven* (S. 71–89). VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-322-88719-1_3

Brocke, J. v., Simons, A., Niehaves, B., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. *ECIS 2009*, 161. https://aisel.aisnet.org/ecis2009/161

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. *JCMS: Journal of Common Market Studies*, *61*(5), 1261–1280.

Brophy, J., & Bawden, D. (2005). Is Google enough? Comparison of an internet search engine with academic library resources. *Aslib proceedings*, *57*(6), 498–512.

Bruckner, F., & Howar, F. (2021). Utilizing Remote Evaluation for Providing Data Sovereignty in Data-sharing Ecosystems. *54th Hawaii International Conference on System Sciences*, 7005–7015. https://doi.org/10.24251/HICSS.2021.842

Brüesch, C., Menzi, C., & Mertes, A. (2022). *Digitale Verwaltung: Herausforderungen und Chancen neuer Trends für die Schweiz* (Techn. Ber.). ZHAW Zürcher Hochschule für Angewandte Wissenschaften.

Brugger-Gebhardt, S. (2016). *Die DIN EN ISO 9001: 2015 verstehen*. Springer.

Brühl, V. (2017). Bitcoins, Blockchain, and Distributed Ledgers: Funktionsweise, Marktentwicklungen und Zukunftsperspektiven. *Wirtschaftsdienst*, *97*, 135–142.

BSI. (2025a). *CB-K22/0639*. Verfügbar 5. Februar 2025 unter https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/2022/05/warnmeldung_cb-k22-0639.html

BSI. (2025b). *CSW-Nr. 2025-230373-1032*. Verfügbar 3. April 2025 unter https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2025/2025-230373-1032.pdf?__blob=publicationFile&v=3

BSI. (2023). *Ergebnisse der Studie zur statischen Codeanalyse ausgewählter Open-source Software CAOS 2.0*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/P486-Codeanalyse/Matrix-Kommunikationssoftware.pdf?__blob=publicationFile&v=3

Buhl, H. U., Schweizer, A., & Urbach, N. (2017). Blockchain-Technologie als Schlüssel für die Zukunft. *Zeitschrift für das gesamte Kreditwesen*, *12*, 596–599.

Burgfried, M., & Reckert-Lodde, A. (2022). Die deutsche Verwaltungscloud-Strategie: Auf dem Weg zur Digitalen Souveränität. *Datenschutz und Datensicherheit-DuD*, *46*(10), 611–615. https://doi.org/10.1016/j.techfore.2019.119751

Carayannis, E. G., Christodoulou, K., Christodoulou, P., Chatzichristofis, S. A., & Zinonos, Z. (2022). Known unknowns in an era of technological and viral disruptions—implications for theory, policy, and practice. *Journal of the knowledge economy*, *13*(1), 587–610.

Cavano, J. P., & McCall, J. A. (1978). A framework for the measurement of software quality. *Proceedings of the software quality assurance workshop on functional and performance issues*, 133–139. https://doi.org/10.1145/800283.811113

Chakhava, L., & Hikes-Wurm, D. (2024). Digital and Technological Sovereignty of the European Union: Strategic Necessity to Survive in the Global Competition?! *Journal of Information Warfare*, *23*(3), 95.

Chatterjee, R., & Chatterjee, R. (2017). An overview of the emerging technology: blockchain. *3rd International Conference on Computational Intelligence and Networks (CINE)*, 126–127. https://doi.org/10.1109/CINE.2017.33

Chinosi, M., & Trombetta, A. (2012). BPMN: An introduction to the standard. *Computer Standards & Interfaces*, *34*(1), 124–134. https://doi.org/10.1016/j.csi.2011.06.002

Chow, T., & Cao, D.-B. (2008). A survey study of critical success factors in agile software projects. *Journal of systems and software*, *81*(6), 961–971. https://doi.org/10.1016/j.jss.2007.08.020

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Clarke, V., & Braun, V. (2017). Thematic Analysis. *The Journal of Positive Psychology*, *12*(3), 297–298.

Colombo, E., & Stanca, L. (2014). The impact of training on productivity: evidence from a panel of Italian firms. *International Journal of Manpower*, *35*(8), 1140–1158. https://doi.org/https://doi.org/10.1108/IJM-08-2012-0121

Cook, K. A., Kim, K., & Omer, T. C. (2020). The cost of independence: Evidence from companies' decisions to dismiss audit firms as tax-service providers. *Accounting Horizons*, *34*(2), 83–107.

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

Dalmolen, S., Bastiaansen, H., Kollenstart, M., & Punter, M. (2020). Infrastructural sovereignty over agreement and transaction data ('metadata') in an open network-model for multilateral sharing of sensitive data. *40th International Conference on Information Systems (ICIS 2019)*, *23*, 1–17.

Davies, P., Fritzsche, A., Parry, G., & Wood, Z. (2023). Data, resilience, and identity in the digital age. *Strategic change*, *32*(6), 169–174. https://doi.org/10.1002/jsc.2560

Deelmann, T. (2006). Rahmenbedingungen und Geschäftsmodell der IT-Beratung. In *Beratung in der Softwareentwicklung Modelle – Methoden – Best Practices* (S. 34–47). Gesellschaft für Informatik e.V.

Derby, E., Schwaber, K., & Larsen, D. (2006). *Agile retrospectives: Making good teams great*. The pragmatic bookshelf. https://www.achievedigital.com/Agile/events/Agile%20Retrospectives%20Making%20Good%20Teams%20Great%20by%20Esther%20Derby,%20Diana%20Larsen,%20Ken%20Schwaber%20(z-lib.org).pdf

Die Bundesregierung. (2021). Datenstrategie der Bundesregierung: Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum. Bundeskanzleramt, Berlin. (Abgerufen am 11.03.2025). https://www.publikationen-bundesregierung.de/resource/blob/2277952/1845634/1a4f7ea800bb838562e16fdfe4ffb354/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1

Directorate-General-Communication. (2025). *European Chips Act*. Verfügbar 17. Juli 2025 unter https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en

Dous, M. (2007). *Kundenbeziehungsmanagement für interne IT-Dienstleister:*

Strategischer Rahmen, Prozessgestaltung und Optionen für die Systemunterstützung. (Band 3332). Springer. Gabler Edition Wissenschaft. https://doi.org/10.1007/978-3-8350-5446-2_4

Dreo, G., Eiseler, V., gentschen Felde, N., Gehrke, W., Helmbrecht, U., Hommel, W., & Zahn, J. (2020). Europäische Digitale Souveränität: Weg zum Erfolg?– Ein Bericht zur Jahrestagung CODE 2020. *Zeitschrift für Außen-und Sicherheitspolitik*, *13*, 399–404. https://doi.org/10.1007/s12399-020-00829-2

DSB. (2020). *Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen* (Techn. Ber.). Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 22.09.2020. Verfügbar 9. März 2025 unter https://www.datenschutzkonferenz-online.de/media/en/TOP%208%20Entschlie%C3%9Fung%20digitale%20Souver%C3%A4nit%C3%A4t_final.pdf

Dustdar, S., Gall, H., Hauswirth, M., Dustdar, S., Gall, H., & Hauswirth, M. (2023). Was ist Software-Architektur? In *Software-Architekturen für Verteilte Systeme* (S. 1–11). Springer. https://doi.org/10.1007/978-3-642-55599-2_1

Erben, M., & Günther, W. G. (2018). *Beschaffung von IT-Leistungen* (2.Auflage). Springer.

Esposito, C., Castiglione, A., Frattini, F., Cinque, M., Yang, Y., & Choo, K.-K. R. (2018). On data sovereignty in cloud-based computation offloading for smart cities applications. *IEEE Internet of Things Journal*, *6*(3), 4521–4535.

Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty-Rhetoric and reality. *Journal of European Public Policy*, 1–22. https://doi.org/10.1080/13501763.2024.2358984

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European security*, *31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Fettke, P., & Loos, P. (2002). Methoden zur Wiederverwendung von Referenzmodellen - Übersicht und Taxonomie. [Münster]. In J. Becker & R. Knackstedt (Hrsg.), *Referenzmodellierung 2002 - Methoden - Modelle - Erfahrungen. Tagungsband zur 6. Fachtagung Referenzmodellierung 2002 im Rahmen der MKWI 2002 in Nürnberg (zugl. Arbeitsbericht des Instituts für Wirtschaft* (S. 9–33).

Fettke, P., & Loos, P. (2004). Referenzmodellierungsforschung. *Wirtschaftsinformatik*, *5*(46), 331–340.

Fill, H.-G., Härer, F., & Meier, A. (2020). Wie funktioniert die Blockchain? *Blockchain: Grundlagen, Anwendungsszenarien und Nutzungspotenziale*, 3–19. https://doi.org/10.1007/978-3-658-28006-2_1

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & technology*, *33*, 369–378. https://doi.org/10.1007/s1334702000423-6

Fokusgruppe. (2019). „Digitale Souveränität in einer vernetzten Gesellschaft".(2018). *Digitale Souveränität und Künstliche Intelligenz–Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen.*, 1–6.

Fox, D. (2018). Digitale Souveränität. *Datenschutz und Datensicherheit-DuD*, *42*(5), 271–271.

Friedewald, M., Kreutzer, M., & Hansen, M. (2022). *Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg*. Springer Nature. https://doi.org/10.1007/978-3-658-33306-5

Friedrichsen, M., & Bisa, P.-J. (2016). *Digitale Souveränität - Vertrauen in der Netzwerkgesellschaft*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-07349-7

Fries, I., Greiner, M., Hofmeier, M., Hrestic, R., Lechner, U., & Wendeborn, T. (2022). Towards a layer model for digital sovereignty: a holistic approach. *International Conference on Critical Information Infrastructures Security*, 119–139.

Fritzsche, A. (2022). Konturenbildung im Gestaltungsraum der digitalen Transformation - eine Reflektion der Debatte über >digitale Souveränität< aus betriebswirtschaftlicher Sicht. In G. Glasze, E. Odzuck & R. Staples (Hrsg.), *Was heißt digitale Souveränität?* (S. 229–245). transcript Verlag. https://doi.org/https://doi.org/10.14361/9783839458273

Fritzsche, K., Pohle, J., Bauer, S., Haenel, F., & Eichbaum, F. (2022). Digitalisierung nachhaltig und souverän gestalten - Forschungsbericht zu den sozial-ökologischen Perspektiven für eine selbstbestimmte Digitalpolitik (S. Bauer, Hrsg.). *Positionspapier No.10*, *21*, 1–248. https://codina-transformation.de/wp-content/uploads/Final_CODINA_Forschungsbericht_DS.pdf#page=21

Fritzsche, K., & Spoiala, D. (2022). The EU–AU Digital Partnership: Between

Digital Geopolitics and Digital Sovereignty. In C. Daniels, B. Erforth & C. Teevan (Hrsg.), *Africa–Europe Cooperation and Digital Transformation* (S. 17–31). Routledge. https://doi.org/https://doi.org/10.4324/9781003274322

Fromm, J., Mirbabaie, M., & Stieglitz, S. (2020). A Systematic Review of Empirical Affordance Studies: Recommendations for Affordance Research in Information Systems. *Twenty-Eigth European Conference on Information Systems (ECIS2020)*, 1–11. Verfügbar 21. Mai 2025 unter https://aisel.aisnet.org/ecis2020_rip/42

Fuhr, E. (1977). Militärische Landesverteidigung. *Bundeswehr und Gesellschaft: Ein Wörterbuch*, 185–186.

Gacek, C., & Arief, B. (2004). The many meanings of open source. *IEEE software*, *21*(1), 34–40. https://doi.org/10.1109/MS.2004.1259206

Gao, F., Jia, X., Zhao, Z., Chen, C.-C., Xu, F., Geng, Z., & Song, X. (2021). Bibliometric analysis on tendency and topics of artificial intelligence over last decade. *Microsystem Technologies*, *27*, 1545–1557. https://doi.org/10.1007/s00542-019-04426-y

Genaid, A., et al. (2012). Connecting user stories and code for test development. *Third International Workshop on Recommendation Systems for Software Engineering (RSSE 2012)*, 33–37. https://doi.org/10.1109/RSSE.2012.6233406

Gibson, J. J. (1977). The theory of affordances. *Hilldale, USA*, *1*(2), 67–82.

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., et al. (2023). Contested spatialities of digital sovereignty. *Geopolitics*, *28*(2), 919–958.

Glasze, G., Odzuck, E., & Staples, R. (2022). *Was heißt digitale Souveränität?: Diskurse, Praktiken und Voraussetzungen» individueller «und» staatlicher Souveränität «im digitalen Zeitalter*. transcript Verlag. https://doi.org/10.14361/9783839458273

Glohr, C., Schult, S., & Schulze-Hulitz, E. (2022). *Zukunft gestalten: Erfolgsfaktoren zur Digitalisierung in der öffentlichen Verwaltung* (Techn. Ber.). Detecon International GmbH. https://www.detecon.com/drupal/sites/default/files/2023-08/Studie_ErfolgsfaktorenzurDigitalisierunginderoeffentlichenVerwaltung.pdf

Goldacker, G. (2017). *Digitale Souveränität*. Kompetenzzentrum Öffentliche Informationstechnologie, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS.

Gong, C., & Ribiere, V. (2021). Developing a unified definition of digital transformation. *Technovation*, *102*, 102217. https://doi.org/10.1016/j.technovation.2020.102217

Gräf, E., Lahmann, H., & Otto, P. (2018). Die Stärkung der digitalen Souveränität. *Wege der Annäherung an ein Ideal im Wandel*. Verfügbar 5. Mai 2025 unter https://www.divsi.de/wp-content/uploads/2018/05/DIVSI-Themenpapier-Digitale-Souveraenitaet.pdf

Gregor, S., & Hevner, A. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, *37*(2), 337–355. https://www.jstor.org/stable/43825912

Grund, D. (2013). *Agile Architektur mit .NET - Grundlagen und Best Practices*. entwickler.Press. https://books.google.de/books?id=lXLIEAAAQBAJ

Gundelsweiler, F., Memmel, T., & Reiterer, H. (2004). Agile usability engineering. *Mensch und Computer 2004: Allgegenwärtige Interaktion*, 33–42. https://doi.org/10.1524/9783486598773.33

Häder, M., & Häder, S. (2000). Die Delphi-Methode als Gegenstand methodischer Forschungen. In M. Häder & S. Häder (Hrsg.), *Die Delphi-Technik in den Sozialwissenschaften: Methodische Forschungen und innovative Anwendungen* (S. 11–31). VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-663-09682-5_1

Hanschke, I. (2022). *Enterprise Architecture Management-einfach und effektiv: Ein praktischer Leitfaden für die Einführung von EAM* (3.Auflage). Carl Hanser Verlag GmbH Co KG.

Harrison, R. (2016). *TOGAF® 9 Foundation Study Guide - Preperation for the TOGAF 9 Part 1 Examination* (3rd Edition). Van Haren.

Hartmann, E. A. (2021). Digitale Souveränität in der Wirtschaft-Gegenstandsbereiche, Konzepte und Merkmale. *Digitalisierung souverän gestalten: Innovative Impulse im Maschinenbau*, 1–16. https://doi.org/10.1007/978-3-662-62377-0

Herlo, B., Ullrich, A., & Vladova, G. (2022). *Verantwortungsvolle demokratisch nachhaltige digitale Souveränität* (Kurzstudie). Weizenbaum-Institut e.V.

Hevner, A., & Chatterjee, S. (2010). *Design Research in Information Systems: Theory and Practice* (22. Aufl.). Springer Science & Business Media.

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105.

Hinckeldeyn, J. (2019). Blockchain-Technologie in der Supply Chain. *Essentials*. https://doi.org/10.1007/978-3-658-26440-6

Hofmeier, M., Klare, M., Fries, I., & Weeber, K. (2024). *Digitale Souveränität: Handlungsempfehlungen*. Verfügbar 13. März 2025 unter https://www.unibw.de/lions/lions_handlungsempfehlungen_digital.pdf

Holfelder, W., Mayer, A., & Baumgart, T. (2022). Sovereign Cloud Technologies for Scalable Data Spaces. *Designing Data Spaces*, *419*. https://doi.org/10.1007/978-3-030-93975-5

Huber, A. (2021). *Automobile Wertschöpfung: Eine internationale Untersuchung von Innovations-, Produkt-und Plattformstrategien vor dem Hintergrund der Elektrifizierung* [Diss., Institut für Fahrzeugkonzepte].

Hummel, P., Braun, M., Augsberg, S., Ulmenstein, U., & Dabrock, P. (2021). *Datensouveränität: Governance-Ansätze für den Gesundheitsbereich*. Springer Nature. https://doi.org/10.1007/978-3-658-33755-1

Hummert, C. (2023). Cyberagentur: Der besondere Weg zur digitalen Souveränität: Mehr Handlungsspielraum für disruptive Innovationen erforderlich. *Datenschutz und Datensicherheit-DuD*, *47*(7), 425–428. https://doi.org/10.1007/s11623-023-1791-z

IEEE. (1990). *DIN 610.12-1990: IEEE standard glossary of software engineering terminology*.

IT-Planungsrat. (2013). Zukunftspfade Digitales Deutschland 2020. TNS Infratest. *IT-Planungsrat & IT-Rat.(2020). Eckpunktepapier Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung*, (2020/19). https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2014/zukunftspfade-digitales-deutschland-2020.pdf?__blob=publicationFile&v=1

Janßen, F. (2023). Digitale Souveränität von Kommunen stärken – eine Daueraufgabe. *47*. https://dl.gi.de/items/315d212b-253c-42ba-91f3-154acc8e606d

Jennings, M. D. (2000). Gap analysis: concepts, methods, and recent results. *Landscape ecology*, *15*, 5–20. https://doi.org/10.1023/A:1008184408300

Joecks-Laß, D., & Hadwich, K. (2021). Wollen, Können und Dürfen der Kunden–Digitale Souveränität durch Kundenentwicklung. In E. Hartmann (Hrsg.), *Digitalisierung souverän gestalten: Innovative Impulse im Maschinenbau* (S. 74–85). https://doi.org/10.1007/978-3-662-62377-0_6

Jones, K. S. (2018). What is an affordance? In *How Shall Affordances Be Refined?* (1st Edition, S. 107–114). Routledge.

Kagermann, H. (2021). Digitale Souveränität: Status quo und Handlungsfelder. *Deutsche Nationalbibliothek*, 1–7. Verfügbar 21. Mai 2025 unter https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder/

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. https://doi.org/10.1515/ngs-2021-0015

Kar, R. M., & Thapa, B. (2020). Digitale Souveränität als strategische Autonomie. *Berlin: Kompetenzzentrum Öffentliche IT/Fraunhofer FOKUS*, 5–27.

Kerth, N. L. (2013). *Project retrospectives: a handbook for team reviews*. Addison-Wesley.

Kim, S., & Ji, Y. (2018). Gap Analysis. *The International Encyclopedia of Strategic Communication*, *8*, 1–6. https://doi.org/10.1002/9781119010722.iesc0079

Kinkel, S., Jung Erceg, P., & Lay, G. (2002). *Auslandsproduktion-Chance oder Risiko für den Produktionsstandort Deutschland? Stand, Entwicklung und Effekte von Produktionsverlagerungen im verarbeitenden Gewerbe* (Techn. Ber.). Mitteilungen aus der Produktionsinnovationserhebung Nr.26. https://doi.org/10.24406/publica-fhg-291374

Kipker, D.-K. (2022). *Der Rechtsstaat wird herausgefordert: die BSI-Warnung vor Kaspersky*. Verfügbar 17. Juli 2025 unter https://opus.bibliothek.uni-augsburg.de/opus4/frontdoor/index/index/docId/111374

Klare, M., Hrestic, R., Stelter, A., & Lechner, U. (2025). Digital Sovereignty and Digital Transformation Practice Recommendation for the Software Life Cycle Process. *Procedia Computer Science*, *254*, 221–229. https://doi.org/https://doi.org/10.1016/j.procs.2025.02.081

Klare, M., & Lechner, U. (2023). Digital Sovereignty from the Perspective of IT Consultancy in Germany: A Model. *ICSOB Companion*, 1–14. https://ceur-ws.org/Vol-3621/poster-paper5.pdf

Klare, M., & Lechner, U. (2025). Digital Sovereignty: Affordances in Open Source Projects. In E. Papatheocharous, S. Farshidi, S. Jansen & S. Hyrynsalmi (Hrsg.), *Software Business* (S. 20–34). Springer Nature Switzerland. https://doi.org/https://doi.org/10.1007/978-3-031-85849-9_2

Klare, M., & Lechner, U. (2024a). German Digital Sovereignty–Success Factors in a National Defense Scenario from the Standpoint of IT Consultancy. In I. Fries, M. Grabatin & M. Hofmeier (Hrsg.), *LIONS Sovereign by Design* (S. 41–56). Logos Verlag Berlin. https://doi.org/https://doi.org/10.30819/5834

Klare, M., & Lechner, U. (2024b). A Reference Model to Strengthen Digital Sovereignty in Companies. *ICSOB Companion*, 1–9. Verfügbar 5. Mai 2025 unter https://ceur-ws.org/Vol-3921/phd-paper3.pdf

Klare, M., Lechner, U., & Fritzsche, A. (2025). Digital Sovereignty through Sovereign Clouds? *International Conference on AI and the Digital Economy*.

Klare, M., Verlande, L., Greiner, M., & Lechner, U. (2022). How Blockchain and Artificial Intelligence influence Digital Sovereignty. In M. Papadaki, P. Rupino da Cunha, M. Themistocleous & K. Christodoulou (Hrsg.), *Information Systems. EMCIS 2022* (S. 3–16). Springer Nature Switzerland. https://doi.org/https://doi.org/10.1007/978-3-031-30694-5_1

Kumar, A., Grover, P., Kar, A. K., & Pani, A. K. (2017). IT Consulting: A Systematic Literature Review. *16th IFIP WG 6.11 Conference on E-Business, E-Services, and E-Society (I3E 2017)*, 474–484. https://doi.org/10.1007/978-3-319-68557-1_42

Lai, F. W. (2011). A strategic framework for value enhancing enterprise risk management. *Journal of Global Business and Economics*, *2*(1), 1–25.

Lambach, D., & Oppermann, K. (2023). Narratives of Digital Sovereignty in German Political Discourse. *Governance Journal*, *36*(3), 693–709. https://doi.org/10.1111/gove.12690

Laurent, A. M. S. (2004). *Understanding Open Source and Free Software Licensing: Guide to Navigating Licensing Issues in Existing & Mew Software*. O'Reilly Media, Inc.

Lee, J., Suh, T., Roy, D., & Baucus, M. (2019). Emerging Technology and Business Model Innovation: The Case of Artificial Intelligence. *Journal of Open Innovation: Technology, Market, and Complexity*, *5*(3), 44. https://doi.org/10.3390/joitmc5030044

Leonardi, P. (2023). Affordances and Agency: Toward the Clarification and Integration of Fractured Concepts. *MIS Quarterly*, *47*(4).

Leyh, C., & Bley, K. (2016). Digitalisierung: Chance oder Risiko für den deutschen Mittelstand?–Eine Studie ausgewählter Unternehmen. *HMD Praxis der*

Wirtschaftsinformatik, *53*, 29–41. https://doi.org/10.1365/s40702-015-0197-2

Lindner, D. (2020). Forschungsdesigns der Wirtschaftsinformatik. In *Forschungsdesigns der Wirtschaftsinformatik: Empfehlungen für die Bachelor- und Masterarbeit* (S. 19–44). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-31140-7_4

Lorenc, T., Felix, L., Petticrew, M., Melendez-Torres, G., Thomas, J., Thomas, S., O'Mara-Eves, A., & Richardson, M. (2016). Meta-analysis, complexity, and heterogeneity: a qualitative interview study of researchers' methodological values and practices. *Systematic Reviews*, *5*(1), 192.

Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2019). Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. *IEEE Transactions on Industrial Informatics*, *16*(6). https://doi.org/10.1109/TII.2019.2942190

Madiega, T. A. (2020). *Digital Sovereignty for Europe: Enhancing Strategic Autonomy in the Digital Field, EPRS: European Parliamentary Research Service.* (Techn. Ber.). EPRS: European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

Mandl, H., & Fischer, F. (2000). Mapping-Techniken und Begriffsnetze in Lern- und Kooperationsprozessen. In *Wissen sichtbar machen - Wissensmanagement mit Mapping-Techniken* (S. 1–12). Göttingen: Hogrefe.

Manita, R., Elommal, N., Baudier, P., & Hikkerova, L. (2020). The Digital Transformation of External Audit and its Impact on Corporate Governance. *Technological Forecasting and Social Change*, *150*, 119751.

Martens, K., & Zscheischler, J. (2022). The Digital Transformation of the Agricultural Value Chain: Discourses on Opportunities, Challenges and Controversial Perspectives on Governance Approaches. *Sustainability*, *14*(7), 3905. https://doi.org/doi.org/10.3390/su14073905

Massaro, M. (2021). Digital Transformation in the Healthcare Sector through Blockchain Technology - Insights from Academic Research and Business Developments. *Technovation*, 102386. https://doi.org/10.1016/j.technovation.2021.102386

Mayring, P., & Brunner, E. (2007). Qualitative Inhaltsanalyse. In R. Buber & H. H. Holzmüller (Hrsg.), *Qualitative Marktforschung: Konzepte — Methoden —*

Analysen (S. 669–680). Gabler. https://doi.org/10.1007/978-3-8349-9258-1_42

Mayring, P., & Fenzl, T. (2019). Qualitative Inhaltsanalyse. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 633–648). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-21308-4_42

McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. *20th International Conference on Artificial intelligence and Statistics*, *54*.

Meinel, C., Gayvoronskaya, T., & Schnjakin, M. (2018). *Blockchain: Hype oder Innovation* (Bd. 113). Universitätsverlag Potsdam. https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/10314/file/tbhpi113.pdf

Meline, T. (2006). Selecting Studies for Systemic Review: Inclusion and Exclusion Criteria. *Contemporary Issues in Communication Science and Disorders*, *33*, 21–27. https://doi.org/10.1044/cicsd_33_S_21

Merkel, A., Frederiksen, M., Marin, S., & Kallas, K. (2021). Letter to the President–Digital Sovereignty. *Berlin, Copenhagen, Helsinki, Tallinn: Open Future Foundation*, 1–3. https://openfuture.eu/wp-content/uploads/2022/04/210301DE-DK-FI-EE-Letter-to-COM-President-on-Digital-Sovereignty.pdf

Merkel, A. (2019). *Rede von Bundeskanzlerin Angela Merkel zur Eröffnung des 14. Internet Governance Forums 26. November 2019 in Berlin*. Verfügbar 31. Dezember 2024 unter https://www.bundesregierung.de/breg-de/aktuelles/rede-von-bundeskanzlerin-angela-merkel-zur-eroeffnung-des-14-internet-governance-forums-26-november-2019-in-berlin-1698264

Metakides, G. (2002). A Crucial Decade for European Digital Sovereignty. In H. Werthner, E. Prem, E. A. Lee & C. Ghezzi (Hrsg.), *Perspectives on Digital Humanism* (1. Aufl., S. 2–342). Springer Cham. https://doi.org/https://doi.org/10.1007/978-3-030-86144-5

Meuser, M., & Nagel, U. (2009). The Expert Interview and Changes in Knowledge Production. In *Interviewing Experts* (S. 17–42). Springer. https://doi.org/10.1057/97802302442762

Michels, J. D. (2025). *Sovereign Cloud for Europe: Independent Research Report*

prepared for Broadcom. https://doi.org/http://dx.doi.org/10.2139/ssrn.5146122

Moerel, L., & Timmers, P. (2021). Reflections on Digital Sovereignty. *EU Cyber Direct, Research in Focus Series*, 1–33. https://ssrn.com/abstract=3772777

Möllers, H. (2022). Gemeinsam abwehrbereit: die Bedeutung der Landes-und Bündnisverteidigung. *Zentrum für Militärgeschichte und Sozialwissenschaften der Bundeswehr*.

Mörl, R. (2024). Digitale Souveränität ist eine subjektive Entscheidung, die mit geeigneten Mitteln aktiv gemanagt werden kann!: Verständnisbildung, Herausforderungen und Lösungen für das Management Digitale Souveränität. In *Informatik 2024* (S. 629–648). Gesellschaft für Informatik e.V. https://doi.org/10.18420/inf2024_50

Müller, R., & Jugdev, K. (2012). Critical Success Factors in Projects: Pinto, Slevin, and Prescott–the Elucidation of Project Success. *International Journal of Managing Projects in Business*, *5*(4), 757–775.

Müller-Böling, D., & Klandt, H. (1996). Methoden empirischer Wirtschafts- und Sozialforschung. *Eine Einführung mit wirtschaftswissenschaftlichem Schwerpunkt*, *3*, 1–98.

Németh, T. (1992). Methoden und Werkzeuge für den konstruktiven Entwurf von Objektsystemen. *Eiffel: Fachtagung des German Chapter of the ACM eV in Zusammenarbeit mit der Gesellschaft für Informatik eV, FA 2.1, am 25. und 26. Mai 1992 in Darmstadt*, 39–53. https://doi.org/10.1007/978-3-322-86775-9_4

Nohe, P. (1999). *Methode zur ergebnisorientierten Gestaltung von Entwicklungsprozessen* (1. Aufl.). Springer Berlin, Heidelberg. https://doi.org/https://doi.org/10.1007/978-3-642-47978-6

Opt, S., & Sims, C.-D. L. (2015). Scrum: Enhancing Student Team Organization and Collaboration. *Communication Teacher*, *29*(1), 55–62. https://doi.org/10.1080/17404622.2014.939675

Pashchenko, D. (2024). Excellence Practices in Scrum Paradigm in Software Development. *Journal of Data Science and Intelligent Systems*. https://doi.org/10.47852/bonviewJDSIS42023645

Paulsen, M., Nina und Heger. (2024). *Deutschlands Abhängigkeit von Digitalimporten wächst*. Verfügbar 11. März 2025 unter https://www.bitkom.org/Presse/Presseinformation/Souveraenitaet-Abhaengigkeit-Digitalimp

orten-waechst#:~:text=Aktuell%20sehen%2088%20Prozent%20der,f%C3%BCnf%20Jahren%20verringert%20haben%20wird.

Perens, B., et al. (1999). The Open Source Definition. *Open Sources: Voices from the Open Source Revolution*, *1*, 171–188.

Petit, A., Wala, Z., Ciucci, M., & Martinello, B. (2024). *Digital Agenda for Europe, Fact Sheets on the European Union*. Verfügbar 31. Dezember 2024 unter https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europ

Peuker, E. (2020). *Verfassungswandel durch Digitalisierung: digitale Souveränität als verfassungsrechtliches Leitbild*. DGRI Jahrbuch 2019, herausgegeben von Köln: Verlag Dr. Otto Schmidt, 2021. https://doi.org/10.9785/9783504386900-025

Philipp, U. (2022). *Schriftliche Frage an die Bundesregierung im Monat Januar 2022 Frage Nr.76*. Verfügbar 11. März 2025 unter https://mdb.anke.domscheit-berg.de/wp-content/uploads/2022/03/1-76-Domscheit-BergGeschwaerzt.pdf

Piétron, D. (2019). Digitale Souveränität durch Interoperabilität. *WiSO Direkt*, *24*, 1–4.

Pohle, J. (2020). Digitale Souveränität. Ein neues digitalpolitisches Schlüsselkonzept in Deutschland und Europa? *Konrad-Adenauer-Stiftung*, 1–28. https://www.kas.de/de/einzeltitel/-/content/digitale-souveraenitaet%0A

Pohle, J., & Santaniello, M. (2024). From multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance? *Policy & Internet*, *16*. https://doi.org/https://doi.org/10.1002/poi3.426

Pohle, J., & Thiel, T. (2021). Digitale Souveränität-Von der Karriere eines einenden und doch problematischen Konzepts. In *Der Wert der Digitalisierung: Gemeinwohl in der digitalen Welt* (1. Aufl., S. 319–340, Bd. 36). Bielefeld: transcript Verlag. https://doi.org/https://doi.org/10.14361/9783839456590

Pohle, J., Thüer, L., Dammann, F., & Winkler, J. (2022). Das Subjekt im politischen Diskurs zu „digitaler Souveränität“. In *Handbuch Digitalisierung und politische Beteiligung* (S. 1–23). Springer.

Pretschner, A., Massacci, F., & Hilty, M. (2007). Usage Control in Service-Oriented Architectures. *Trust, Privacy and Security in Digital Business: 4th International Conference*, 83–93.

Price, A. D., & Chahal, K. (2006). A Strategic Framework for Change Management. *Construction Management and Economics*, *24*(3), 237–251. https://doi.org/https://doi.org/10.1080/01446190500227011

Pries-Heje, J., Baskerville, R., & Venable, J. (2014). Soft Design Science Methodology. In J. Simonsen, C. Svabo, S. Strandvad, K. Samson, M. Hertzum & O. Hansen (Hrsg.), *Situated Design Methods* (S. 77–95). MIT Press. https://books.google.de/books?hl=de&lr=&id=VEJvEAAAQBAJ&oi=fnd&pg=PR7&dq=Situated+Methods+in+Design&ots=iz90SjjPFA&sig=z2M89mKOsoTcENWZHixuiT8tpP8&redir_esc=y#v=onepage&q=Situated%20Methods%20in%20Design&f=false

Rath, M., Keller, L., & Spies, A. (2023). Sovereign Clouds—An overview of the current privacy challenges associated with the use of US cloud services, and how sovereign clouds can address these challenges. *Computer Law Review International*, *24*(3), 78–84.

Rea, L., & Parker, R. (2014). *Designing and Conducting Survey Research: A Comprehensive Guide*. Wiley. https://books.google.de/books?id=Ub8BBAAAQBAJ

Rehm, S., & Schulz, H. (2020). *Digitalisierung durchdenken und gestalten: Ein Plädoyer für strategisches Handeln.* Bauer, Reinhard [Hrsg.]; Hafer, Jörg [Hrsg.]; Hofhues, Sandra [Hrsg.]; Schiefner-Rohs, Mandy [Hrsg.]; Thillosen, Anne [Hrsg.]; Volk, Benno [Hrsg.]; Wannemacher, Klaus [Hrsg.]: Vom E-Learning zur Digitalisierung. Mythen, Realitäten, Perspektiven. Münster; New York: Waxmann 2020. Medien in der Wissenschaft. https://doi.org/10.25656/01:21744

Reiners, W. (2021). Die Digitalisierungsstrategie der Europäischen Union–Meilensteine und Handlungsfelder zwischen digitaler Souveränität und grüner Transformation. *Integration*, *44*(4), 266–286.

Reis, J., Amorim, M., Melão, N., Cohen, Y., & Rodrigues, M. (2020). Digitalization: A literature review and research agenda. *Proceedings on 25th International Joint Conference on Industrial Engineering and Operations Management (IJCIEOM): The Next Generation of Production and Service Systems 25*, 443–456.

Reis, J., Amorim, M., Melão, N., & Matos, P. (2018). Digital Transformation: A Literature Review and Guidelines for Future Research. In Á. Rocha, H. Adeli, L. P. Reis & S. Costanzo (Hrsg.), *Trends and Advances in*

Information Systems and Technologies (S. 411–421). Springer International Publishing. https://doi.org/https://doi.org/10.1007/978-3-319-77703-0_41

Reisach, U. (2018). Die Digitale Transformation Chinas-eine Herausforderung für Deutschland?(The digital transformation of China-a challenge for Germany?) *DLR/Deutsch-Chinesische Plattform Innovation: Policy Briefs der deutschen Expertengruppe*, 38–44.

Rentrop, C. (2024). COBIT als Rahmenwerk der IT-Governance. In *IT-Governance: Zentraler Erfolgsfaktor für die digitale Transformation* (S. 91–113). Erich Schmidt Verlag GmbH & Co. KG. https://doi.org/10.37307/b.978-3-503-14487-7.05

Richter, J.-P., Haller, H., & Schrey, P. (2005). Serviceorientierte Architektur. *Informatik-Spektrum*, *28*(5), 413–416.

Rikap, C., Durand, C., Paraná, E., Gerbaudo, P., & Marx, P. (2024). *Reclaiming digital sovereignty: A roadmap to build a digital stack for people and the planet*. A collective proposal by the Democratic; Ecological Digital Sovereignty Coalition. https://lutpub.lut.fi/bitstream/handle/10024/168600/LUT%20whitepaper_reclaiming-digital-sovereignty.pdf?sequence=3&isAllowed=y

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*. https://doi.org/http://dx.doi.org/10.2139/ssrn.3937345

Rone, J. (2024). 'The Sovereign Cloud' in Europe: Diverging Nation State Preferences and Disputed Institutional Competences in the Context of Limited Technological Capabilities. *Journal of European Public Policy*, 1–27. https://doi.org/10.1080/13501763.2024.2348618

Rothmann, P.-C. (2016). Digitale Souveränität - aus Sicht eines Beratungsunternehmens und deren Kunden. *Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft*, 213–222.

Royce, W. W. (1970). Managing the Development of Large Software Systems (1970). *Proceedings of the 9th International Conference on Software Engineering*.

Royce, W. W. (1987). Managing the Development of Large Software Systems: Concepts and Techniques. *Proceedings of the 9th International Conference on Software Engineering*, 328–338.

Rubin, E., & Rubin, H. (2011). Supporting agile software development through

active documentation. *Requirements Engineering*, *16*, 117–132. https://doi.org/https://doi.org/10.1007/s00766-010-0113-9

Sauer, S., Staples, R., & Steinbach, V. (2022). Der relationale Charakter von> digitaler Souveränität<. Zum Umgang mit dem >Autonomie/Heteronomie<-Dilemma in sich transformierenden Arbeitswelten. *Georg Glasze/Eva Odzuck/Ronald Staples (Hg.), Was heißt digitale Souveränität*, 287–315.

Schauf, T., Neuburger, R., Ganten, P., Bending, T., Bienert, J., Dapp, T., Ehmann, P., Krosta-Hartl, P., Mentzinis, P., Pfeiffer, M., et al. (2019). *Digitale Souveränität im Kontext plattformbasierter Ökosysteme*. Verfügbar 27. August 2025 unter https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/digitale-souveraenitaet.pdf?__blob=publicationFile&v=3

Scheer, A.-W., & Köppen, A. (2013). *Consulting: Wissen für die Strategie-, Prozess- und IT-Beratung*. Springer-Verlag.

Scholze, M., Grauf, K., & Urband, T. (2023). *Why it pays to be independent - Digital Sovereignty*. Verfügbar 25. Februar 2025 unter https://www.pwc.de/en/digitale-transformation/open-source-software-management-and-compliance/digital-sovereignty-why-it-pays-to-be-independent.html

Schuh, G., Anderl, R., Gausemeier, J., Ten Hompel, M., & Wahlster, W. (2017). *Industrie 4.0 Maturity Index: Die digitale Transformation von Unternehmen gestalten*. Herbert Utz Verlag.

Schütte, R. (2013). *Grundsätze ordnungsmäßiger Referenzmodellierung: Konstruktion konfigurations-und anpassungsorientierter Modelle* (Bd. 233). Springer-Verlag.

Seffah, A., Kececi, N., & Donyaee, M. (2001). QUIM: a Framework for Quantifying Usability Metrics in Software Quality Models. *Proceedings second asia-pacific conference on quality software*, 311–318. https://doi.org/10.1109/APAQS.2001.990036

Seifried, M., & Bertschek, I. (2021). *Schwerpunktstudie Digitale Souveränität - Bestandsaufnahme und Handlungsfelder* (Techn. Ber.). Bundesministerium für Wirtschaft und Energie. https://www.de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-download-schwerpunkt-digitale-souveraenitaet-2021.pdf

Seyffarth, M. (2023). Mehr digitale Souveränität für die öffentliche Verwaltung: Mit Open Source! *Digitale Souveränität*, *47*. https://dl.gi.de/items/b0b03b

c9-473d-41f9-8363-b3a7744c7b3f

Sheikh, H. (2022). European digital sovereignty: a layered approach. *Digital Society*, *1*(3), 25. https://doi.org/https://doi.org/10.1007/s44206-022-00025-z

Shinde, P. P., & Shah, S. (2018). A Review of Machine Learning and Deep Learning Applications. *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 1–6. https://doi.org/10.1109/ICCUBEA.2018.8697857

Skierka, I. (2020). *5G-Debatte: Ein Test für die digitale Souveränität Europas* (K.-A.-S. e.V., Hrsg.). JSTOR. https://www.jstor.org/stable/pdf/resrep25286.pdf?acceptTC=true&coverpage=false&addFooter=false

Smit, S., Tyreman, M., Mischke, J., Ernst, P., Hazan, E., Jurica, N., Hieronimus, S., & Dagorretm, G. (2022). *Securing Europe's competitiveness* (Techn. Ber.). McKinsey & Company. Verfügbar 15. Mai 2025 unter https://www.mckinsey.com/~/media/mckinsey/business%20functions/strategy%20and%20corporate%20finance/our%20insights/securing%20europes%20competitiveness%20addressing%20its%20technology%20gap/securing-europes-competitiveness-addressing-its-technology-gap-september-2022.pdf

Starke, G. (2020). *Effektive Softwarearchitekturen: Ein praktischer Leitfaden*. Carl Hanser Verlag GmbH Co KG.

Stelter, A., Klare, M., & Lechner, U. (2025). Digital Sovereignty and Digital Transformation Extension for the Software Life Cycle Process in ISO/IEC/IEEE 12207:2017. *Artificial Intelligence in Context of Digital Sovereignty*.

Sunny, J., Undralla, N., & Pillai, V. M. (2020). Supply chain transparency through blockchain-based traceability: An overview with demonstration. *Computers & Industrial Engineering*, *150*, 106895.

Szvetits, M., & Zdun, U. (2016). Systematic literature review of the objectives, techniques, kinds, and architectures of models at runtime. *Software & Systems Modeling*, *15*, 31–69.

Thomas, O. (2005). Understanding the Term Reference Model in Information Systems Research: History, Literature Analysis and Explanation. In C. J. Bussler & A. Haller (Hrsg.), *International Conference on Business Process Management* (S. 484–496). https://doi.org/https://doi.org/10.1007/11678564_45

Toth, S., & Vigenschow, U. (2013). Architektur und Agilität—so passt das zusammen. *HMD Praxis der Wirtschaftsinformatik*, *50*, 44–55.

Umar, M. A. (2023). Corporate Restructuring: A strategy for improving organizational performance. *International Journal of Strategic Decision Sciences (IJSDS)*, *14*(1), 1–11.

Unger, W. J. (2014). Cyber Defence–eine nationale Herausforderung. *Sicherheit und Frieden (S+ F)/Security and Peace*, *32*, 8–16. http://www.jstor.org/stable/24233886

Urban, M. (2024). Sovereign Cloud Stack (SCS): Offene föderierbare Cloud-Technologie für jeden Sektor. *FOSSGIS 2024*.

Urban, M., & Garloff, K. (2022). Sovereign Cloud Stack: Technische Souveränität durch offene, föderierbare und modulare Cloud-Plattformen vollständig auf Basis von Open-Source-Software. *Datenschutz und Datensicherheit-DuD*, *46*(10), 616–621.

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of business research*, *122*, 889–901.

Verwijmeren, M. (2004). Software component architecture in supply chain management. *Computers in industry*, *53*(2), 165–178.

Vogel, O., Arnold, I., Chughtai, A., & Kehrer, T. (2011). *Software Architecture: A Comprehensive Framework and Guide for Practitioners*. Springer Berlin Heidelberg. https://books.google.de/books?id=M3RzjWmMgBwC

Vogt, R. (2021). Digitale Souveränität und Künstliche Intelligenz für den Menschen. *Digitalisierung souverän gestalten*, 143–150. https://doi.org/https://doi.org/10.1007/978-3-662-62377-0_11

Volkoff, O., & Strong, D. M. (2017). Affordance theory and how to use it in IS research. *The Routledge companion to management information systems*.

Volkoff, O., & Strong, D. M. (2013). Critical realism and affordances: Theorizing IT-associated organizational change processes. *MIS Quarterly*, 819–834.

Vom Brocke, J. (2003). *Referenzmodellierung: Gestaltung und Verteilung von Konstruktionsprozessen* (Bd. 2). Logos-Verlag.

Wallenhorst, D. (2023). Informationstechnologie. In *Perspektivenwechsel in der Digitalisierung: Interdisziplinäre Ansätze für die digitale Epoche* (S. 99–123). Springer.

Weber, H. (2022). Digitale Souveränität. *Informatik Spektrum*, 1–12. https://gi.de/fileadmin/GI/Mitgliederbereich/Informatik-Spektrum/287_45_2_web.pdf#page=5

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press.

Weyer, J. (2018). Digitale Transformation und öffentliche Sicherheit. *Forschungsforum Öffentliche Sicherheit*. https://doi.org/10.17169/refubium-25159

Wirnsperger, P., Dinnessen, F., & Hilberg, J. (2021). *Mit digitaler Souveränität ins europäische digitale Jahrzehnt*. Verfügbar 8. Mai 2025 unter https://www.deloitte.com/de/de/Industries/government-public/perspectives/digitale-souveraenitaet-im-oeffentlichen-sektor.html

Wittpahl, V. (2018). *Digitale Souveränität: Bürger/ Unternehmen/ Staat*. Springer Nature. https://link.springer.com/book/10.1007/978-3-662-55796-9

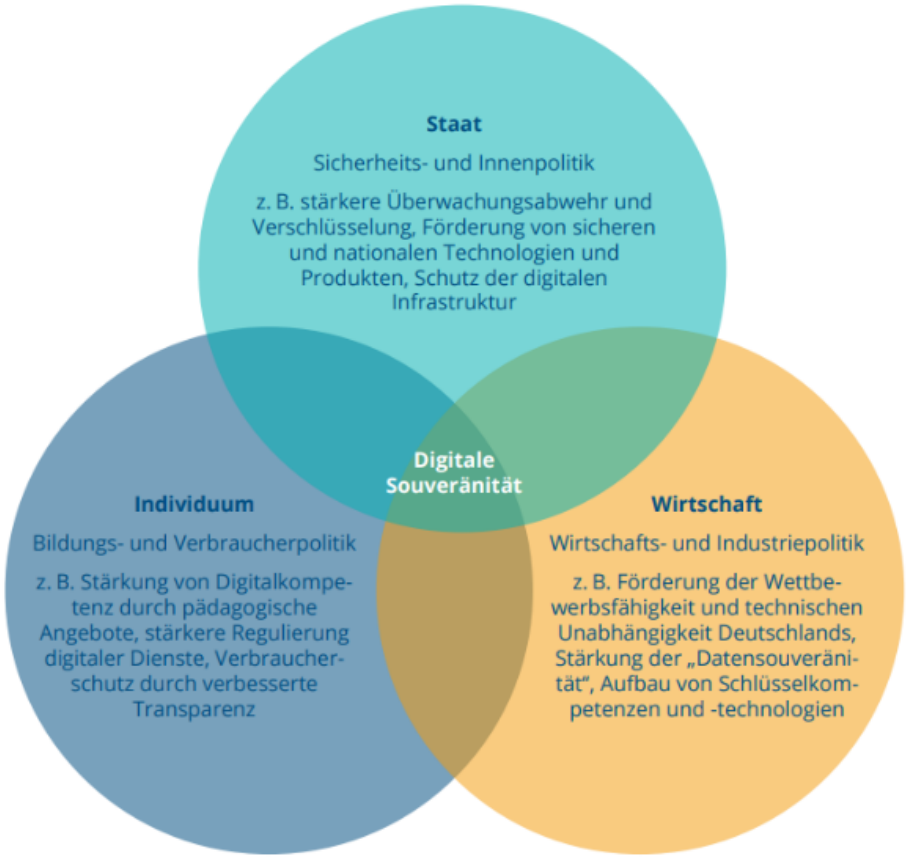
Witzel, A., & Reiter, H. (2022). *Das problemzentrierte Interview - eine praxisorientierte Einführung*. Beltz Juventa. https://katalog.ub.uni-heidelberg.de/cgi-bin/titel.cgi?katkey=69132355

Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. *Knowledge-Based Systems*, *216*, 106775.

Zillmann, M. (2021). *Der Markt für IT-Beratung und IT-Service in Deutschland - Marktstruktur, Trends Entwicklungen aus Sicht von IT-Dienstleistern und Anwenderunternehmen* (Lünendonk & H. GmbH, Hrsg.). Verfügbar 27. August 2025 unter https://www.datagroup.de/wp-content/uploads/2021/08/LUE_IT_Studie-2021_DATAGROUP.pdf

Anhang

Abbildung 1: Dimensionen digitaler Souveränität und Umsetzungsfelder



Mit freundlicher Genehmigung freigegeben durch Dr. Julia Pohle

Abbildung 1: Dimensionen digitaler Souveränität nach Pohle (2020)

Nr.	Jahr	Autor(en)	Titel	Zuordnung	Kurze Zusammenfassung	Perspektive
1.	2021	Pohle, Julia; Thiel, Thorsten	Digitale Souveränität - Von der Karriere eines einenden und doch problematischen Konzepts	Staat	**Herausforderungen** **-** Geopolitik: Rivalität zu China & USA - Wirtschaft: Grundsätze und Entwicklungsgeschwindigkeit im Bereich KI unterscheiden sich sehr **Maßnahmen** 1. Wirtschafts- & industriepolitischer Diskurs: Aufbau von Schlüsselkompetenzen so wie Software- und Hardware-Entwicklung, Fokus auf Cyber-Security, Big Data und Smart Data sowie Cloud-Diensten, Open-Source-Software 2. Rechtswissenschaftlicher Diskurs 3. Bildungs- und verbraucherpolitische Diskurs: Volkssouveränität erreichen durch ein stärkeres Selbstbestimmungsrecht (z.B.verbraucherorientierter Datenschutz, Stärkung der Digitalkompetenzen, Gleichbehandlung, Diversität, Toleranz und Wertschätzung) 4. Politischer Diskurs: öffentliche Sicherheit gewährleisten, gemeinsames, freies, offenes und sicheres globales Internet, kein Protektionismus, sondern vielmehr mehr Regelwerke für große Plattformunternehmen (Autoren nennen diese „Quasi-Souveräne") 5. Europäischer Diskus: Stärkung der Sicherheit digitaler Infrastrukturen und Technologien, Etablierung eines wettbewerbsfähigen europäischen Technologiesektors, strategische Allianzen, Anpassung an neue Technologien wie KI, Regulierung digitaler Angebote für Anbieter, rechtliche Rahmenbedingungen als strategisches Instrument, Ergänzung der Digitalstrategie 2020, „Verteidigung" europäischer Werte (Datenschutz und Individualrechte) ggü. chinesischer und US-amerikanischer Konkurrenz	Politik
2.	2020	Gabi Dreo, Volker Eiseler, Nils gentschen Felde, Wolfgang Gehrke, Udo Helmbrecht, Wolfgang Hommel und Julius Zahn	Europäische Digitale Souveränität: Weg zum Erfolg?–Ein Bericht zur Jahrestagung CODE 2020	Staat	**Strategische Perspektiven mit Fokus auf Verteidigungspolitik:** - Stärkung der europäischen Resilienz - Cybersicherheit als Enabler digitaler Souveränität - Zusammenarbeit von unterschiedlichen Akteuren (Forschung, Indistrie, öffentliche Institutionen und Start-Ups) - Aufbau eines digitalen Ökosystems (EU-Projekt CONCORDIA) - Aufbau eines europäischen Datenraums zur Wahrung mehr Privatsphäre und Datenschutz bei digitalen Identitäten - hohe Bedeutung von Verfügbarkeit vertrauenswürdiger IT für die Handlungsfähigkeit der Streitkräfte - Kooperation, Zusammenarbeit und Vertrauen ist wichtig für ein digital souveränes Europa - Schutz kritischer Infrastrukturen - Förderung vn Innovation - Förderung von digitalen Kompetenzen - Investments in Schlüsseltechnologien: Qantum Technologie	Verteidigung
3.	2020	Julia Pohle	Digitale Souveränität. Ein neues digitalpolitisches Schlüsselkonzept in Deutschland und Europa?	Staat, Unternehmen, Individuum	**Staat** Insbesondere Sicherheits- und Innenpolitik (z.B. stärkere Überwachungsabwehr und Verschlüsselung, Förderung von sicheren und nationalen Technologien und Produkten, Schutz der digitalen Infrastruktur) **Wirtschaft** Insbesondere Wirtschafs- und Industriepolitik (z.B. Förderung der Wettbewerbsfähigkeit und technischen Unabhängigkeit Deutschlands, Stärkung der Datensouveränität, Aufbau von Schlüsselkompetenzen und - technologien) **Individuum** Insbesondere Bildungs- und Verbraucherpolitik (z. B. Stärkung von Digitalkompetenz durch pädagogische Angebote, stärkere Regulierung digitaler Dienste, Verbraucherschutz durch verbesserte Transparenz)	Politik
4.	2017	Stephanie Christmann-Budian, Johannes Geffers	Wie Zuhause so im Cyberspace? Internationale Perspektiven auf digitale Souveränität	Staat, Wirtschaft, Individuum	**Staat** - Mehr Daten, weniger Vertrauen in Statistik --> Nutzer müssen lernen, wie sie - Fake News besser erkennen können - Internationale Perspektiven auf digitale Souveränität --> Partizipation und Artikulation im Sinne der zu stützenden Meinungsfreiheit und Demokratisierung, mehr Sicherheit, erweiterte Möglichkeiten der staatlichen Einflussnahme, Pluralisierung politischer, transnationaler Akteure, Sicherung des nationalen Wohlstands, verbesserte Kommunikationsmöglichkeiten, stärkere Rechtwissenschaft und -sichtbarkeit - Bildung als Voraussetzung digitaler Souveränität --> Forschungskompetenzen, Arbeitskompetenzen, Medienkompetenzen, Sozialkompetenzen, Problemlösekompetenzen + forschungsbasiertes Lernen, problembasiertes Lernen, arbeitsbasiertes Lernen **Unternehmen** - Bereiche mit großem Potenzial für den Standort Deutschland: Energieeffizienz, Elktromobilität, Batterie-/Speichertechnologie, Smart Grid, Industrie 4.0, Smart Traffic, Smart Car, IT-Sicherheit, IoT, Robotik, schnelles Internet, Smart Home, Big Data Aalytics, Cloud Computing, Wearables **Bürger** - Medien- und informationstechnische Kompetenz stärken, wissenschaftlich-technische Arbeiten zur Enttarnung und Kennzeichnung fördern - Digitale Partizipation in Wissenschaft und Wirtschaft --> Kollaboration, Open Acess, Transparenz fördern *Von digitaler zu soziodigitaler Souveränität* --> Selbstbestimmung in der Datenwelt, Kompetenz durch Erfahrung, Identität entfalten, das große Ganze mitgestalten	Innovations-management

Tabelle 1: Google Scholar Suche »digitale Souveränität«

5.	2016	Michael von Foerster	Digitale Souveränität ist möglich	Staat, Wirtschaft, Individuum	**Politik** - Medienkompetenz, Zurückgewinnung der Netzneutralität, Verantwortung & Vertrauen, Verschlüsselung, Qaulitätsmedien	Sozial- und Rechts-wissenschaften
6.	2016	Thomas Jarzombek, Peter Bisa	Digitale Souveränität–nur ein Faktor für einen Wirtschaftsstandort Deutschland in Zeiten der digitalen Transformation	Staat, Wirtschaft, Individuum	**Wirtschaft** - Anpassung der digitalen Standortpolitik, Förderung der Gründungskultur als Basis für digitale Souveränität **Gesellschaft** - Digitale Bildung	Sozial- und Rechts-wissenschaften
7.	2016	Marco Zingler	Gründungskultur im digitalen Bereich als Basis für digitale Souveränität	Staat, Wirtschaft	**Juristische Ebene** - Meinungsfreiheit und Persönlichkeitsrecht (Wirtschaftsfreiheit, Datenschutz) + Entwicklungen von Big Data mit Grundsätzen des Datenschutzrechts **Kulturelle Ebene** - Digitale Souveräbnität als Bedürfnis, Gewöhnung, Engagement	Sozial- und Rechts-wissenschaften
8.	2019	Fokusgruppe - Digitale Souveränität und Künstliche Intelligenz	Digitale Souveränität in einer vernetzten Wirtschaft	Wirtschaft	**Politik und Verwaltung** - Schaffung investitionsfreundlicher und -fördernder Rahmenbedingungen - Errichtung eines echten Level-Playing-Fields auf europäischer Ebene, so dass wettbewerbsfähige europäische Angebote entstehen können - Kontroll- und Innovationsfähigkeit sichern - Cloud-Angebote bevorzugen - Datenstrategie erstellen - Forschungsförderung - Aufbau leistungsfähige KI-Forschung und Innovationscluster (z.B. Design-Prinzip für KI-Entwicklung verstetigen) - digitale Kompetenzen bei Menschen ausbauen **Wirtschaft** - Wirtschaft muss Aufklärung der Öffentlichkeit intensivieren - verstärkt in Infrastruktur, Forschung und Entwicklung & in (Weiter-)Bildung investieren - Daten- und Analyseinfrastruktur focieren **Wissenschaft und Forschung** - Kontinuierliches Technologie-Monitoring (mit möglichst konkreten Angaben über Einsatzgebiete und möglichen wirtschaftlichen Nutzen), - Aufbau von Technologiekompetenzen durch Grundlagen- und Anwendungsforschung	Politik, Forschung, Technik
9.	2018	Dirk Fox	Digitale Souveränität	Staat, Wirtschaft	**Maßnahmen auf Anbieterseite** - Regulatorische Chancengleichheit europäischer IT-Unternehmen - einheitliche Gesetzgebung - gezielte Forschungsförderung von Digitaltechnik **Maßnahmen auf Nutzerseite** - Umgang mit digitaler Technik - Wahlfreiheit für den Nutzer - Datenportabilität **Sonstige Maßnahmen** - Kompetenz und Verständis festigen - Security by Design - Privacy by Default - Datensparsamkeit - neue Zertifizierungsverfahren	Informatik
10.	2019	Thomas Schauf, Thomas Bendig, Philipp Ehmann, Pablo Mentzinis, Max Pfeifer, Jörg Bienert, Peter Ganten, Thomas Mosch, Thomas Dapp, Pamela Krosta-Hartl, Rahild Neuburger, Fabian Zacharias	Digitale Souveränität im Kontext plattformbasierter Ökosysteme	Staat, Wirtschaft, Individuum	**Anforderungen an Technologie- und Marktrahmen** - Hard- und Software-Souveränität - Souveränität hinsichtlich der Plattformumgebung - Datensouveränität (Daten unter eigener Kontrolle) - Ermöglichung von föderierten Plattformen **Anforderungen an den Marktrahmen** - Netzwerkeffekte und First-Mover-Vorteile nutzen - Kooperationen mit Wettbewerbern eingehen - Datenzugang schaffen - Kapitalisierung (Wachstumspotenzial, vor allem für junge Unternehmen) **Anforderungen an einen souveränen Marktort Europa** 1. Regulierungsrahmen: Stärkung der europäischen Anbieterlandschaft – Marktortprinzip ausbauen, Datensouveränität als Enabler für Plattformen „made in Europe“, Interoperabilität fördern und Marktortprinzip stärken, Erleichterung von Kooperationsmodellen mit Wettbewerbern, Missbrauch begegnen und Datenportabilität sowie Interoperabilität, Verbesserung des Datenzugangs einfordern 2. Förderung und Projektentwicklung: F&E-Förderung für verteilte und föderierte Plattformen, Trennung technischer und wirtschaftlicher Betreiber, Förderung von „Standards made in Europe“, Projekte der öffentlichen Hand mit Vorbildcharakter, Entwicklung der erforderlichen Kompetenzen,	Politik

Tabelle 2: Google Scholar Suche »digitale Souveränität«

11.	2020	Luciano Floridi	The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU	Staat, Wirtschaft	**Begriffsverständnis digitaler Souveränität** - britische Regierung hat Herausforderung 2020 eine Coronavirus-App zu entwickeln, ohne auf Google-APIs zurückzugreifen - Google und Apple können jedoch die Daten über die Covid-19-App auf die jeweiligen Kontakte zurückführen, was datenschutzrechtlich als sehr kritisch einzustufen ist **Umsetzung digitaler Souveräniät** - hybride Idee eines teilweise vernetzten Netzes: Volkssouveränitäten, die über Knotenpunkte supranationale Souveränitäten legitimieren (wenn das erfolgreich gestaltet wird, könnte dieses Gefhlecht aus individuellen, nationalen und supranationalen Souveränitäten innovative Flexibilität und demokratische Legitimation vereinen)	Philosophie/ Technologie
12.	2016	Viviane Reding	Digital Sovereignty: Europe at a Crossroads	Staat	**Beendigung der Rechtszersplitterung - die Fähigkeit, unsere eigenen Normen zu bestimmen** - Wir müssen sicherstellen, dass Europa bei der Festlegung von Gesetzen und Normen für das digitale Zeitalter ein Mitspracherecht hat. **Hochgeschwindigkeitsinfrastruktur - ein Baustein des digitalen Kontinents** - Dies wird nur möglich sein, wenn es geschlossen auftritt und eine klare Strategie verfolgt, die durch die notwendigen finanziellen Mittel unterstützt wird. **Schlussfolgerung: Europa befindet sich heute an einem Scheideweg.** - Wir können unsere europäische Souveränität nutzen, um im Bereich des Datenschutzes und darüber hinaus Standards zu setzen.	Politik
13.	2017	Reinhard Posch	Digital Sovereignty and IT-Security for a Prosperous Society	Staat, Wirtschaft	**Push-Benachrichtigungen** - Es ist ein Problem, dass Push-Benachrichtigungen nicht angepasst wurden, nachdem sie im Zusammenhang mit der Souveränität und der grenzüberschreitenden Nutzung von Rechtsordnungen geprüft worden waren - Wir stellen weiterhin fest, dass Anwender nicht kontrollieren können, was hierbei mit ihren Daten passiert **Cloud-Speicher** - Wenn es um selnsible Daten in der Cloud und sensible Daten geht, dann stellen wir fest, dass abgefangene Daten zum Wettbewerbsvorteil von privaten Akteuren genutzt werden - Es gilt diese Situation nicht nur in der Industrie, sondern auch für Regierungen zu verbessern **Zuständigkeitsbewusste IT und Kommunikation** - Es besteht die Notwendigkeit, es privaten und beruflichen Nutzern einfacher zu machen, ein hohes Maß an Schutz vor Datenklau zu ermöglichen **Mobile Verbindungen umschalten** - Identitätsmanagement für Betreiber mit Roaming und Rekonfiguration einführen und dieses zur Geräteverwaltung hinzuzufügen, um eine effiziente Kontrolle durch den Nutzer zu ermöglichen **Dokumentenzusammenarbeit** - Aus Sicht der Souveränität wären die grundlegenden Anforderungen: eID als Basis zur Gewährleistung von Verfügbarkeit und Validierung aktiver Elemente, verschlüsselte Zusammenarbeit auf Basis verschlüsselter statische Daten	Informatik
14.	2019	Stephane Couture, Sophie Toupin	What does the notion of "sovereignty" mean when referring to the digital?	Wirtschaft	**Digitale Souveränität als umstrittener Begriff** - Digitale Souveränität wird in vielen Beiträgen als kollektiver Kontrollversuch verstanden, über digitale Infrastrukturen oder digitale Inhalte zu herrschen - Wir stellen aber an verschiedenen Stellen unterschiedliche, teils divergente Interpretationen, Themen und Definitionen digitaler Souveränität fest	Medienwissenschaft
15.	2015	Francesca Bria	Public policies for digital sovereignty	Staat, Wirtschaft	**Öffentliche Politik** - Barcelona, auf dem Weg zu einer demokratischen, gemeinwohlorientierten Stadt unter dem Deckmantel digitaler Souveränität - Rekommunalisierung von Netzinfrastrukturen und gemischtes öffentliches/gemeinschaftliches Eigentum - Datenpolitik und Eigentumsregelungen rund um Daten - Missionsorientierte Politik und alternative Modelle für Innovation	Betriebswirtschaft
16.	2021	Luca Belli	BRICS countries to build digital sovereignty	Staat, Wirtschaft	**Gestaltung digitaler Souveränität für Indivduen** - Positiven Kreislauf aus Forschung und politischen Vorschlägen anregen - Einrichtung eines BRICS-Kooperationsmechanismus zur Förderung kompatibler digitaler Strategien	Technologie, Gesellschaft
17.	2020	Jane Müller, Mareike Thumel, Katrin Potzel, Rudolf Kammerl	Digital Sovereignty of Adolescents	Individuum	**Umfrage zum individuellen Status digitaler Souveränität bei Jugendlichen** - Die Ergebnisse zeigen, dass die meisten Jugendlichen nur eine vage Vorstellung von ihren eigenen Datenspuren und deren Nutzung haben - Nur eine kleine Anzahl von Schülern (N=7) wiesen ein außergewöhnliche tiefgreifendes Verständnis zu digitalen Medien aus.	Medienwissenschaft
18.	2021	Simona Autolitano and Agnieszka Pawlowska	Europe's quest for digital sovereignty: GAIA-X as a case study	Staat	**Definition der europäischen digitalen Souveränität** - Der Aufstieg der souveränen Cloud in Europa - GAIA-X: Ein praktischer Ansatz für europäische digitale Souveränität	Informatics

Tabelle 3: Google Scholar Suche »digital sovereignty«

19.	2021	Paola Pierri, Bianca Herl	Exploring digital sovereignty: open questions for design in digital healthcare	Individuum	**Verständnis digitaler Souveränität** - neue Formen digitaler Ungleichheiten - digitale Souveränität basiert auf Prinzipien der Gerechtigkeit bei der Entwicklung von digitalen Lösungen - Autonomie, Unabhängigkeit und Kontrolle für die Nutzer dieser Lösungen **Maßnahmen** - stärkere Sensibilisierung - aktuive Rolle von Designern bei der Gestaltung digitaler Kompetenzen - Entwicklung einer entsprechenden Version, wie man Daten kontrollieren will	Design Forschung
20.	2018	Sarah Mckune, Shazeda Ahmed	Authoritarian practices in the digital age| the contestation and shaping of cyber norms through China's internet sovereignty agenda	Staat	**Internet-Souveränität in China** - Entwicklung des chinesischen Konzepts der Internet-Souveränität vor 2013 - Veränderungen in Chinas Strategie der Internet-Souveränität nach 2013 - Entstehung von Normen rund um digitale autoritäre Praktiken **Anfechtung und Verbreitung der Internet-Souveränitätsagenda** - Durch die Shanghaier Organisation für Zusammenarbeit - Durch den Wuzhen-Prozess **Bewertung der Internetsouveränität aus einer internationalen Rechtsperspektive** - eine Dimension der Regierungsführung - eine Dimension der nationalen Verteidigung - eine Dimension der internen Einflussnahme.	Kommunikation
21.	2014	Norbert Pohlmann, Michael Sparenberg, Ilya Siromaschenko, Kilian Kilden	Secure Communication and Digital Sovereignty in Europe	Staat, Wirtschaft	**Das Internet unter dem Gesichtspunkt der Infrastruktur** -Trends, Bedrohungen und Gegenmaßnahmen - "Schengen-Netz": Simulation eines eingeschränkten Routing-Modells für Europa - Aufbau eines Datenmodells für die Routing-Analyse - Kryptographie als alternativer Ansatz zur Verbesserung der Sicherheit - IPSec-Verschlüsselung - SSL/TLS-Verschlüsselung - Vertrauenswürdige IT-Sicherheitstechnologien und -dienste	Internet Sicherheit
22.	2021	Martin Kaloudis	Digital Age–How Can We Measure Digital Sovereignty and Support the EU's Action Plan?	Staat	**Bildung eines Indexes für digitale Souveränität wird vorgeschlagen** - Souveränität = θn = Θ + ≡, Θ = η, ≡ = β1 + β2 + β3 + β4 + β5 + β6 + λ (1) für einen Staat n - Dieser Index basiert auf einem quantitativen Beschreibungsmodell ist der sogenannte World Governance Indicator (WGI) - Der Index muss wissenschaftlich weiter ausgearbeitet werden, um anwendbar zu sein	Business and Economics
23.	2022	George Metakides	A Crucial Decade for European Digital Sovereignty	Staat, Wirtschaft	**Verständnis digitaler Souveränität** - Fairness für Daten, Algorithmen und Potenzialprüfung der digitalen Technologien - Nutzung von Potenzial digitaler Technologien, die ungerechte Behandlung von Menschengruppen zu vermindern. **Platform Power** - die EU muss sich unabhängiger aufstellen von Megaplattformen wie Twitter, Google, Facebook (sie haben eine wichtige Rolle in der Pandemie gespielt und haben Auswirkungen auf bestimmte Branchen und deren Geschäftsmodelle) **Bildung und Qualifikationen** - Lernen durch Krisen, Realisierung von „digital Humanism", Gestaltung von Systemen auf Basis einer Strategie „Zukunft für Arbeit" unter Berücksichtigung von Veränderungen durch die digitale Welt	Digitaler Humanismus
24.	2019	Przemysław Roguski	Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment	Staat	**Kartierung der Souveränitätsebenen auf den Ebenen des Cyberspace** 1) Basissouveränität - Ausschließliche Autorität des Territorialstaats über IKT-Komponenten der physischen Schicht 2) Begrenzte Autorität über die logische Schicht 3) Konkurrierende Souveränität über Daten, die sich IKT-Infrastruktur in einem anderen Staat befinden	Recht
25.	2018	Stéphane Couture and Sophie Toupin	What Does the Concept of'Sovereignty'Mean in Digital, Network and Technological Sovereignty?	Wirtschaft	**Souveränitätsdimensionen von digitale und Netzwerksouveränität** 1) Staatliche und nationale technologische Souveränität 2) Soziale Bewegungen und technologische Souveränität 3) Indigene technologische Souveränität 4) Persönliche technologische Souveränität, und 5) Technologie als Mittel zur Souveränität.	Kommunikations-wissenschaft

Tabelle 4: Google Scholar Suche »digital sovereignty«

26.	2021	Hannes Werthner	Geopolitics, Digital Sovereignty… What's in a Word?	Staat	**Beschreibung potenzieller Ziele digitaler Souveränität** - Das größte Bruttoinlandsprodukt der Welt und ein Markt von 500 Millionen Menschen - Führend in mehreren Bereichen (z. B. Luftfahrt, Kryptographie, Banken, Automobilhandel) - Eine sehr dynamische KMU-Szene - F&E und intellektuelles Kapital - Hochwertige Konnektivität und Netzwerke (Verkehr, Energie, Telekommunikation) - Kulturelle Vielfalt und eine Charta der Grundrechte	Geopolitik
27.	2020	Edoardo Celeste	Digital sovereignty in the EU: challenges and future perspectives	Staat, Wirtschaft	**Maßnahmen für Europa zur Stärkung digitaler Souveränität** - Die europäische DNA bewahren - Initiativen der Mitgliedstaaten und der Union nutzen - Das Risiko des digitalen Souveränismus berücksichtigen	Recht/ Verwaltung
28.	2021	Ciaran Martin	Geopolitics and Digital Sovereignty	Wirtschaft	**Wesentliche Einflussfaktoren für digitale Souveränität** - Grundwerte ändern sich - Digitalisierung schreitet weiter voran - das internationale Systems erfordert Agilität **Vorschlag zum Umgang mit den Einflussfaktoren** - Kultur tech-Diplomatie könnte ein erfolgreicher Vorschlag sein, der den Weg für die Zukunft der internationalen Beziehungen im digitalen Zeitalter ebnet.	Geopolitik
29.	2016	Dr. Simon Scerri	Industrial Data Space–Digital sovereignty over data	Wirtschaft	**Digitale Souveränität in der Industrie** - Daten als Bindeglied zwischen der "Smart Service Welt" und "Industrie 4.0" Daten als Wirtschaftsgut - industrieller Datenraum notwendig für ausgewählte Anwendungsfälle, z.B. Lkw- und Frachtmanagement in der Inbound-Logistik, Entwicklung von medizinischen und pharmazeutischen Produkten, Kollaboratives Management von Produktionsanlagen, End-to-End-Überwachung von Waren während des Transports - Struktur und Organisation dieses industriellen Datenraums: Forschungsprojekte vorantreiben, Anwender des industriellen Datenraums zusammenführen, Kooperationen fördern	Informationssysteme für Unternehmen
30.	2021	Henning Kagermann, Karl-Heinz Streibich, Katrin Suder, Florian Sussenguth	Digital Sovereignty: Status Quo and Perspectives	Staat	**Das Technologie-Schichtenmodell** - Europäisches System der Gesetze und Werte - Software-Technologie - Europäische Datenräume - Plattform-as-a-Dienst (PaaS) - Infrastruktur-as-a-Service (IaaS) - Kommunikations-Infrastruktur - Komponenten - Rohstoffe und Zwischenprodukte **Komponenten/ Fokus** - Cybersecurity (cryptography, e-Identität, - EU Zertifikate und Standards) - App-Entwicklung (Office, ERP, AI, - middleware, robotics software, blockchain, algorithms, EU open source, VR/AR, QC) - Mobilität, Gesundheit, öffentlicher Sektor - Applikationen und Entwicklungs-Ökosysteme - Virtuelle distributed Could-Ökosysteme, Edge Technologie - Beitbrand-Infrastuktur, Mobilfunk-Netze, Gelileo Navigation - Mikrochips, Sensoren. Altprem. etc - Seltene Erdelemente	Technologie
31.	2018	Beniamin Shakhnazarov	Territorial principle of intellectual property protection and the effect of state sovereignty in the digital space	Staat, Individuum	**Territoriale Anstrengungen im digitalen Raum in Russland** - Russische Anstrengungen zur Wahrung des geistigen Eigentums - genaue Analyse der Auswirkungen der staatlichen Souveränität im digitalen Raum	Recht

Tabelle 5: Google Scholar Suche »digital sovereignty«

32.	2021	Liaropoulos Andreas	EU Digital Sovereignty: A Regulatory Power Searching for its Strategic Autonomy in the Digital Domain	Wirtschaft	**Ziel: politische Dilemmata aufzeigen, mit denen die EU konfrontiert ist** - Stärkung der diplomatischen Diplomatie - Verbesserung der Cyberresilient - Der Aufbau einer starken technologisch-industriellen Basis - Stärkung technologischer Wettbewerbsfähigkeit in Europa - strategische Vision notwendig **Aus einer Cyber-Kriegsführungs-Perspektive** - Entscheidung zwischen Kartellpolitik, Datenlokalisierung und dem Risiko eines Datenkriegs bzw. Technologiekriegs mit China oder den USA - EU muss seine Schwachstellen erkennen und sollte Risiken bewerten, die mit einer digitalen Festung verbunden sind	Cyber-Kriegsführung und Sicherheit
33.	2020	Willem Gravett	Digital neo-colonialism: The Chinese model of internet sovereignty in Africa	Individuum	**Internet Souveränität** - China ist aktiv beteiligt an der Neugestaltung von Freiheit, Sicherheit und Offenheit im digitalen Raum - Afika ist aufgerufen, die Technologien Chinas kritisch zu bewerten - Afrika und die EU müssen damit einstehen für eine Gesellschaft, die sie sich wünschen im Gegensatz zu der Internetsouveränität, die die Chinesen vorschlagen **Die Rolle der EU (zwischen China un Afrika)** - die EU sollte den rechtlichen und politischen Rahmen dieser Debatte bestimmen - sie sollten dafür sorgen, von der Konzeption, bis zur Umsetzung einer Technologie Berücksichtigung zu finden - die Konzeption über die Entwicklung von Technologien ist ebenfalls entscheidend	Recht
34.	2020	Pohle, Julia	Digital sovereignty. A new key concept of digital policy in Germany and Europe	Staat	**Ableitung von Ebenen, in denen digitale Souveränität Anwendung findet (aufgrund des unterschiedlichen Begriffsverständnisses besonders auf politischer Ebene)** - Ebenen, innerhalb derer eine Stärkung digitaler Souveränität angestrebt wird: Staat, Wirtschaft und Individuum. - Hier gibt es erhebliche Interessens-, und Zielkonflikte, die sich teilweise nicht auflösen lassen **Anforderungen an digitale Souveränität:** - strategischere und ganzheitlichere Digitalpolitik: politischer Wille der EU, konzeptionelle Arbeit und politischen Wille ein demokratisches und liberales Verständnis von Souveränität umzusetzen	Sozialwissenschaft
35.	2021	Alexandru Circiumaru	The EU's Digital Sovereignty-The role of Artificial Intelligence and Competition Policy	Staat	**Erreichung digitaler Souveränität durch KI-Politik und Wettbewerbspolitik** - größte Herausforderungen: Kohärenz der beiden Ebenen gewährleisten.	Europäische öffentliche Politik
36.	2021	Bianca Herlo, Daniel Irrgang, Gesche Joost, Andreas Unteidig	Practicing Sovereignty: Digital Involvement in Times of Crises	Staat, Wirtschaft, Individuum	**Prototyping digitaler Souveränität** - ein gemeinsames Verständnis für eine kollektive Souveränität aufbauen - souveräne Imaginäre der Unternehmen für politische Praktiken berücksichtigen - - Handlungsfähigkeit gewährleisten und gleichzeitig Privatsphäre - Den Staat als wichtigen Akteur bei der Gestaltung von Netzwerktechnologie und des Dateninfrastrukturraums inkludieren - die Bedeutung feministischer Digitalpolitik verstehen	Medienwissenschaft
37.	2021	Sergey Volodenkov, Alexander Voronov, Lidia Leontyeva, Maria Sukhareva	Digital sovereignty of a modern state in the context of technological transformations: content and features	Staat, Wirtschaft, Individuum	**Verständnis digitaler Souveränität** - komplexes System, das die Eigenschaften digitaler Infrastruktur des Staates mit Fähigkeiten und Möglichkeiten vereint - Fokus sind dabei die Fähigkeiten und Möglichkeiten von sozialen, administrativen, politisch-öffentlichen, wirtschaftlichen Institutionen sowie von Bürgern - Ziel ist eine unabhängigere Nutzung von Daten und digitalen Technologien durch den Staat und seine Institutionen zur Erreichung nationaler Ziele	Öffentliche Politik/ Wirtschaft/ Verwaltung/ Innovation
38.	2020	Theodore Christakis	European Digital Sovereignty': Successfully Navigating Between the'Brussels Effect'and Europe's Quest for Strategic Autonomy	Staat	**Verständnis digitaler Souveränität** - Souveränität als strategische Autonomie und Regelungsbefugnis - Fähigkeit, im digitalen Markt zu handeln und gleichzeitig nicht zu stark durch externe Abhängigkeiten eingeschränkt zu sein **Handlungsempfehlung ist die Vereinigung von Gesetzgebungsvorschlägen (wie den Data Governance Act) und aktuellen Debatten zu digitalen Themen** - internationaler Datentransfer - 5G-Einführung - Cybersicherheitsbedenken - Regulierung künstlicher Intelligenz - Zugang ausländischer Regierungen zu Daten - die Gestaltung von Cloud Computing - Steuer auf digitale Dienste - Wettbewerbsrecht	Internationales Recht

Tabelle 6: Google Scholar Suche »digital sovereignty«

39.	2021	Anke S. Obendiek	Take back control? Digital sovereignty and a vision for Europe	Staat	**Eine Vision für Europa** Unterstützung der Schaffung von Technologien und Infrastrukturen mit „Werten durch Design" Vollständige Entwicklung und Verpflichtung auf die normative Agenda der EU	Politik
40.	2020	James A. Lewis	Digital Sovereignty in a Time of Conflict	Wirtschaft	**Ziel digitaler Souveränität** - Verteidigung des Internets als Raum für Individuen zu handeln - Dimensionen: Daten, Sprache, Innovation **Maßnahmen für digitale Souveränität** - Einführung eines Mechanismus zur Steuerung von Maßnahmen digitaler Souveränität, um Ineffizienzen durch zu viel Verantwortungsdiffusion zu verringern - die UN, die als Möglichkeit für eine solche Steuerungsinstanz in Frage kommen könnte, steckt selbst in der Krise	Strategische und internationale Studien
41.	2021	Johannes Thumfart	The COVID-Crisis as Catalyst for the Norm Development of Digital Sovereignty. Building Barriers or Improving Digital Policies?	Staat	**Arten der Souveränität** 1) digitale Souveränität 2) technologische Souveränität 3) Internetsouveränität 4) Datensouveränität 5) Netzsouveränität 6) Informationssouveränität 7) souveränes Internet	Rechtswissenschaft/ Technologie/ Gesellschaft
42.	2020	FRANCES G. BURWELL AND KENNETH PROPP	The European Union and the Search for Digital Sovereignty	Staat	**Beweggründe für digitale Souveränität** - chinesishce und amerikanische Unternehmen dominieren den Digitalmarkt in Europa und sind als eigenständige Akteure kaum zu steuern - Europäer konsumieren größtenteils amerikanische Clouddienste - Definition digitaler Souveränität fällt schwer **Ableitende Überlegungen** - Neue Definition von Souveränität nach der Covid-Krise notwendig - EU-Investitionen in digitale Märkte müssen erhöht werden (Investitionen in China oder den USA sind deutlich höher) - Schlüsselsektoren der europäischen Wirtschaft fördern	Politik
43.	2020	Nicola Fabiano	Digital Sovereignty Between "Accountability" and the Value of Personal Data	Individuum	**Notwendige Faktoren, die es für mehr digitale Souveränität zu berücksichtigen gilt** - Rechenschaftspflicht nach GDPR - Wert persönlicher Daten nach der Datenschutz-Grundverordnung - Rechenschaftspflicht quantifizieren/ Stand von Maßnahmen bewerten	Forschung/ Technologie
44.	2019	Atilla Aydın. Türksel Kaya Bensghir	Digital Data Sovereignty: Towards a Conceptual Framework	Wirtschaft	**Die vorgeschlagenen technischen Lösungen für die digitale Datensouveränität sind im Folgenden kurz aufgeführt:** - Nationaler E-Mail-Dienst: Durchführung lokaler E-Mail-Dienste und der gesamten E-Mail-Korrespondenz über Server innerhalb des Landes - Neue Transitkabel: Neue Transit-Glasfaserleitungen zwischen Ländern, Regionen und Kontinenten - Internet-Leitweglenkung: Leitung und Lenkung des inländischen Datenflusses in einem geografisch begrenzten Gebiet - Nationaler Cloud-Speicher: Implementierung von privaten und öffentlichen Lösungen für Cloud-Speicherdienste - Verschlüsselungstools: Bessere Verschlüsselung der Ende-zu-Ende-Kommunikation	Unternehmen/ digitale Tranformation
45.	2020	André-Yves Portnoff	Sovereignty in the digital era	Staat	Innovationen in der Weltwirtschaft werden größtenteils durch Tencent, Baidu, Amazon, Facebook und Amazon gestaltet **Digitale Souveränität und Innovation** - Bedeutung innovativer kleiner und mittlerer Unternehmen für die Wirtschaft eines Landes **Mögliche Maßnahme** - aktive öffentliche Unterstützung ihrer Entwicklung und ihres Wachstums	Digital Transformation
46.	2020	Karola Marky	Privacy-Sovereign Interaction: Enabling Privacy-Sovereignty for End-Users in the Digital Era	Individuum	**Konkrete Vorschläge aus der Informatik für mehr digitale Souveränität** (1) *Stärkerer Schutz privater Daten durch 2-Faktor-Authentifizierung:* Erarbeiung, Umsetzung und Nutzung einer 2-Faktor-Authentifizierung auf Basis eines 3-D-Objekts, das zur mobilen Anwendung genutzt wird (2) *Verifizierung von Daten:* kryptografische Protokolle werden kategorisiert und in einer Nutzerstudie evaluiert. Die best bewertetsten werden genauer analysiert. (3) *Persönliche IoT-Daten:* Konzept zum Schutz der Privatsphäre wird vorgestellt und evaluiert, das auf Wahrnungen der Nutzer basiert	Informatik

Tabelle 7: Google Scholar Suche »digital sovereignty«

47.	2020	Didier Danet, Alix Desforges	Digital sovereignty and strategic autonomy in Europe: From concept to geopolitical reality	Staat	**Digitale Souveränität und Geopolitik** - geopolitische Herausforderungen - Bedeutung des strategischen Ziels - industrielle Bedingungen zur Umsetzung digitaler Souveränität	Geografie/ Geopolitik
48.	2020	Gregory Rolan, Sue McKemmish, Gillian Oliver, Joanne Evans, Shannon Faulkhead	Digital equity through data sovereignty: A vision for sustaining humanity	Wirtschaft, Individuum	**Datensouveränität und Menschenrechte** - Betrachtung von Menschenrechten bei der Erreichung von Datensouveränität durch sicherere und intelligente Informationstechnologien - historische und soziale Gerechtigkeit im Datenraum - Umgang mit Menschenrechtsverletzungen im digitalen Raum - Identitäten, Beweise für Rechenschaftspflichten	Technologie
49.	2021	Mihajlo VUČIĆ	EUROPEAN UNION'S QUEST FOR DIGITAL SOVEREIGNTY: POLICY CONTINUATIONS AND STRATEGY INNOVATIONS	Staat, Wirtschaft	**Ziel digitaler Souveränität** - Macht der EU weiter ausbauen - ein drittes Modell zwischen China und den USA etablieren **Maßnahmen** - Weitere Förderung von föderierten Cloud-Infrastruktur-Vorhaben in Europa (Gaia-X) - Datenfluss über Binnengrenzen hinweg begrenzen - nur eine stärkere Einigung der Mitgliedstatten wird die Strategie zum Erfolg führen	Internationale Politik
50.	2020	Tambiama Madiega	Digital sovereignty for Europe	Staat, Wirtschaft, Individuum	**Handlungsempfehlungen für Europa** 1. Europäische Cloud- und Dateninfrastruktur 2. EU-Rechtsrahmen für Daten 3. Mehrjähriger Finanzrahmen und digitales Europa 4. Öffentlich-private Partnerschaften in den Bereichen KI, Daten und Robotik 5. Groß angelegter EU-Rahmen für die Forschungszusammenarbeit 6. Überprüfung der Datenschutz-Grundverordnung 7. Datenschutzrichtlinie für elektronische Kommunikation (e-Privacy) 8. Festlegung einer obligatorischen EU-weiten Cybersicherheitszertifizierung 9. Förderung der Koordinierung der Cybersicherheit auf EU-Ebene 10. Überarbeitung der NIS-Richtlinie 11. Normung für 5G und darüber hinaus 12. Normung im IoT 13. Transparenz der Entscheidungssysteme 14. EU-Rahmen für den Einsatz von Gesichtserkennungstechnologie 15. EU-Produktsicherheits- und Haftungsregelung 16. Richtlinie über den elektronischen Geschäftsverkehr (Gesetz über digitale Dienstleistungen) 17. Koordinierte Umsetzung der EU-Vorschriften für das öffentliche Auftragswesen 18. Neues Instrument zur Bewertung von Übernahmen von EU-Hochtechnologieunternehmen 19. Einrichtung einer EU-Taskforce für strategische Industrien und Technologien 20. EU-Rahmen für digitale Besteuerung 21. EU-Rahmen für die digitale Besteuerung 22. Kontrolle digitaler Torwächter 23. Offene digitale Ökosysteme fördern 24. Governance-Mechanismen und Koordinierung zwischen digitalen Regulierungsbehörden	Europäische parlamentarische Forschung
51.	2021	Rina Dwihana Fitriani	DIGITAL DIPLOMACY AND CYBER SOVEREIGNTY IN 10 CARIBBEAN ISLANDS COUNTRIES (Comparison of Indonesia and 10 Countries in the Caribbean Islands)	Staat, Wirtschaft	**Best Pracitices für digitale Souveränität auf Basis anderer Nationen** - Ein Beispiel an den britischen Jungerninseln nehmen: haben den höchsten Grad an Sicherheit für ihre Cyber Infrastruktur - Ein Beispiel an Aruba nehmen: sie vereinen die regelbasierten Vorgaben aus der diplomatischen Welt mit der digitalen Welt am besten - Ein Beispiel an Anguilla/Aruba nehmen: sie besitzen die höchste Kernsouveränität,	Sozialwissenschafte n/ Psychologie
52.	2021	Januar Arief Martharaharja	National Defense Model Based On Data Sovereignty: Strategy To Overcome Threats In Digital Era	Staat, Wirtschaft	**Formulierung eines Konzepts für mehr Cyberverteidigung** - Förderung der Transparenz über Datenverarbeitungsaktivitäten - Bildung repräsentativer Datenagenten, die den Datenfluss entsprechend den individuellen Präferenzen verwalten - Erkundung von Dateneigentum - Erhöhung der Datenkompetenz	Technologie

Tabelle 8: Google Scholar Suche »digital sovereignty«

53.	2020	Carla Hobbs	Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry	Staat, Wirtschaft	**Der euorpäische Weg zu mehr digitaler Souveränitä** - Multi-Stakeholder-Ansatz zur Internetregulierung - Einsatz von Richtern, die die Komplexität von Herausforderungen bei der Internetregulierung durchdringen können - ausreichend mit Informationen ausgestattene politische Entscheidungsträger - Inklusion der europäischen Tech-Gemeinschaft - Miteinbeziehung von Unternehmen, da sie diejeigen sind, die den größten Teil digitaler Infrastruktur verwalten und besitzen - Regierungsbehörden, die Grenzen setzen/ Unternehmen, die Regeln für sich festlegen - Politik muss Anreize für die Rechenschaftspflicht schaffen	Politik (Europäische Außenbeziehungen)
54.	2021	Ramon Fernandez, Katrin Suder	Digital Compass. Europe's Digital Sovereignty	Staat	**Handlungsfelder digitaler Souveränität** - eigene Kompetenzen in der europäischen Union entwickeln - Wahlfreiheit bei der Nutzung ausländischer Dienstleistungen bewahren - Um zu ermöglichen, dass europäische Unternehmen wachsen können und mit internationalen Unternehmen mithalten können, ist der Fojus auf die kleineren Länder in Europa zu richten - es ist eine bessere Kommunikation zwischen den europäischen Ländern notwendig - die Strategie sollte auf ein gemeinsames Interesse beruhen - damit die Koordinierung gelingt, sind die Verantwortlichkeiten zwischen den Ländern aufzuteilen	Politik (Digitalisierung der Bundesregierung Deutschland)
55.	2019	Thieulin, B.	Towards a European digital sovereignty policy.	Staat	**Handlungsbereiche für Europa** - Ethische und sicherheitsrelevante Aspekte machen das Datenmanagement zu einer entscheidenden politischen Frage für Europa - Stärkere Regulierung digitaler Plattformen EU-weit - Schaffung der Voraussetzungen für ein digitales „Ökosystem" im Einklang mit den Grundsätzen und Werten der EU	Politik
56.	2021	Merkel, A., Frederiksen, M., Marin, S., & Kallas, K.	Letter to the President–Digital Sovereignty	Staat, Wirtschaft, Individuum	**Europäische Perspektive** 1. Wohlstand 2. Sicherheit 3. Wettbewerbsfähigkeit 4. Wohlergehen der Gesellschaft	Politik
57.	2020	Bria, Francesca	Towards a Digital Green New Deal: A European Alliance on Digital Sovereignty to Reconquer Democratic Control of Data and to Put Tech and Innovation	Wirtschaft, Individuum	**Wirtschaft in Europa** - Ziel sollte eine demokratische, nachhaltige, auf die Bürger ausgerichtete, digitale Wirtschaft sein - Dies umfasst eine politische, eine soziale und eine wirtschaftliche Dimension - positive Vision für das digitale Europa mittels einer politischen Agenda, die viel Ehrgeiz verlangt **Maßnahme zur Erreichung einer starken Wirtschaft in Europa** - Vorantreiben einer Bewegung von unten - Schaffung neuer Allianzen - Beteiligung von Städten, Innovatoren, Unternehmen, Arbeitnehmern, Gewerkschaften, politischen Parteien, sozialen Bewegungen, Bürgern und Forschern	Politik (italienische Perspektive)
58.	2020	Kumar, Abhay	Securing digital sovereignty: In context to present day challenges of cyber space	Individuum	**Verständnis digitaler Souveränität** - digitale Sicherheit wahren - Entwicklung von Wohlstand - Nutzer sind Eigentümer über ihre Daten und Unternehmen gewährleisten Integrität - Auswahl, Kontrolle ind Atonomie im Cyberraum **Ableitung von 4 Prinzipien digitaler Souveränität:** 1. Wahlfreiheit 2. Selbstbeschränkung 3. Selbstkontrolle 4. Sicherheit.	Philosophie
59.	2020	Malhotra, Charru	Digital Sovereignty & Mergers/Acquisition	Wirtschaft	**Balance-Akte, um digitale Souveränität zu erreichen, zum Beispiel** - Cyber-Souveränität des Staates vs. freier Geist des Internets - uneingeschränkte Interkonnektivität - Cybersouveränität vs. Menschenrechte - Cyber-Souveränität vs. mehrere Interessengruppen in der Verwaltung.	Verwaltung/ Technik (Informations- und Kommunikationstechnik)
60.	2021	Calzada, I	Postpandemic technopolitical democracy: Algorithmic nations, data sovereignty, digital rights, and data co-operatives	Individuum	**Notwendige Voraussetzungen für eine erfolgreiche Umgestaltung** 1. Neoliberalismus (Neoliberale Kommodifizierung der Bürgerbeteiligung) 2. Skalen (Die Stadt, die Urbanisierung und die Ungleichheiten) 3. Beteiligung der Bürger (Das Recht zu entscheiden: vom liberal-demokratischen Konzept zum radikal-demokratischen Instrument) 4. Generierung von Wissen, Forschungsmethoden in demokratischer Vertiefung (Methoden und Strategien zum Aufbau demokratisch-partizipativer Prozesse)	Innovation

Tabelle 9: Google Scholar Suche »digital sovereignty«

61.	2020	Ryzhov, V. A.	Role of the industrial complex for the country's sovereignty in the new world order and the formation of the IT industry after the digital transformation of society.	Staat	**Welches IT-Modell sollte ein Staat wählen, um digitale Souveränität zu erreichen?** **Vorschlag** - möglichst passendes IKT-Modell mit Industriegruppen A und B (Produktionsmittel und Konsumgüter), Gruppen C + D (Herstellung von Universalprodukten - Energie-Strom und Information-Wissen) und die Gruppe X (Produktion von öffentlichen und kollektiven Gütern, die zu den Staatszielen beitragen).	Daten
62.	2013	Couture, S.	Logiciels Libres: Réduction Des Coûts et Souveraineté Numérique. Note socio-économique [Free Software: Cost Reduction and Digital Sovereignty. Socio-economic note]	Staat	**Digitale Souveränität und Open Source** - Nutzung von Open-Source-Software - Kosten offenlegen - Einsparungen offenlegen - internationale Erfahrungen mit der Einführung dieser Software verücksichtigen	Kommunikations-wissenschaft
63.	2006	Bernard Benhamou, Laurent Sorbier	Sovereignty and Digital Networks	Staat	**Grundprinzipien digialer Souveränität** - Neutralität des Internets - Interoperabilität - Zugänglichkeit - Netzverwaltung, die die demokratischen Grundsätze respektiert.	Forecasting & Internet Governance, E-Government Development Agency
64.	2020	Resa Mohabbat; Kar und B. E. Thapa	Digitale Souveränität als strategische Autonomie	Staat	**Verständnis digitaler Souveränität** - Umgang mit Abhängigkeiten in digitalen Cyberräumen umzugehen - Stärkung der europäischen strategische Autonomie **Umgang auf Basis dieses Verständnisses** - Abhängigkeiten im Rahmen von technischen Lösungen und Prozessen vermeiden - Balance finden zwischen Fremdbezug und eigene Erstellung am europäischen Markt: Finanzierung, Strukturierung und Regulierung von Leistungen - politische Strategien nutzen, um Schlüsseltechnologien zu fördern: staatliche Steuerungselemente nutzen wie strategische Partnerschaften, Risikomanagement und Gemeingüteransätze	Beratung öffentliche IT
65.	2021	Ernst Andreas Hartmann	Digitale Souveränität in der Wirtschaft – Gegenstandsbereiche, Konzepte und Merkmale	Wirtschaft	**Dimensionen digitaler Souveränität** - Gestaltung von Arbeit - Datenschutz - Sicherheit von Daten - Recht von Bürgern - Fähigkeiten von von Unternehmen im internationalen Wettbewerb mitzuhalten **Konzeptionierung und Messung digitaler Souveränität** - Handlungskonstrukts von Oesterreich wird vorgeschlagen, um digitale Souveränität konzeptionell besser zu fassen und eine Messgrundlage als Diskussion zu haben	Innovation/ Technik

Tabelle 10: Google Scholar Suche »digital sovereignty«

Nr.	Jahr	Autor(en)	Titel	Zuordnung	Kurze Zusammenfassung	Perspektiven
1.	2019	Harrie Bastia	Infrastructural Sovereignty over Agreement and Transaction Data ('Metadata') in an Open Network-Model for Multilateral Sharing of Sensitive Data	Wirtschaft	**Balance-Akt zwischen Innovation und Datensouveränität** - Es handelt sich um ein Spannungsfeld - Einereits Primärdaten gemeinsam nutzen, d.h. gemeinschaftliche Datennutzung zu fördern; Metadaten auf Basis von unternehmerischen Prozessen sammeln; Integrationsaufwand gering halten - Andererseits Übertragung der Datenkontrolle, Prozessauslagerung und Annahme von Unternerstützung bei der Nutzung von Daten zur Steigerung der Effizienz im Betrieb - Risikoabwägung notwendig - Offene Netzwerkmodelle für sensitive Daten	Wirtschafts-informatik
2.	2019	Boris Otto	Interview with Reinhold Achatz on "Data Sovereignty and DataEcosystems'	Wirtschaft	**Ökosystem für mehr Datensouveränität** - Durch einen gemeinschaftlichen Austausch von Daten wird das Potenzial gesteigert, digitale Geschäftsmodelle durch die Nutzung von mehr Daten zu entwickeln - Unternehmen wollen jedoch nicht die Kontrolle verlieren - Es braucht ein sicheres Ökosystem, in dem Unternehmen Potenziale nutzen können und gleichzeitig sicher handeln können	Informations-management
3.	2019	Matthias Jark	Data Sovereignty and Data Space Ecosystems	Wirtschaft, Individuum	**Vertragskonformität für Datensouveränität gewährleisten** - Datenaustausch unter Recht- und Vertragsgrundlagen stärker automatiseren - Ziel sollte es sein, mehr Daten zu erhalten, die für KI-Anwendungen, Big Data Analysen und die Automatisierung von Prozessen notwendig sind und gleichzeitig Vertragskonformität zu gewährleisten **Datensouveränität als kritischer Erfolgsfaktor für KI-Anwendungen** 1) Aspekt der Datenportabilität im Rahmen der Datensouveränität - dem durch die DSGVO garantierten Recht, die eigenen Daten von einem Online-Dienst zu einem anderen zu übertragen. 2) Datenanalyse und maschinelles Lernen, insbesondere im Falle von erworbenen externen Daten, verfolgen Zwecke, die sich von den ursprünglichen Zielen der Datensammler stark unterscheiden 3) sekundäre Nutzung von persönlichen Informationen die in Ereignisprotokollen enthalten sind	Unternehmen/Wirtschafts-informatik
4.	2021	Fabian Bruck	Utilizing Remote Evaluation for Providing Data Sovereignty in Data-sharing Ecosystems	Wirtschaft	**Remote Processing als Ansatz für mehr Datensouveränität** - Mechanismen zur Nutzungskontrolle von Datenverarbeitungen - Erweiterung von Remote-Processings - gemeinsame Nutzung von Daten möglich, gleichzeitig Kontrolle - Es werden Ausführungsprotokolle der Daten geteilt und nicht die Klassifizierungen - So können sensible Daten nicht gegenüber Dritten offengelegt werden - Die Inklusion der Kontrollmechanismen senken die Wahrscheinlichkeit, dass jemand Unerwünschtes eindringt und Daten klaut	Digitale Services/ Nachhaltigkeit

Tabelle 11: UniBw Suche

Nr.	Jahr	Autor(en)	Titel	Abstract	Zuordnung	Perspektiven
1.	2022	Glasze, Georg , Odzuck, Eva Helene , Staples, Ronald	Was heißt digitale Souveränität? : Diskurse, Praktiken und Voraussetzungen "individueller" und "staatlicher Souveränität" im digitalen Zeitalter	**Verhältnis digitale Souveränität, souveränes Subjekt, souveräner Staat** - Debatte im Rahmen von Wirtschaft, Politik, Recht, Technik notwendig - Den gewünschten Umgang mit Daten klären - das Verhältnis von Fremd- und Selbstbestimmung klären	Staat, Wirtschaft, Individuum	Politik
2.	2020	Peuker, Enrico	Verfassungswandel durch Digitalisierung : digitale Souveränität als verfassungsrechtliches Leitbild	**Digitale Souveränität und das Verfassungsrecht** - fordert Grundgesetzweiterentwicklungen - Verwantortung des Staates für eine sichere, resiliente Infrastruktur - Inklusion von Bedingungen, die für eine stärkere Digitalisierung notwendig sind	Staat	Rechtswissenschaft
3.	2019	Piétron, Dominik	Digitale Souveränität durch Interoperabilität : zur Möglichkeit dezentraler sozialer Netzwerke in der Plattformökonomie	**Digitale Souveränität und Interoperabilität** - Mit mehr Interoperabilität kann man Monopolstellungen entgegenwirken - Mehr Interoperabilität ist jedoch datenschutzrechtlich kritisch - Verpflichtungen für progressive Interoperabilität können diesem Problem entgegenwirken	Staat, Wirtschaft	Wirtschaft- und Sozialpolitik
4.	2018	Blossfeld, Hans-	Digitale Souveränität und Bildung : Gutachten	**Digitale Souveränität und Medien** - ein souveräner Umgang mit Medien erfordert Bildung - die kommende Generation ist auf die Transformation vorzubereiten - Aktionspläne für verschiedene Altergruppen sind erforderlich - Die Lernziele müssen auch ethisch reflektiert werden	Individuum, Wirtschaft	Betriebswirtschaft
5.	2018	Volker Wittpahl	Digitale Souveränität: Bürger| Unternehmen| Staat	**Digitale Souveränität und die sozialen Bots** - Souveränes Handeln von Nutzern notwendig - Es sollte Anspruch sein, stärkere Selbstbestimmung zu realisieren - Die Rolle von Drittanbietern sollte im Zuge von sozialen Bots neu verhandelt werden	Individuum	Innovation/ Technik
6.	2016	Friedrichsen, Mil	Digitale Souveränität : Vertrauen in der Netzwerkgesellschaft	**Verständnis von digitaler Souveränität** - digitale Souveräntität als Gegenbewegung zur Globalisierungswelle - Europäer sind Konsumenten zwischen Asien und den USA - Forderung nach mehr Protektionismus kommt auf **Maßnahmen auf verschiedenen Ebenen: Recht, Gesellschaft, Technologie, Politik, Wirtschaft, Kultur** - Rechtliche Voraussetungen für Datenschutz und Privatsphäre - Gesellschaftlicher Beitrag zur mediellen Nutzung und Bildung - Datensicherheit muss auf technischer Ebene gewährleistet werden - Politik kann Rahmenbedingungen schaffen - Unternehmen fokussieren sich auf ihre Wertschöpfung und wollen die Vorteile der Globalisierung nutzen - Die Psychologie beim Handeln im digitalen Raum hat einen Einfluss darauf, die Individuen im digitalen Raum handeln und damit der Informationsfluss erfolgt	Staat, Wirtschaft, Individuum	Kommunikations- und Medienwissenschaft, Politikwissenschaft, Wirtschaftswissenschaft
7.	2021	Hummel, Patri	Datensouveränität : Governance-Ansätze für den Gesundheitsbereich	**Datensouveränität aus der Sicht von Recht und Ethik** - konkrete Governance notwendig - besondere Anforderungen im Gesundheitssektor	Staat, Wirtschaft	Gesundheitswesen
8.	2021	Ternès, Anabel	Ferngesteuert?! : hin zur digitalen Souveränität	**Datensouveränität und digitaler Alltag** - Unser Verhalten ist häufig ferngesteuert im digitalen Raum - Herausforderung aus diesem Konstrukt auszubrechen - Individuen müssen den Willen haben, ihre Zukunft anderweitig in die Hand zu nehmen und die digitale Zukunft mit mehr Eigenverantwortung zu gestalten	Individuum	Kommunikations-wissenschaft

Tabelle 12: AIS Library Suche

Nr.	Jahr	Autor(en)	Titel	Abstract	Zuordnung	Disziplin
1.	2021	Peter J. Wirnsperger, Felix Dinnessen, . Soentje Julia Hilberg	Mit digitaler Souveränität ins europäische digitale Jahrzehnt	**Empfehlungen für europäische Initiativen** - Förderung von KI - Gestaltung einer Datenökonomie - Gestaltung von sicherer Cloud Infrastruktur - Förderung von mehr Cybersicherheit	Staat	Beratung

Tabelle 13: Suche nach Beratungskonzepten

Lfd.Nr.	Potenzielles Risiko	Zuordnung strategisches Risiko	Zuordnung operatives Risiko	Vorschlag zum Umgang mit dem Risiko
	Projekt 1: Informationssteckbrief			
1	Sicherheit Kubernetes --> Fehlkonfigurationen als Sicherheitsrisiko (sind die häufigste Ursache für Sicherheitsrisiken bei containerisierten Anwendungen, die auf Kubernetes ausgeführt werden)		x	**Fördern sicherer Softwareentwicklung** '-Beschreibung konkreter Sicherheitsanforderungen -> präzise und verständliche -Sicherheitsanforderungen beschreiben, in agilen Softwareprojekten müssen Anforderungen an die Anwendungssicherheit kontinuierlich angepasst werden - Sicherheitsarchitektur erstellen -> Gesamtarchitektur, wie das zusammenhängende Gesamtkonzept aussieht - IS-Risikoanalyse für das Vorhaben muss unter Berücksichtigung der elementaren Gefährdungen des BSI durchgeführt werden
2	Dashboard = Grafana --> Das BSI hat einen aktuellen IT-Sicherheitshinweis für Grafana veröffentlicht		x	
3	MangoDB --> Das BSI hat am 31.08.2023 ein Update zu einer Sicherheitslücke für MongoDB herausgegeben.		x	
4	PostGreSQL --> Das BSI meldet bekannte Schwachstelle für PostgreSQL. Nun ist ein Update erfolgt.		x	
5	Mögliche Stelle eines Missbrauchsvorfalls: Auskunft über Personen und Orte via Twitter			**Vermeidung von Daten-Diebstahl, Missbrauchsvorfällen oder Offenlegung schützenswerter Informationen** Ziel --> Datensicherheit und die „Datensouveränität“ nachhaltig und effektiv stärken
6	Möglichkeit eines Diebstahls von Geräten, Datenträgern oder von Dokumenten			
7	Beim Scraping der externen Websites: Offenlegen schützenswerter Informationen möglich		x	
8	Ausspähen von Informationen (Spionage) oder Abhören		x	
9	Zu wenig Awareness bei den Entwicklern für das Thema Resilienz und souveräne Entscheidungsfindung		x	**Awareness zu dem Thema erhöhen** Insbesondere für Entwickler kurze Impulsschulungen anbieten
11	Chancen und Risiken der Nutzung digitaler Dienste werden in der Regel durch die Product Owner oder Projektleiter festgelegt		x	**Verantwortlichkeiten festlegen** Abläufe definieren
12	Abhängigkeit zum Hyper-Scaler Amazon vorhanden		x	**Sichere Cloud-Technologien nutzen** Die gewählte Technologie im Projekt sollte die Anforderungen des Projektes treffen. Fällt die Wahl auf eine Cloud-Technologie, so sollte diese sicherstellen, dass man hier sicher entwickeln, implementieren, als auch verwalten (z.B. Datenschutzeinstellungen, Netzwerksicherheitseinstellungen) kann
13	Schlüsseltechnologie KI im Projektkontext --> Die vielversprechendsten NLP-Modelle für das vorliegende Projekt sind in Englisch		x	**Anbietervielfalt erhöhen** Anbieter im Zusammenspiel mit Nutzerfreundlichkeit, Kosten, Nähe zum Kunden und Transportwege für das Projekt bewerten.
14	Regeln und Standards zur Gewährleistung von Datenintegrität sind nicht in den anfänglichen Analyse-, und Designphase vom Projekt inkludieren worden		x	Offenlegung von Implementierungen gegenüber vertrauenswürdigen Prüfstellen, wissenschaftlich abgesicherte Prüfverfahren sowie Prüfsiegel mit für Endkunden nachvollziehbaren Bedeutungen
15	Es wurden keine Prozesse geschaffen, d.h. Wen kann ich wann ansprechen und wie erreichen, wenn ich digitale Souveränität umsetzen will?		x	**Abläufe und Prozesse definieren** Jeder im Unternehmen sollte stets wissen, an wen er sich ohne Bedenken wenden kann, wenn es um das Thema digitale Souveränität geht.
16	Einbußen im Sinne der digitalen Souveränität bleiben durch das Ausbleiben der Aktualisierung des Informationssicherheitskonzeptes weiterhin bestehen.		x	**Zu Beginn des Projektgeschehens ist das Thema digitale Souveränität zu inkludieren** Digitale Souveränität sollte bereits zu Beginn eines Softwareprojektes mitgedacht werden. Eine konkrete Formulierung von operativen Maßnahmen trägt dazu bei, die identifizierten Risiken im Projektgeschehen zu minimieren.
17	Risiko, dass man digitale Souveränität versucht als Einheitslösung für Entwicklungsprojekte zu verkaufen, was in Anbetracht der unterschiedlichen Nutzer, des Einsatzes von verschiedensten Systeme und damit zusammenhängenden ihrer Schutzmaßnahmen so sicherlich nicht möglich ist.		x	
18	Keine Ausschreibungskriterien für digitale Souveränität sind definiert worden		x	
19	Man hat zu wenig Optionen, die Interoperabilität bieten oder zum Standard passen		x	**Höhere Kosten für mehr Sicherheit in Kauf nehmen** Vertrauenswürdigkeit erhöhen durch eigene Hardware und Software als Alternative zu vertrauenswürdigen Partnern; Offenlegung der Entwicklungsarbeit; Datenschutz berücksichtigen; Risikoabwägung für unterschiedliche Szenare durchführen
20	Insbesondere Eigeninteressen in Entwicklungsteams könnten vorangetrieben und die eigene Arbeit statt der Notwendigkeit nach digitaler Souveränität in den Vordergrund gerückt werden		x	
21	Alternativen sind nicht hinreichend betreiberfreundlich		x	
22	Wenn kein Vertrauen zu einem Partner vorliegt, ist das herausfordernd		x	

Tabelle 14: Übersicht über die Risiken im Projekt Informationssteckbrief und Empfehlungen zum Umgang mit dem Risiko (1/2)

Lfd.Nr.	Potenzielles Risiko	Zuordnung strategisches Risiko	Zuordnung operatives Risiko	Vorschlag zum Umgang mit dem Risiko
	Projekt 1: Informationssteckbrief			
23	Politische Einflüsse können z.B. dafür sorgen, dass bewusst Verschlüsselungen abgeschwächt werden und so zu fehlerhafter Hard- und Software führen.	x		Unternehmen müssen sich entscheiden, wie Sie mit einem derartig transformativen Thema umgehen wollen.
24	Bei einer Definition von Qualitätsmerkmalen und -indikatoren lediglich technischen Fokussierung und einem Ausklammern der organisatorischen Notwendigkeiten wird eine erfolgreiche Berücksichtigung digitaler Souveränitätsanforderungen erschwert		x	**Abläufe und Prozesse definieren** Jeder im Unternehmen sollte stets wissen, an wen er sich ohne Bedenken wenden kann, wenn es um das Thema digitale Souveränität geht.
25	Kompetenz nicht vorhanden, digitale Souveränität in Softwareentwicklungsprojekten umzusetzen		x	**Langfristig sollte es Ziel sein eine Kultur zu etablieren, die automatisch das Thema digitale Souveränität inkludiert.** Um dies zu erreichen, braucht es Zeit. Kampagnen dieser Natur sind aufwendig in Planung, Vorbereitung und Durchführung.
26	Personen sind selbst nicht in der Lage, den Quellcode auf Korrektheit und das Nichtvorhandensein unerwünschter Funktionen zu prüfen		x	**Impulsschulungen** können insbesondere die Awareness der Entwickler im Projekt fördern und sie in die Lage versetzen kleinere Prüfungen eingenständig vorzunehmen.
27	Management von digitaler Souveränität allein durch Inhouse-Systeme ggf. nicht möglich	x		**Vorteile von Open-Source-Software nutzen** Unternehmen können frei entscheiden, bei welchem Provider sie ihre Anwendungscontainer betreiben und welche Software sie zur Verwaltung nutzen möchten. Außerdem kann quelloffene Software kontinuierlich auf Schwachstellen geprüft und herstellerunabhängig weiterentwickelt werden. Organisationen haben die Möglichkeit, Anwendungen bei verschiedenen Anbietern zu betreiben: Performance-hungrige Business-Anwendungen bei Hyperscalern a la Amazon & Co und die zugehörigen Datenbanken bei europäischen oder lokalen Anbietern. Um die Vorteile von OSS im Rahmen der Stärkung digitaler Souveränität realisieren zu können, braucht es geeignete Managementsysteme. Die Normen ISO/IEC 5230 und ISO/IEC DIS 18974 als Basis verwenden, um Maßnahmen zu beschreiben und zu konkretisieren, wie OSS sicher und regelkonform einzusetzen ist.
28	Wenn Kunden beim Betrieb von Software-Anwendungen ausschließlich auf die Technologien bestimmter Anbieter setzen, ergibt sich beinahe automatisch ein Lock-in-Effekt. Sind die Lösungen im Alltagsgeschäft etabliert und die zugehörigen Datenbanken mit Daten befüllt, ist der Geschäftserfolg der Unternehmen vom jeweiligen Anbieter abhängig.	x		**Lieferketten besser kontrollieren** Es bietet sich an, Szenare, bewertet nach Eintrittswahrscheinlichkeit und Schadenshöhe, zu formulieren und für ebendiese eine Risikoabwägung durchzuführen.
29	Störungen von Bereitstellungsinfrastruktur können zu einem eingedämmten Wirkungsgrad von Unternehmen führen	x		
30	Sanktionen haben die Eigenschaft, wenn diese zu Konkursen oder erzwungenen Stilllegungen führen, Ausfälle und fehlenden Support eines Herstellers oder Lieferanten von verbreiteten oder kritischen Produkten herbeizuführen	x		**Unternehmerische Ziele mit Forschung und Politik zusammenführen** Es bedarf größerer Anstrengung als innerhalb des Projektgeschehens, um Digitale Souveränität zu erreichen.
31	Kontrolle über eine digitale Infrastruktur bei dominanten Herstellern in wenigen Ländern kann dazu führen, dass politische Akteure diese Sonderstellung für ihre Gegebenheiten nutzen, um politische Macht auszuüben	x		
32	Wiederhochfahren von Logistikketten, Energie-, oder Transportnetzen ist bei einem potenziellen Angriff eine schwerwiegende Aufgabe	x		**Strategische Allianzen zur Erhöhung digitaler Souveränität bilden** Interessant ist eine Allianz für mehr digitale Souveränität auf technologischer Ebene als auch auf finanzieller Ebene. Mit einem Zusammenschluss kann man neben einem Innovationsvorteil ggü. Wettbewerbern, Umsetzungskosten sparen und Risiken minimieren.
33	Im schlimmsten Fall müssen abgewanderte Geschäfte, Kunden oder Partner zurückgewonnen werden oder es muss auf andere Bereiche ausgewichen werden	x		
34	Man sollte berücksichtigen, dass das Risiko mit der Auswahl des Partners einhergeht, hohe Folgekosten zu erzeugen	x		
35	Folgefehler, die durch Einbußen digitaler Souveränität entstehen können. So können Schäden wie z.B. der Wideraufbau von manipulierter oder zerstörter Infrastruktur derartige Kosten erzeugen	x		
36	Sind erst die Software-Anwendungen beim Kunden mit bestimmten Anbietern im Betrieb, ergibt sich ein Lock-In-Effekt	x		**Open-Source-Software in weiteren Projekten einsetzen** Unternehmen können frei entscheiden, bei welchem Provider sie ihre Anwendungscontainer betreiben und welche Software sie zur Verwaltung nutzen möchten.
37	Das Risiko, das entsteht, wenn man digitale Souveränität versucht in Unternehmen zu stärken, ist, dass ein Verlust von Kostenvorteilen, der Nähe von Großkunden, und von günstigen Transportwegen die Folge sein kann	x		**Unternehmerische Ziele mit Forschung und Politik zusammenführen** Es bedarf größerer Anstrengung als innerhalb des Projektgeschehens, um Digitale Souveränität zu erreichen.
38	Es ist herausfordernd, Standards so zu setzen, dass man langfristig Marktführerschaften auf deutscher und europäischer Ebene unterstützt und man gleichzeitig keine Einbußen bei der Wettbewerbsfähigkeit macht	x		

Tabelle 15: Übersicht über die Risiken im Projekt Informationssteckbrief und Empfehlungen zum Umgang mit dem Risiko (2/2)

Lfd.Nr.	Potenzielles Risiko	Zuordnung strategisches Risiko	Zuordnung operatives Risiko	Vorschlag zum Umgang mit dem Risiko
	Projekt 2: Messenger			
1	Angreifer könnten neue Nutzer in E2E-verschlüsselte Räume einfügen. Damit kann ein Angreifer E2E-verschlüsselte Chats von Nutzern mitlesen		x	Sicherheitsrisiken transparent (open access) im Projektteam teilen und managen
2	Wenn sich ein neuer Besitzer einer Domain als der vorherige ausgibt, kann dieser Nachrichten erhalten und alte Nachrichten anfragen		x	
3	Angreifer könnte sich als vertrauenswürdiges Gerät eines Nutzers ausgeben und Backups anfordern, um Zugriff auf Daten zu erhalten		x	
4	Angreifer nutzen die Kontrolle des Homeservers über die Raumteilnehmer, um die Ziel-Clients zu zwingen, Entschlüsselungsschlüssel mit Geräten zu teilen.		x	
5	Angreifer erhält eine kryptografische Signierung		x	
6	Angreifer erhält Authentifizierung, die durch das Key Request Protokoll weitergegeben werden		x	
7	Angreifer geht so vor, dass eine neue Mogolm-Sitzung initiiert wird, der durch den vorherigen Angriff aufgebaut wurde		x	
8	Out-of-Band-Selbstverifizierung führt dazu, dass das Gerät ein SSSS-Protokoll verwenden kann, um eine Kopie des verwendeten Schlüssels zu erhalten.		x	
9	Angreifer entschlüsselt durch Abfrage von Verschlüsselungs- und Entschlüsselungsorakel einen Chiffretext		x	
10	Risiko: VS-NfD-Zulässigkeit bei dem Kommunikationsprotokoll Matrix ist kritisch '-BSI hat eine Bewertung des Matrix-Protokolls vorgenommen, das jedoch als VS-NfD eingestuft ist - In Zeitungen wird behauptet, dass matrix VS-NfD tauglich ist. Die Sicherheit für einen VS-NfD—Gebrauch kann nicht durch matrix sichergestellt werden, sondern erfolgt durch andere IT-Sicherheitsprodukte (z.B. SINA Laptops oder SecuSUITE Smartphones)		x	Für VS-NfD -> SINA Laptops oder SecuSUITE Smartphones als Endgeräte nutzen + BSI-zertifizierte Verschlüsselung auf dem Endgerät + zertifizierte VPN-Verbindung
11	Bedeutende Fassetten der Softwareentwicklung werden nicht hinreichend durchdrungen (Kryptographie) --> Risiko eines erhöhten Abhängigkeitsverhältnisses zu NewVector.		x	Weiterbildungen (z.B. für das Thema Kryptographie) anbieten
12	Abhängigkeit zu anderen Providern wird nicht hinreichend gemanagt --> Dies kann zu Fehlentwicklungen, Problemen bei der Überführung zum Kunden, Zeitverlust führen	x		Externe Unterauftragnehmer besser steuern Stakeholder in die Matrix Foundation einbetten

Tabelle 16: Übersicht über die Risiken im Projekt Messenger und Empfehlungen zum Umgang mit dem Risiko

Kapitel	Studie	Die wichtigsten Ergebnisse	Thema aus dem DISO-A Modell	Quantifizierung
4.4.	Umfrage: Herausforderungen digitale Souveränität mit den Technologien KI und Blockchain einzuführen & Maßnahmenkatalog zum Umgang mit den Herausforderungen	Künstliche Intelligenz als Schlüsseltechnologie kann in Zusammenhang mit dem Konzept des Federated Learnings zu mehr Datensouveränität führen	Schlüsseltechnologie	N=2 wesentliche Schlüsseltechnologien für die Stärkung von Datensouveränität in Unternehmen
4.4.	Umfrage: Herausforderungen digitale Souveränität mit den Technologien KI und Blockchain einzuführen & Maßnahmenkatalog zum Umgang mit den Herausforderungen	Blockchain als Schlüsseltechnologie kann aufgrund seiner manipulationssicheren, transparenten Struktur einen Beitrag zu mehr Datensouveränität leisten	Schlüsseltechnologie	
4.4.	Umfrage: Herausforderungen digitale Souveränität mit den Technologien KI und Blockchain einzuführen & Maßnahmenkatalog zum Umgang mit den Herausforderungen	Wahrung der Datensouveränität	Schlüsseltechnologie	N=8 Maßnahmen (Maßnahmenkatalog) zur Stärkung digitaler Souveränität mit den Schlüsseltechnologien KI und Blockchain
4.4.	Umfrage: Herausforderungen digitale Souveränität mit den Technologien KI und Blockchain einzuführen & Maßnahmenkatalog zum Umgang mit den Herausforderungen	Die Transformation mitgestalten	Schlüsseltechnologie	
4.4.	Umfrage: Herausforderungen digitale Souveränität mit den Technologien KI und Blockchain einzuführen & Maßnahmenkatalog zum Umgang mit den Herausforderungen	Fachwissen aufbauen	Schlüsseltechnologie	
4.4.	Umfrage: Herausforderungen digitale Souveränität mit den Technologien KI und Blockchain einzuführen & Maßnahmenkatalog zum Umgang mit den Herausforderungen	Förderung der Wahlfreiheit	Schlüsseltechnologie	
4.4.	Umfrage: Herausforderungen digitale Souveränität mit den Technologien KI und Blockchain einzuführen & Maßnahmenkatalog zum Umgang mit den Herausforderungen	Define responsibilities	Schlüsseltechnologie	
4.4.	Umfrage: Herausforderungen digitale Souveränität mit den Technologien KI und Blockchain einzuführen & Maßnahmenkatalog zum Umgang mit den Herausforderungen	Verantwortlichkeiten festlegen	Schlüsseltechnologie	
4.4.	Umfrage: Herausforderungen digitale Souveränität mit den Technologien KI und Blockchain einzuführen & Maßnahmenkatalog zum Umgang mit den Herausforderungen	Bedenken ausräumen und Bewusstsein schaffen	Schlüsseltechnologie	
4.4.	Umfrage: Herausforderungen digitale Souveränität mit den Technologien KI und Blockchain einzuführen & Maßnahmenkatalog zum Umgang mit den Herausforderungen	Messkriterien für digitale Souveränität finden	Schlüsseltechnologie	

Tabelle 17: Analyseergebnis 1: Referenzmodellierung

Kapitel	Studie	Die wichtigsten Ergebnisse	Thema aus dem DISO-A Modell	Quantifizierung
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Sicherheit Kubernetes --> Fehlkonfigurationen als Sicherheitsrisiko (sind die häufigste Ursache für Sicherheitsrisiken bei containerisierten Anwendungen, die auf Kubernetes ausgeführt werden)	Open Source	N=37 Risiken für die Stärkung digitaler Souveränität mit Hilfe von Open Source in Softwareentwicklungsprojekten
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Dashboard = Grafana --> Das BSI hat einen aktuellen IT-Sicherheitshinweis für Grafana veröffentlicht	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	MangoDB --> Das BSI hat am 31.08.2023 ein Update zu einer Sicherheitslücke für MongoDB herausgegeben.	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	PostGreSQL --> Das BSI meldet bekannte Schwachstelle für PostgreSQL. Nun ist ein Update erfolgt.	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Mögliche Stelle eines Missbrauchsvorfalls: Auskunft über Personen und Orte via Twitter	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Möglichkeit eines Diebstahls von Geräten, Datenträgern oder von Dokumenten	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Beim Scraping der externen Websites: Offenlegen schützenswerter Informationen möglich	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Ausspähen von Informationen (Spionage) oder Abhören	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Zu wenig Awareness bei den Entwicklern für das Thema Resilienz und souveräne Entscheidungsfindung	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Chancen und Risiken der Nutzung digitaler Dienste werden in der Regel durch die Product Owner oder Projektleiter festgelegt	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Abhängigkeit zum Hyper-Scaler Amazon vorhanden	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Schlüsseltechnologie KI im Projektkontext --> Die vielversprechendsten NLP-Modelle sind in Englisch	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Regeln und Standards zur Gewährleistung von Datenintegrität sind nicht in den anfänglichen Analyse-, und Designphase vom Projekt inkludiert worden	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Es wurden keine Prozesse geschaffen, d.h. Wen kann ich wann ansprechen und wie erreichen, wenn ich digitale Souveränität umsetzen will?	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Einbußen im Sinne der digitalen Souveränität bleiben durch das Ausbleiben der Aktualisierung des Informationssicherheitskonzeptes weiterhin bestehen.	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Risiko, dass man digitale Souveränität versucht als Einheitslösung für Entwicklungsprojekte zu verkaufen, was in Anbetracht der unterschiedlichen Nutzer, des Einsatzes von verschiedensten Systemen und damit zusammenhängenden ihrer Schutzmaßnahmen so sicherlich nicht möglich ist.	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Keine Ausschreibungskriterien für digitale Souveränität sind definiert worden	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Man hat zu wenig Optionen, die Interoperabilität bieten oder zum Standard passen	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Insbesondere Eigeninteressen in Entwicklungsteams könnten vorangetrieben und die eigene Arbeit statt der Notwendigkeit nach digitaler Souveränität in den Vordergrund gerückt werden	Open Source	

Tabelle 18: Analyseergebnis 2 (1/3): Referenzmodellierung

4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Alternativen sind nicht hinreichend betreiberfreundlich	Open Source	N=37 Risiken für die Stärkung digitaler Souveränität mit Hilfe von Open Source in Softwareentwicklungsprojekten
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Wenn kein Vertrauen zu einem Partner vorliegt, ist das herausfordernd	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Politische Einflüsse können z.B. dafür sorgen, dass bewusst Verschlüsselungen abgeschwächt werden und so zu fehlerhafter Hard- und Software führen.	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Bei einer Definition von Qualitätsmerkmalen und -indikatoren lediglich technischen Fokussierung und einem Ausklammern der organisatorischen Notwendigkeiten wird eine erfolgreiche Berücksichtigung digitaler Souveränitätsanforderungen erschwert	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Kompetenz nicht vorhanden, digitale Souveränität in Softwareentwicklungsprojekten umzusetzen	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Personen sind selbst nicht in der Lage, den Quellcode auf Korrektheit und das Nichtvorhandensein unerwünschter Funktionen zu prüfen	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Management von digitaler Souveränität allein durch Inhouse-Systeme ggf. nicht möglich	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Wenn Kunden beim Betrieb von Software-Anwendungen ausschließlich auf die Technologien bestimmter Anbieter setzen, ergibt sich beinahe automatisch ein Lock-in-Effekt. Sind die Lösungen im Alltagsgeschäft etabliert und die zugehörigen Datenbanken mit Daten befüllt, ist der Geschäftserfolg der Unternehmen vom jeweiligen Anbieter abhängig.	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Störungen von Bereitstellungsinfrastruktur können zu einem eingedämmten Wirkungsgrad von Unternehmen führen	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Sanktionen haben die Eigenschaft, wenn diese zu Konkursen oder erzwungenen Stilllegungen führen, Ausfälle und fehlenden Support eines Herstellers oder Lieferanten von verbreiteten oder kritischen Produkten herbeizuführen	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Kontrolle über eine digitale Infrastruktur bei dominanten Herstellern in wenigen Ländern kann dazu führen, dass politische Akteure diese Sonderstellung für ihre Gegebenheiten nutzen, um politische Macht auszuüben	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Wiederhochfahren von Logistikketten, Energie-, oder Transportnetzen ist bei einem potenziellen Angriff eine schwerwiegende Aufgabe	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Im schlimmsten Fall müssen abgewanderte Geschäfte, Kunden oder Partner zurückgewonnen werden oder es muss auf andere Bereiche ausgewichen werden	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Man sollte berücksichtigen, dass das Risiko mit der Auswahl des Partners einhergeht, hohe Folgekosten zu erzeugen	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Folgefehler, die durch Einbußen digitaler Souveränität entstehen können. So können Schäden wie z.B. der Wideraufbau von manipulierter oder zerstörter Infrastruktur derartige Kosten erzeugen	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Sind erst die Software-Anwendungen beim Kunden mit bestimmten Anbietern im Betrieb, ergibt sich ein Lock-In-Effekt	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Das Risiko, das entsteht, wenn man digitale Souveränität versucht in Unternehmen zu stärken, ist, dass ein Verlust von Kostenvorteilen, der Nähe von Großkunden, und von günstigen Transportwegen die Folge sein kann	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Es ist herausfordernd, Standards so zu setzen, dass man langfristig Marktführerschaften auf deutscher und europäischer Ebene unterstützt und man gleichzeitig keine Einbußen bei der Wettbewerbsfähigkeit macht	Open Source	

Tabelle 19: Analyseergebnis 2 (2/3): Referenzmodellierung

Kapitel	Studie	Die wichtigsten Ergebnisse	Thema aus dem DISO-A Modell	Quantifizierung
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Affordanzen „Standards und Richtlinien“ mit „Know-How“ kombinieren	Open Source	N=15 abgeleitete Affordanzen aus den Open Source-Projekten und N=5 Anpassungsvorschläge dieser Affordanzen zur Einbettung digitaler Souveränität in Softwareentwicklungsprojekte
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Alternative Partner im digitalen Raum für die Affordanzen „Penetrationstests“, „Testsoftware“, „Cloud-Kapazität“ und „Projektmanagement-Tools“ in zukünftigen Projekten in Betracht ziehen	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Die Affordanzen „Front-End-Lösung“, „Open-Source-System“, „Datenbank“ und „Datenbankmanagementlösung“ auf Vertrauenswürdigkeit und Produkthoheit ausrichten	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Ausrichten von „automatisierten Extraktionen“ an der Datenhoheit	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Berücksichtigung wirtschaftlicher und wettbewerblicher Herausforderungen und Bilden strategischer Allianzen, um „KI-Modelle“ souveräner zu gestalten	Open Source	
4.5.	Gap-Analyse: Herausforderungen in Open-Source-Projekten & Affordanz-Analyse: Affordanzen für den Umgang mit den Herausforderungen	Affordanzen „Sammlung von Algorithmen und APIs“ sowie „Suchtechnologie“ in ihrer derzeitigen Form beizubehalten	Open Source	

Tabelle 20: Analyseergebnis 2 (3/3): Referenzmodellierung

Kapitel	Studie	Die wichtigsten Ergebnisse	Thema aus dem DISO-A Modell	Quantifizierung
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Cluster 1: Mehr Unabhänigigkeit in der Lieferkette	Lieferketten	N=4 Cluster und N=10 Zusammenhänge, die wesentlich sind, für die Einführung digitaler Souveränität im Softwarelebenszyklus von Unternehmen
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Cluster 2: Mehr IT-Skills für souveränere Lieferketten	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Cluster 3: Berücksichtigung von Kosten für souveränere Lieferketten	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Cluster 4: Berücksichtigung von Komplexität souveränerer Lieferketten	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Realistische Erwartungen	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Zielvorstellung des Unternehmens vs. Zielvorstellung der IT	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Je mehr Maßnahmen, desto mehr Zeit wird benötigt	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Personalressourcen erforderlich zur Umsetzung der IT-Fähigkeiten	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Die Ausbildung erfordert Personalressourcen, ein entsprechendes Mindset und eine sinnvolle Nutzung der im Unternehmen vermittelten Kenntnisse	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Ein modernes, komplexes Arbeitsumfeld erfordert IT-Kenntnisse, einschließlich spezifischer Kenntnisse	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Die Einführung neuer IT-Fähigkeiten kann zu einem vorübergehenden Overlead führen (Zunahme der Komplexität)	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Wenn ich die Wahl zwischen IT-Produkten mit unterschiedlicher Komplexität habe, entscheide ich mich eher für das Produkt mit der geringsten Komplexität	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Wenn mehr technologische Unabhängigkeit erforderlich ist, wird es komplexer	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Wenn mehr strategische Unabhängigkeit erforderlich ist, wird es komplexer	Lieferketten	

Tabelle 21: Analyseergebnis 3 (1/2): Referenzmodellierung

4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Akquisition	Lieferketten	N=13 Prozessse und N=4 Prozessgruppen für souveränere Softwareeinführung in Unternehmen
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Angebot	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Life Cycel Model Management	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Management der Humanressourcen	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Portfoliomanagement	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Qualitätsmanagement	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Wissensmanagement	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Projektplanung	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Risikomanagement	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Sicherung der Qualität	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Geschäfts- oder Auftragsanalyse	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Definition der Bedürfnisse und Anforderungen der Stakeholder	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Definition der Architektur	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Prozessgruppe: Agreement	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Prozessgruppe: Organisatorische Projektbefähigung	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Prozessgruppe: Technisches Management	Lieferketten	
4.6.	Soft Design Science Studie: Herausforderungen im Softwarelebenszyklus, Empfehlungen & ISO 12207:2017 erweitert um digitale Souveränitätsanforderungen	Prozessgruppe: Technik	Lieferketten	

Tabelle 22: Analyseergebnis 3 (2/2): Referenzmodellierung

Kapitel	Studie	Die wichtigsten Ergebnisse	Thema aus dem DISO-A Modell	Quantifizierung
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Transparenz	IT-Infrastruktur	N=25 Faktoren für Manager, um digitale Souveränität im Rahmen eines passenden souveränen Cloudkonzepts zu berücksichtigen
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Kontrolle	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Skalierung	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Kosteneffizienz	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Schnelligkeit (durch Zugriffe)	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	API-Anbindung	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Compliance	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	IT-Security	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Skills	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Resilienz	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Komplexität	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Unabhängigkeit	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	SLAs und Kosten	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Schnelligkeit	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Innovation	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Digitale Supply Chain	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Distaster Recovery	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Datenhoheit	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Selbstbestimmte Entscheidungen	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Mehraufwand	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Betriebliche Unterstützung	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Skalierungsmöglichkeiten	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Bereitstellung eines Data Centers	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Best Practices	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Support	IT-Infrastruktur	

Tabelle 23: Analyseergebnis 4 (1/2): Referenzmodellierung

Tabelle 24: Analyseergebnis 4 (2/2): Referenzmodellierung

4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Datensouveränität	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Operationale Souveränität	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Provider Souveränität	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Minimierung von Datensilos	IT-Infrastruktur	N=9 Faktoren aus IT-Architektur-Perspektive, um digitale Souveränität im Rahmen eines passenden souveränen Cloudkonzepts zu berücksichtigen
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Vendor Lock-In Souveränität	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Transparenz	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Autarkie	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Consulting	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Management	IT-Infrastruktur	
4.7.	Interviewstudie: Herausforderungen souveräne Clouds und Darstellung wesentlicher Perspektiven zur Entscheidungsunterstützung	Aus der Nutzerperspektive, dass es den Nutzern egal ist, ob die Cloud souverän ist. Der Schwerpunkt liegt darauf, die Cloud schnell und einfach nutzen zu können.	IT-Infrastruktur	N=1 Prozess aus Nutzer-Perspektive

Fragebogen zum Thema digitale Souveränität in der IT-Beratung

der Bundeswehr Universität München

in Zusammenarbeit mit der

BWI IT für Deutschland

Abbildung 2: Fragebogen erste Fallstudie (1/18)

frei verwendbar

Fragebogen zum Thema digitale Souveränität[1] in der IT-Beratung[2]

Ziel des folgenden Fragebogens ist es den Stand zum Thema digitale Souveränität in der BWI zu ermitteln und eine Einschätzung zu erhalten, wie der Bereich Digital Enabling Services, kurz DES sinnvoll im Rahmen der Stärkung digitaler Souveränität in der BWI unterstützen kann.

Um diesen Stand zu ermitteln, teilt sich der Fragebogen in drei Teilbereiche:

1) Allgemeine Fragen
2) Digitale Souveränität aus Sicht der BWI
3) Digitale Souveränität aus Sicht der IT-Beratung.

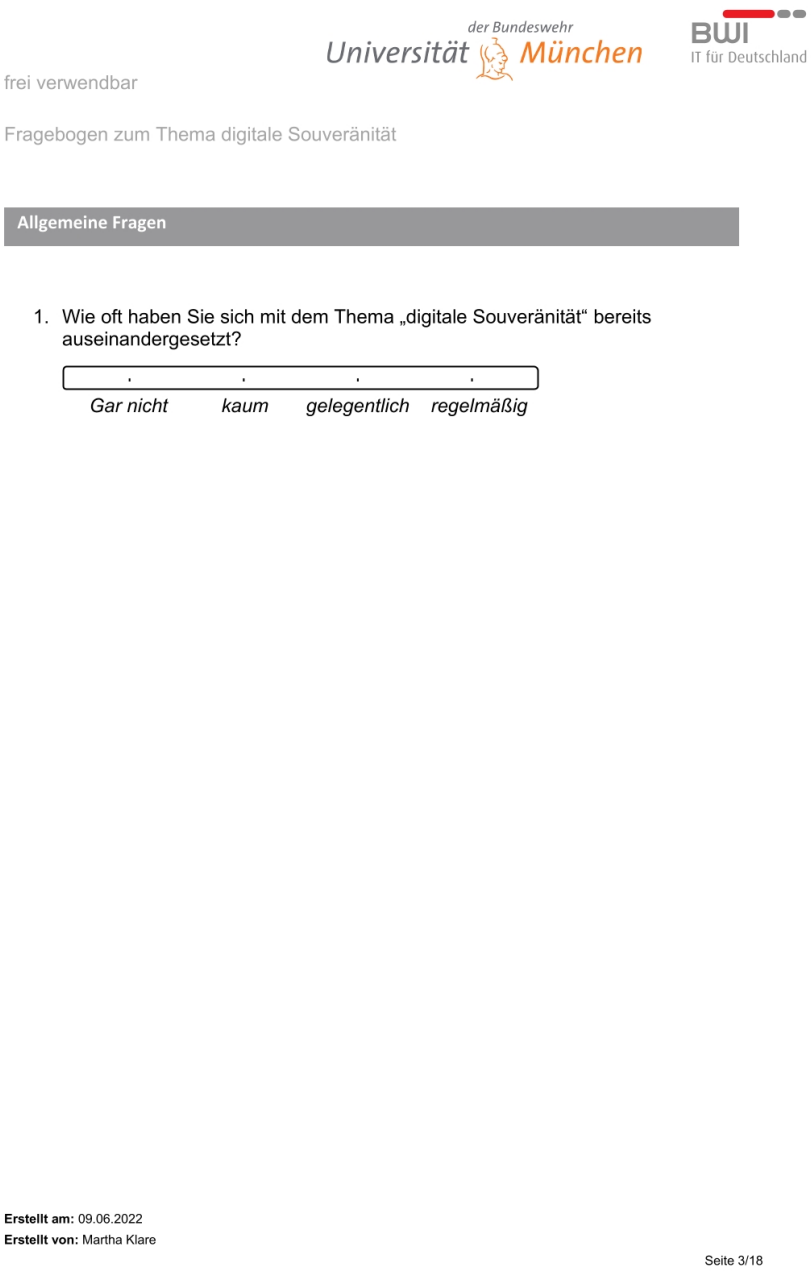
Viel Spaß beim Ausfüllen!

[1] An dieser Stelle wird der Begriff „digitale Souveränität“ bewusst nicht definiert, da im Rahmen des Fragebogens eine Einschätzung abgefragt wird, wie digitale Souveränität durch den jeweiligen Experten verstanden wird.

[2] IT-Beratungen verstehen sich als Dienstleister, die Kunden und Unternehmen bei der Analyse, Einführung, dem Bau oder der Wartung von IT-Systemen unterstützen. Dabei setzen sich IT-Beratungen im Kern mit den Themen Prozessanalyse, Architektur- und der Entwicklungsberatung und der Konzeptionierung von IT-Infrastruktur (Hardware, Software) sowie Organisationsanpassungen auseinander (vgl. Uelpenich et al., 2005, S. 228f).

Erstellt am: 09.06.2022
Erstellt von: Martha Klare

Abbildung 3: Fragebogen erste Fallstudie (2/18)



der Bundeswehr Universität München

BWI IT für Deutschland

frei verwendbar

Fragebogen zum Thema digitale Souveränität

Allgemeine Fragen

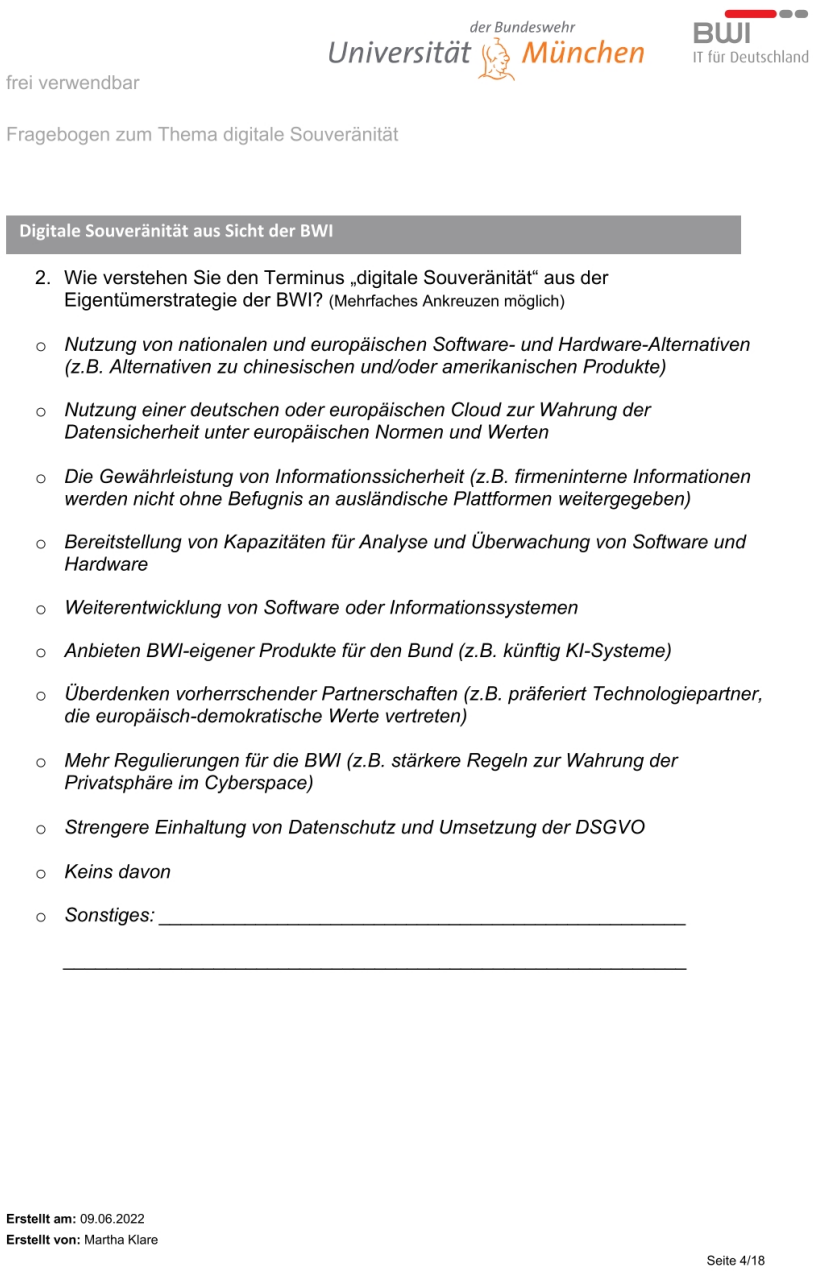
1. Wie oft haben Sie sich mit dem Thema „digitale Souveränität“ bereits auseinandergesetzt?

Gar nicht *kaum* *gelegentlich* *regelmäßig*

Erstellt am: 09.06.2022
Erstellt von: Martha Klare

Seite 3/18

Abbildung 4: Fragebogen erste Fallstudie (3/18)



der Bundeswehr Universität München

BWI IT für Deutschland

frei verwendbar

Fragebogen zum Thema digitale Souveränität

Digitale Souveränität aus Sicht der BWI

2. Wie verstehen Sie den Terminus „digitale Souveränität" aus der Eigentümerstrategie der BWI? (Mehrfaches Ankreuzen möglich)

- ○ *Nutzung von nationalen und europäischen Software- und Hardware-Alternativen (z.B. Alternativen zu chinesischen und/oder amerikanischen Produkte)*
- ○ *Nutzung einer deutschen oder europäischen Cloud zur Wahrung der Datensicherheit unter europäischen Normen und Werten*
- ○ *Die Gewährleistung von Informationssicherheit (z.B. firmeninterne Informationen werden nicht ohne Befugnis an ausländische Plattformen weitergegeben)*
- ○ *Bereitstellung von Kapazitäten für Analyse und Überwachung von Software und Hardware*
- ○ *Weiterentwicklung von Software oder Informationssystemen*
- ○ *Anbieten BWI-eigener Produkte für den Bund (z.B. künftig KI-Systeme)*
- ○ *Überdenken vorherrschender Partnerschaften (z.B. präferiert Technologiepartner, die europäisch-demokratische Werte vertreten)*
- ○ *Mehr Regulierungen für die BWI (z.B. stärkere Regeln zur Wahrung der Privatsphäre im Cyberspace)*
- ○ *Strengere Einhaltung von Datenschutz und Umsetzung der DSGVO*
- ○ *Keins davon*
- ○ *Sonstiges:* _____

_____

Erstellt am: 09.06.2022
Erstellt von: Martha Klare

Seite 4/18

Abbildung 5: Fragebogen erste Fallstudie (4/18)

3. Was hat die BWI in der Vergangenheit bereits getan, um digital souveräner zu werden? (Mehrfaches Ankreuzen möglich)

- o *Ausbau der Sicherheitsmechanismen im Cyberspace*
- o *Ausbau eines Entwicklungs-Ökosystems (z.B. für App-Entwicklung oder Applikationen, die zugänglich für alle im Unternehmen sind)*
- o *Schaffung von Interoperabilität (=nahtlose Zusammenarbeit von Systemen)*
- o *Schaffung regulierender Rahmenbedingungen (z.B. festgelegte Standortmöglichkeiten für unternehmensinterne Rechenzentren)*
- o *Schaffung innovationsfreudiger Rahmenbedingungen (z.B. Förderung potenzieller Innovationsfelder)*
- o *Förderung von Forschungsprojekten (z.B. mit der UniBw München)*
- o *Mehr Eigenentwicklung ggü. dem Kauf ausländischer Software*
- o *Nichts davon*
- o *Sonstiges:* _____

_____

Abbildung 6: Fragebogen erste Fallstudie (5/18)

4. Was wird die BWI in Zukunft noch tun, um sich digital souveräner aufzustellen?
(Mehrfaches Ankreuzen möglich)

- ○ *Ausbau der Sicherheitsmechanismen im Cyberspace*
- ○ *Ausbau eines Entwicklungs-Ökosystems (z.B. für App-Entwicklung oder Applikationen, die zugänglich für alle im Unternehmen sind)*
- ○ *Schaffung von Interoperabilität (=nahtlose Zusammenarbeit von Systemen)*
- ○ *Schaffung regulierender Rahmenbedingungen (z.B. festgelegte Standortmöglichkeiten für unternehmensinterne Rechenzentren)*
- ○ *Schaffung innovationsfreudiger Rahmenbedingungen (z.B. Förderung potenzieller Innovationsfelder)*
- ○ *Förderung von Forschungsprojekten (z.B. mit der UniBw München)*
- ○ *Mehr Eigenentwicklung ggü. dem Kauf ausländischer Software*
- ○ *Nichts davon*
- ○ *Sonstiges:* _____

_____

Abbildung 7: Fragebogen erste Fallstudie (6/18)

5. Wie gut ist die BWI derzeit im Eigenbetrieb in folgenden Themen aufgestellt?

- *Softwareentwicklung*

  sehr schlecht *eher schlecht* *eher gut* *sehr gut*

- *Cyber-Security*

  sehr schlecht *eher schlecht* *eher gut* *sehr gut*

- *Umgang mit Big Data und Smart Data*

  sehr schlecht *eher schlecht* *eher gut* *sehr gut*

- *Umgang mit Cloud-Diensten*

  sehr schlecht *eher schlecht* *eher gut* *sehr gut*

- *Umgang mit Open-Source-Software*

  sehr schlecht *eher schlecht* *eher gut* *sehr gut*

- *Datensouveränität*[3]

  sehr schlecht *eher schlecht* *eher gut* *sehr gut*

[3] selbstbestimmte Kontrolle über Erhebung, Speicherung, Nutzung und Verarbeitung eigener Daten

Abbildung 8: Fragebogen erste Fallstudie (7/18)

6. Welche der in Punkt 5 genannten Punkte empfinden Sie am wichtigsten zur Stärkung der digitalen Souveränität der BWI?

- ○ *Softwareentwicklung*
- ○ *Cyber-Security*
- ○ *Umgang mit Big Data und Smart Data*
- ○ *Umgang mit Cloud-Diensten*
- ○ *Umgang mit Open-Source-Software*
- ○ *Datensouveränität*
- ○ *Keins davon*

7. *Gibt es noch weitere als die in Frage 6 genannten Punkte, die Sie als wichtig für die Stärkung digitaler Souveränität der BWI erachten?*

_____

_____

Abbildung 9: Fragebogen erste Fallstudie (8/18)

8. Was muss die BWI verändern, um digitale Souveränität stärker treiben zu können?

- o *Verantwortlichkeiten festlegen*
- o *Die Anforderungen des Staates auf das eigene Unternehmen herunter brechen*
- o *Den Kunden bei der Entwicklung von Maßnahmen involvieren*
- o *Mehr Kooperationen mit Unternehmen aus potenziellen innovationstreibenden Bereichen inkludieren (z.B. Quantum-Computing)*
- o *Stärkere Überprüfung potenzieller Unterauftragnehmer vollziehen*
- o *Schaffung von Transparenz bei Entscheidungssystemen*
- o *Schnellere Anpassungen der eigenen IT-Infrastruktur ermöglichen*
- o *Neuartige Technologien für den Kunden bereitstellen (z.B. KI)*
- o *Keins davon*
- o *Sonstiges:* _____

_____

Abbildung 10: Fragebogen erste Fallstudie (9/18)

der Bundeswehr Universität München

BWI IT für Deutschland

frei verwendbar

Fragebogen zum Thema digitale Souveränität

9. Inwieweit glauben Sie, dass die BWI die eigenen Angebote digital souveräner gestalten sollte?

.	.	.	.
Gar nicht	*wenig*	*schon eher*	*sehr*

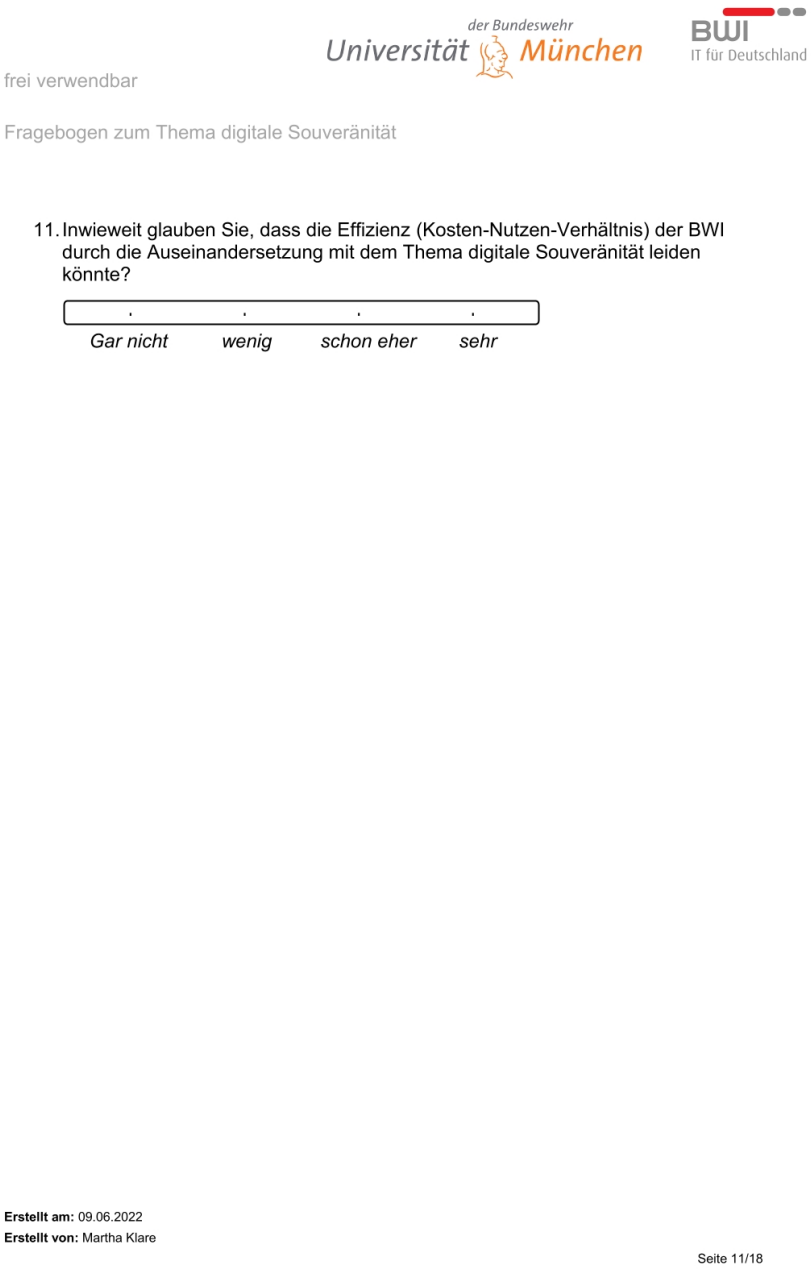
10. Wie könnte man Ihrer Meinung nach die Souveränität von Angeboten (z.B. Software) der BWI stärken?

- ○ *Prüfung auf Informations- und Wissenszugang (z.B. Zugang zu Berechnungen und Ergebnissen)*
- ○ *Prüfung auf Selbstbestimmung bei Entscheidungen (z.B. Möglichkeit zu prüfen, ob die eigenen unternehmerischen Anforderungen umgesetzt wurden)*
- ○ *Prüfung auf Handlungsfreiheit im Rahmen der Entwicklung und Anwendung eines digitalen Produkts (z.B. Zugang zu Ressourcen und Kenntnissen)*
- ○ *Prüfung auf die Einhaltung von unternehmerischen Sicherheitsanforderungen (z.B. lt. Eigentümerstrategie)*
- ○ *Prüfung auf die Gewährleistung von Resilienz*
- ○ *Prüfung auf die Gewährleistung von Nachhaltigkeit*
- ○ *Prüfung auf Harmonisierung der IT-Landschaft (z.B. Vereinheitlichung von Tools, die ähnliche Funktionen aufweisen)*
- ○ *Keins davon*
- ○ *Sonstiges:* _____

_____

Erstellt am: 09.06.2022
Erstellt von: Martha Klare

Abbildung 11: Fragebogen erste Fallstudie (10/18)



der Bundeswehr Universität München

BWI IT für Deutschland

frei verwendbar

Fragebogen zum Thema digitale Souveränität

11. Inwieweit glauben Sie, dass die Effizienz (Kosten-Nutzen-Verhältnis) der BWI durch die Auseinandersetzung mit dem Thema digitale Souveränität leiden könnte?

Gar nicht | wenig | schon eher | sehr

Erstellt am: 09.06.2022
Erstellt von: Martha Klare

Seite 11/18

Abbildung 12: Fragebogen erste Fallstudie (11/18)

frei verwendbar

Fragebogen zum Thema digitale Souveränität

Digitale Souveränität aus Sicht der IT-Beratung

12. Welche Schwerpunkte muss man in der IT-Beratung legen, um digital souverän zu sein?

- ○ *Unterstützung bei der Entwicklung und Umsetzung einer Datenstrategie*
- ○ *Unterstützung bei der Anpassung des IT-Portfolios (u.a. Ausrichtung des IT-Portfolios auf die digitalen Souveränitätsanforderungen des Unternehmens)*
- ○ *Unterstützung bei der Nutzung von Netzwerkeffekten (z.B. Zusammenarbeit mit Forschungsinstituten)*
- ○ *Unterstützung bei der Auswahl von Kooperationspartnern (z.B. den verbraucherorientierten Datenschutz fördern)*
- ○ *Unterstützung bei internen Prozessanpassungen*
- ○ *Unterstützung im Veränderungsprozess (z.B. Mitarbeiter-Pflichtschulungen zum Thema)*
- ○ *Sonstiges:* _____

_____

Erstellt am: 09.06.2022
Erstellt von: Martha Klare

Seite 12/18

Abbildung 13: Fragebogen erste Fallstudie (12/18)

frei verwendbar

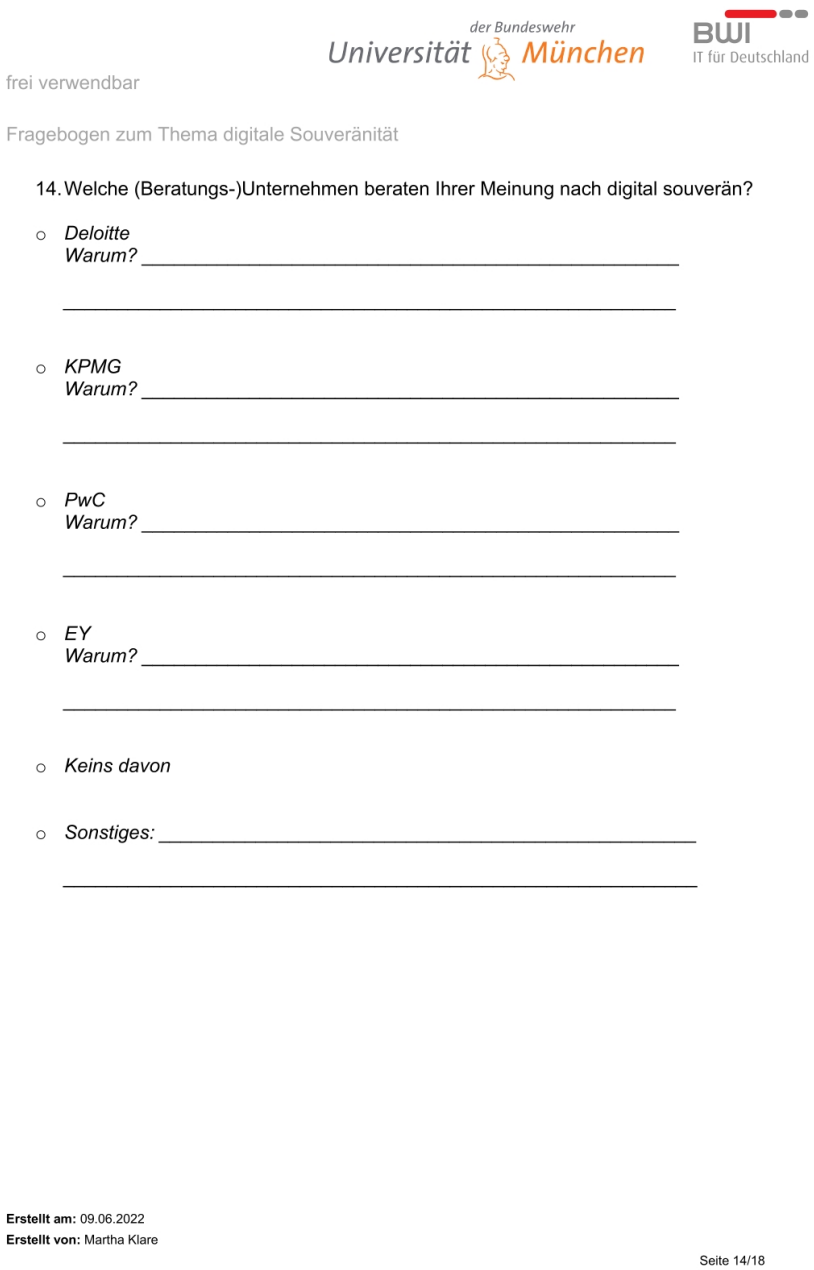
Fragebogen zum Thema digitale Souveränität

13. Welche (Beratungs-)Unternehmen würden sie einem hohen Grad an digitaler Souveränität zuschreiben und warum?

- ○ *Deloitte*
  Warum? _____
  _____
- ○ *KPMG*
  Warum? _____
  _____
- ○ *PwC*
  Warum? _____
  _____
- ○ *EY*
  Warum? _____
  _____
- ○ *Keins davon*
- ○ *Sonstiges:* _____
  _____

Erstellt am: 09.06.2022
Erstellt von: Martha Klare

Abbildung 14: Fragebogen erste Fallstudie (13/18)



der Bundeswehr Universität München

BWI IT für Deutschland

frei verwendbar

Fragebogen zum Thema digitale Souveränität

14. Welche (Beratungs-)Unternehmen beraten Ihrer Meinung nach digital souverän?

- ○ *Deloitte*
  Warum? _____
  _____
- ○ *KPMG*
  Warum? _____
  _____
- ○ *PwC*
  Warum? _____
  _____
- ○ *EY*
  Warum? _____
  _____
- ○ *Keins davon*
- ○ *Sonstiges:* _____
  _____

Erstellt am: 09.06.2022
Erstellt von: Martha Klare

Seite 14/18

Abbildung 15: Fragebogen erste Fallstudie (14/18)

15. In welchen Fällen würden Sie Kooperationen mit anderen Unternehmen in Erwägung ziehen, um ihre digitale Souveränität zu erhöhen?

- o *Zum Know-How-Austausch (z.B. Einholen von Best Practices)*
- o *Bei der Entwicklung von KI-Modellen*
- o *Bei der Entwicklung einer eigenen Cloud-Lösung*
- o *Zur Stärkung der Privatsphäre und des Schutzes eigener Daten*
- o *Um Bildungsangebote für Mitarbeiter einzuholen*
- o *Bei keinem der genannten Fälle*
- o *Sonstiges:* _____

_____

Abbildung 16: Fragebogen erste Fallstudie (15/18)

16. In welchen der folgenden Fälle könnte Ihrer Meinung nach die interne IT-Beratung besonders gut die BWI unterstützen?

- ○ *Nutzung BWI-externer Potenziale*

  ☐ . ☐ . ☐ . ☐ .
  Gar nicht *wenig* *schon eher* *sehr*

- ○ *Einhaltung von Datenschutz-Anforderungen*

  ☐ . ☐ . ☐ . ☐ .
  Gar nicht *wenig* *schon eher* *sehr*

- ○ *Nachhaltige Entwicklung*

  ☐ . ☐ . ☐ . ☐ .
  Gar nicht *wenig* *schon eher* *sehr*

- ○ *Krisenfestigkeit*

  ☐ . ☐ . ☐ . ☐ .
  Gar nicht *wenig* *schon eher* *sehr*

- ○ *Bei keinem der genannten Fälle*

- ○ *Sonstiges:* _____

  _____

17. Inwieweit glauben Sie, dass die Einführung von Open-Source-Software[4] bei der Stärkung digitaler Souveränität helfen könnte?

☐ . ☐ . ☐ . ☐ .
Gar nicht *wenig* *schon eher* *sehr*

[4] Software, deren Quelltext öffentlich und von Dritten eingesehen werden kann

Abbildung 17: Fragebogen erste Fallstudie (16/18)

18. *Wenn Schieberegler auf "ein wenig oder sehr" gesetzt wurde:*
Glauben Sie, dass die IT-Beratung sinnvoll bei der Einführung von Open-Source-Software unterstützen kann?

- o Ja
- o nein

19. Würde die IT-Beratung der BWI bei der Anpassung folgender Punkte unterstützen, um die digitale Souveränität der BWI zu steigern?

- o *Ermittlung von Sicherheitslücken innerhalb des Unternehmens*
- o *Ermittlung von kritischen Prozessen im Kontext der digitalen Souveränität*
- o *Beschreibung von potenziellen, neuen Technologien (z.B. Blockchain)*
- o *Ermittlung von Gaps im Rahmen der grünen IT-Entwicklung für die Bw*
- o *Entwicklung einer Strategie zur Stärkung der digitalen Souveränität in der BWI*
- o *Keins davon*
- o *Sonstiges:* _____

_____

Abbildung 18: Fragebogen erste Fallstudie (17/18)

20. Wie kann das Bewusstsein der Mitarbeiter für das Thema digitale Souveränität in der BWI gestärkt werden?

- ○ Stärkere Vermittlung des Themas über die Geschäftsführung
- ○ Weiterbildung der Führungskräfte im Bereich der digitalen Souveränität
- ○ Schulungen für Mitarbeiter zum Thema (z.B. Pflichtschulungen)
- ○ Erweiterung der Medienkompetenz der Mitarbeiter (z.B. Erklärung bei neuen Einführungen)
- ○ Erweiterung der Arbeitskompetenz der Mitarbeiter (z.B. Vorgaben zur Betrachtung des Themas in den täglichen Arbeitsprozessen)
- ○ *Keins davon*
- ○ *Sonstiges:* _____

_____

Dankeschön :-)

Erstellt am: 09.06.2022
Erstellt von: Martha Klare

Abbildung 19: Fragebogen erste Fallstudie (18/18)

Board zur Befragung der Experten
Zweite Fallstudie: Interviewstudie zu Faktoren digitaler Souveränität aus Perspektive der IT-Beratung (Landesverteidigung)

1. Herzlich Willkommen!



2. Was ist digitale Souveränität?

„Digitale Souveränität" beschreibt die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können (vgl. Pohle, 2020). Man spricht bei digitaler Souveränität auch oft von einem Balanceakt zwischen Autarkie und Fremdbestimmung. Ist man fremdbestimmt, hat man kaum Handlungsmöglichkeiten, weil man sehr abhängig ist. Ist man autark, versucht man vollkommen unabhängig zu sein, also Kooperationen mit anderen auszuschließen. Digital souverän zu sein, heißt also aktionsfähig und autark Entscheidungen treffen zu können und trotzdem mit Unternehmen in der digitalen Welt zu kooperieren (vgl. Bitkom, 2015).

Abbildung 20: Leitfaden zweite Fallstudie (1/3)

3. Wie können sich Unternehmen digital souveräner aufstellen?

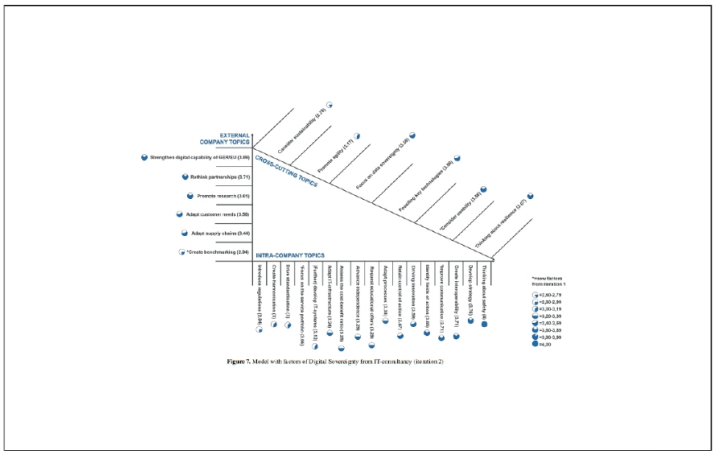


Figure 7. Model with factors of Digital Sovereignty from IT-consultancy (iteration 2)

Gibt es Faktoren, die in diesem Szenario, obsolet werden?

Obsolet nicht, aber es gibt Faktoren, die wichtiger sind, als andere. Ich würde das so gewichten:

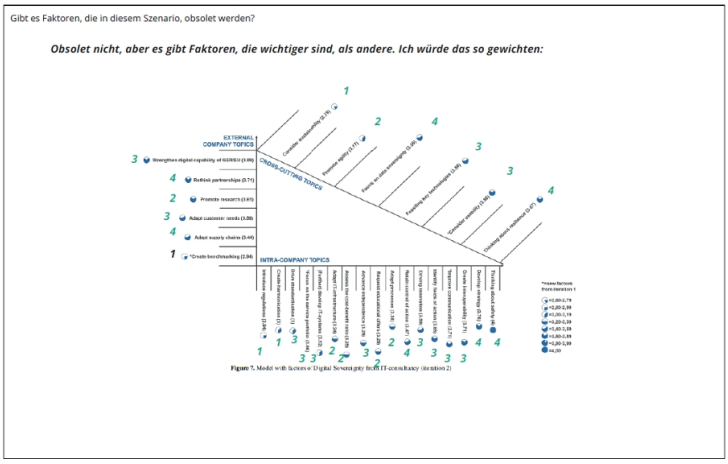
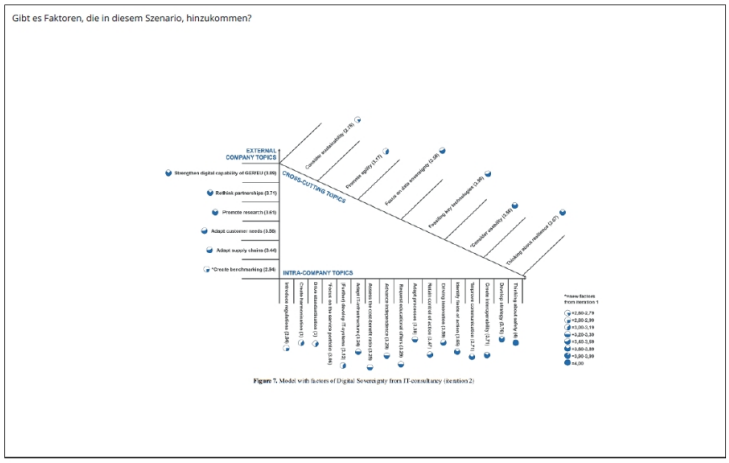


Figure 7. Model with factors of Digital Sovereignty from IT-consultancy (iteration 2)

Abbildung 21: Leitfaden zweite Fallstudie (2/3)



5. Ausblick

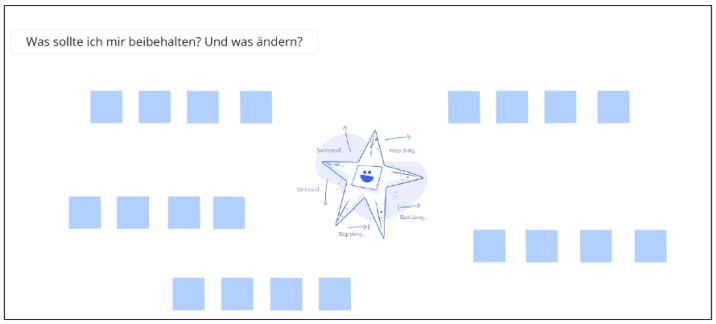
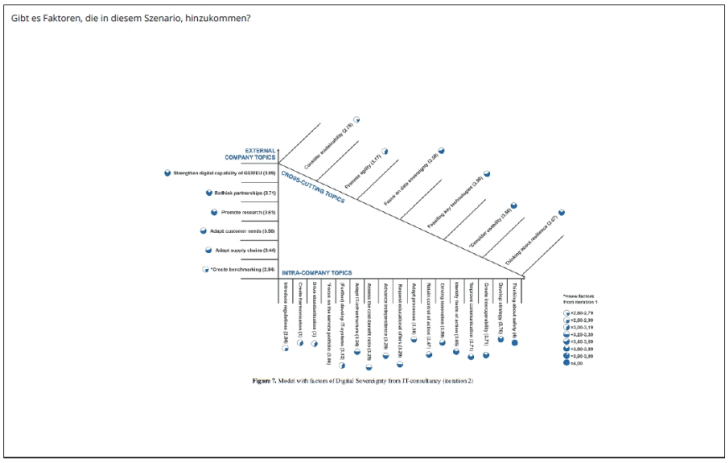


Abbildung 22: Leitfaden zweite Fallstudie (3/3)



5. Ausblick

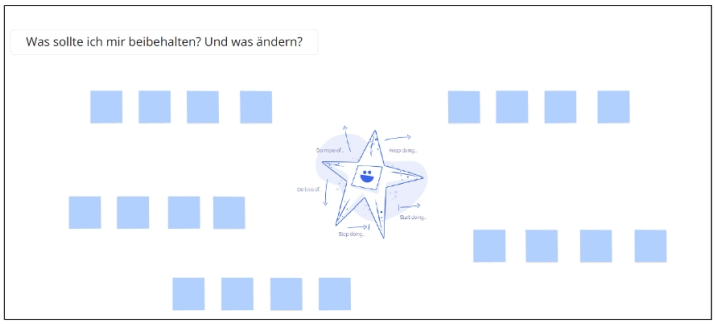
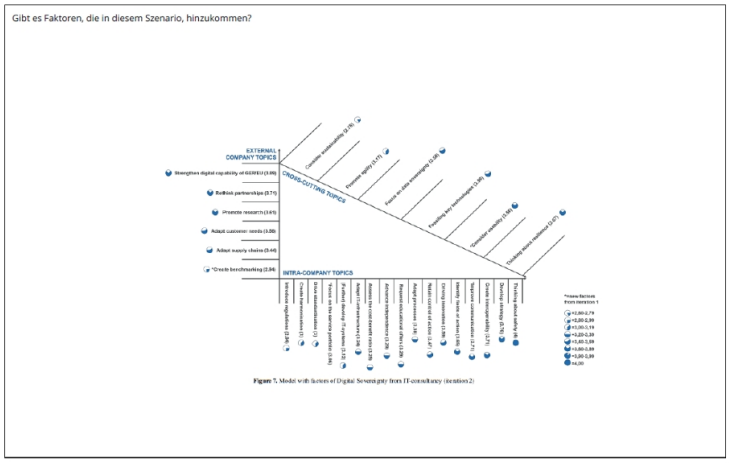


Abbildung 23: Leitfaden zweite Fallstudie (3/3)



5. Ausblick

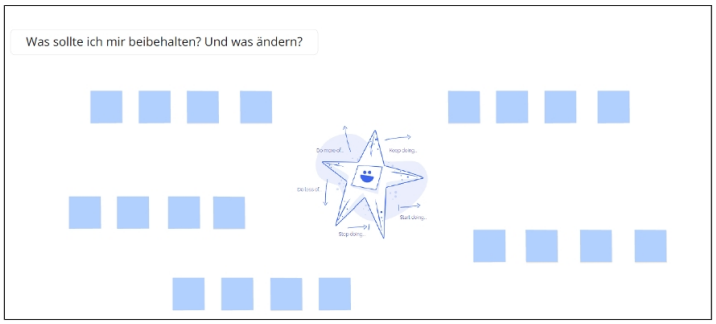


Abbildung 24: Leitfaden zweite Fallstudie (3/3)

Martha Klare 19.10.2022

Experteninterview: Stärkung der digitalen Souveränität Deutschlands im Kontext der China-Taiwan-Krise

Audio

Ich habe Ihnen heute einen Audio-Auszug aus der Tagesschau vom 10.08.2022 mitgebracht und würde Sie bitten sich diesen jetzt einmal im Hinblick auf die Frage anzuhören, ob sie die öffentliche Meinung zur China-Taiwan-Krise teilen, die hier dargestellt wird.

Audio anmachen

F1) Teilen Sie die Meinung aus dem Beitrag?

F2) Wie hoch würden Sie die Wahrscheinlichkeit einschätzen, dass die Handelsbeziehungen zwischen Deutschland und Taiwan bzw. China so bleiben wie sie es derzeit sind?

Universität der Bundeswehr München, Lehrstuhl Wirtschaftsinformatik,
Institut für Schutz und Zuverlässigkeit

Abbildung 25: Leitfaden dritte Fallstudie (1/14)

Martha Klare 19.10.2022

Digitale Souveränität [1]

F3) Inwieweit sollte sich Deutschland digital souveräner aufstellen?

Optionale Fragen

- ⇨ Welche Handelsoptionen schätzen Sie für uns als Staat besonders wichtig im Handel mit China ein?
- ⇨ Welche Branchen schätzen Sie für uns als Staat besonders wichtig im Handel mit Taiwan ein?

[1] „Digitale Souveränität" beschreibt „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können". Man spricht bei digitaler Souveränität auch oft von einem Balanceakt zwischen Autarkie und Fremdbestimmung. Ist man fremdbestimmt, hat man kaum Handlungsmöglichkeiten, weil man sehr abhängig ist. Ist man autark, versucht man vollkommen unabhängig zu sein, also Kooperationen mit anderen auszuschließen. Digital souverän zu sein, heißt also aktionsfähig und autark Entscheidungen treffen zu können und trotzdem mit Unternehmen in der digitalen Welt zu kooperieren.

Abbildung 26: Leitfaden dritte Fallstudie (2/14)

Martha Klare 19.10.2022

F4) Gehen wir mal davon auf folgendes Szanario trifft ein: China wird in Zukunft eine Intervention in Taiwan starten. Was sollte der Staat jetzt tun?

F5) Wir sind immer noch beim Szenario einer Intervention. Wie sollten sich Unternehmen auf ein derartiges Szenario vorbereiten?

F6) Was würde eine Intervention für Bürger und Bürgerinnen in Deutschland bedeuten?

Institut für Schutz und Zuverlässigkeit

Abbildung 27: Leitfaden dritte Fallstudie (3/14)

Martha Klare 19.10.2022

F7) Gehen wir mal davon aus, dass es weiterhin gewisse Handelswege über See oder Luft von Deutschland nach Taiwan sowie anders herum, gibt. Welche Strategie sollte die deutsche Regierung in diesem Szenario verfolgen?

F8) Welche Folgen hätten Sperrungen von Handelswegen für deutsche Unternehmen?

Optionale Fragen:

- ⇨ Das derzeit wertvollste Unternehmen Taiwans ist TSMC. TSMC beliefert weltweit riesige Konzerne mit Chips. Darunter gehören Unternehmen wie Apple, AMD, Intel, aber eben auch unsere deutschen Automobilkonzerne.
- ⇨ So stellt sich natürlich die Frage: Was tun, wenn wir nicht mehr so viele Chips aus Taiwan erhalten?

F9) Was würden Sperrungen von Handelswegen für Folgen für Bürger und Bürgerinnen in DEU haben?

Universität der Bundeswehr München, Lehrstuhl Wirtschaftsinformatik,
Institut für Schutz und Zuverlässigkeit

Abbildung 28: Leitfaden dritte Fallstudie (4/14)

Martha Klare 19.10.2022

F10) Gehen wir mal davon aus, dass die Handelsbeziehungen zwischen Deutschland und Taiwan bleiben wie sie grade sind. Sollte der Staat in diesem Szenario etwas anderes tun als das, was er derzeit tut?

F11) In dem Beitrag heißt es, dass sich deutsche Unternehmen ein zweites regionales Standbein aufbauen sollten. Wie sehen Sie diese Anforderung im Rahmen der derzeit debattierten Energie-Krise?

F12) Was können Bürger und Bürgerinnen tun, um mit dem Wandel zu gehen und den Bestrebungen des Staates und der Unternehmen, unabhängiger zu werden, mitzuhalten?

Abbildung 29: Leitfaden dritte Fallstudie (5/14)

Martha Klare 19.10.2022

Fragen, die auf die Profs ausgerichtet sind

F13) Inwieweit glauben Sie, dass es möglich ist, dass Start-Ups dabei helfen können, bestimmte Innovationen voranzutreiben und so die digitale Souveränität eines gesamten Staates zu stärken? *(allen stellen)*

F14) Im Audio heißt es, dass der Großteil der DAX-Unternehmen eine neue Regional- und Global-Strategie braucht. Was heißt das für unsere Lieferketten? *(nur den Betriebswirten stellen)*

Universität der Bundeswehr München, Lehrstuhl Wirtschaftsinformatik,
Institut für Schutz und Zuverlässigkeit

Abbildung 30: Leitfaden dritte Fallstudie (6/14)

Martha Klare 19.10.2022

F15) Im Audio heißt es: 1/3 der deutschen Produktion soll zurück nach Europa, Deutschland oder ins eigene Unternehmen gehen. Wie beurteilen Sie diese Aussage? Was hat diese Aussage ihrer Meinung nach für Konsequenzen? *(allen stellen)*

F16) Im Audio wurde der Faktor Sicherheit nicht betrachtet. Doch hier ein anderes Beispiel zur Unterstreichung der Anstrengungen im Kontext der digitalen Souveränität: das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 15.03, also knapp 3 Wochen nach Kriegsinvasion der Russen in die Ukraine eine Warnung ausgesprochen, die russische Viren-Software Kaspersky zu nutzen. Wie bewerten Sie diese Reaktion? *(allen stellen)*

Universität der Bundeswehr München, Lehrstuhl Wirtschaftsinformatik,
Institut für Schutz und Zuverlässigkeit

Abbildung 31: Leitfaden dritte Fallstudie (7/14)

Martha Klare 19.10.2022

F17) Data Science jetzt nur noch in Deutschland bzw. in Europa. Was halten Sie von dieser Aussage? *(an die (Wirtschafts-)Informatiker)*

F18) Die Debatte rund um die Stärkung digitaler Souveränität in Richtung China beschäftigt sich viel mit den Themen technologische Unabhängigkeit, Daten schützen, aber auch technischer Ethik. Sollte man Ihrer Meinung nach globalen Wettbewerb mit diesen Schlagworten verbinden? *(allen stellen)*

F19) Einige Experten sind der Meinung, dass sich digitale Souveränität ggü. China bzw. Taiwan nur erreichen lässt, wenn wir als Land oder auch im Konglomerat mit anderen europäischen Ländern innovieren. Die Vorreiter sollten Unternehmen sein, heißt es. Was sind denn ihrer Meinung nach die wichtigen und richtigen Innovationsbereiche? *(allen stellen)*

Institut für Schutz und Zuverlässigkeit

Abbildung 32: Leitfaden dritte Fallstudie (8/14)

Martha Klare 19.10.2022

Optionale Frage:

⇨ Wie sehen Sie das im Kontext der Lebensmittel-Handel?

F20) Das Zentrum für Digitale Souveränität der öffentlichen Verwaltung nimmt sich gegenwärtig vor, Ideen zu evaluieren und diese in Open-Source-Communities zu kommunizieren. Wie schaffen wir es mehr Ideen zu generieren und zu verwirklichen? *(nur für die (Wirtschafts-)Informatiker)*

F21) „Im Kontext technischer Souveränität wird mir zu viel über KI und Cloud gesprochen. Ich finde, dass mehr über Automatisierungstechnik im Maschinenbau gesprochen werden soll. Das ist meiner Meinung nach die größte Stärke Deutschlands", Zitat von Norbert Gaus (Vice President for Research and Development for Digitalization and Automation at Siemens Corporate Technology). Wie bewerten Sie diese Aussage? *(nur für die (Wirtschafts-)Informatiker)*

Abbildung 33: Leitfaden dritte Fallstudie (9/14)

Martha Klare 19.10.2022

F22) Während es im Jahr 2021 301 Unicorns[2] in China gab, kann Deutschland nur 26 Unicorns nachweisen. Wie bewerten Sie die Abstrebungen Deutschlands Innovationen fördern zu wollen, um digital souveräner zu werden, wenn Sie solche Zahlen hören? *(allen stellen)*

F23) Rund ein Drittel mehr deutsche Unternehmen haben im September die Insolvenz angemeldet, als im Vormonat August 2022. Das veröffentlichte diese Woche das Statistische Bundesamt. Welche Probleme bedingen dies ihrer Meinung nach im Zuge der digitalen Souveränität? *(allen stellen)*

[2] Junge, innovative Unternehmen, die eine Bewertung von mindestens einer Milliarde US-Dollar erhalten (siehe Anhang)

Abbildung 34: Leitfaden dritte Fallstudie (10/14)

Martha Klare 19.10.2022

F24) Die chinesische KI-Forschung wird für den freizügigen Umgang mit schützenswerten Daten chinesischer Bürger und Bürgerinnen scharf von der europäischen Seite kritisiert. Die Entwicklung von KI dürfe nicht auf Kosten der Privatsphäre gehen, heißt es in einem Bericht der Konrad Adenauer Stiftung. Um jedoch mit der Forschung Chinas Schritt halten zu können, brauchen Forscher und Unternehmer mehr Daten zum Experimentieren. Wie kommen wir an diese Daten? *(nur den Wirtschafts-)Informatikern stellen)*

Optionale Frage:

⇨ Um Schritt halten zu können. Gibt es Alternativen?

F25) Im Diskurs rund um das Thema digitale Souveränität wird häufig auch über digitale Ethik gesprochen, sprich über regulative Vorgaben und Normen im digitalen Raum, die nachvollziehbar und legitim sind. Welche Themen scheinen Ihnen in diesem Kontext besonders wichtig (z.B. ethische KI)? *(nur den Betriebswirten stellen)*

Universität der Bundeswehr München, Lehrstuhl Wirtschaftsinformatik,
Institut für Schutz und Zuverlässigkeit

Abbildung 35: Leitfaden dritte Fallstudie (11/14)

Martha Klare 19.10.2022

F26) “Am Ende werden wir uns entscheiden müssen, China oder die USA”, so heißt es im Audio. Wie ist Ihre Einschätzung zu dieser Aussage? Müssen wir uns Ihrer Meinung nach wirklich Software- und Hardwaretechnisch für einen der großen Wirtschaftsmächte entscheiden? *(allen stellen)*

F27) Würde man die Bundesrepublik als Unternehmen betrachten, so könnte man sich jetzt die Frage stellen: Wie viel sollte man als Republik selbst bauen und wie viel einkaufen? Gibt es Ihrer Meinung nach hierfür auch eine “80-20-Regel”? *(allen stellen)*

F28) Im Video heißt es, dass uns ein Stopp einer Kooperation mit China 6x so viel kosten könnte wie der Brexit. Wie bewerten Sie diese Aussage? *(allen stellen)*

Universität der Bundeswehr München, Lehrstuhl Wirtschaftsinformatik,
Institut für Schutz und Zuverlässigkeit

Abbildung 36: Leitfaden dritte Fallstudie (12/14)



Martha Klare 19.10.2022

F29) Gibt es sonstige Punkte, die man im Rahmen der Stärkung digitaler Souveränität aus Sicht ihres Fachgebiets diskutieren sollte?

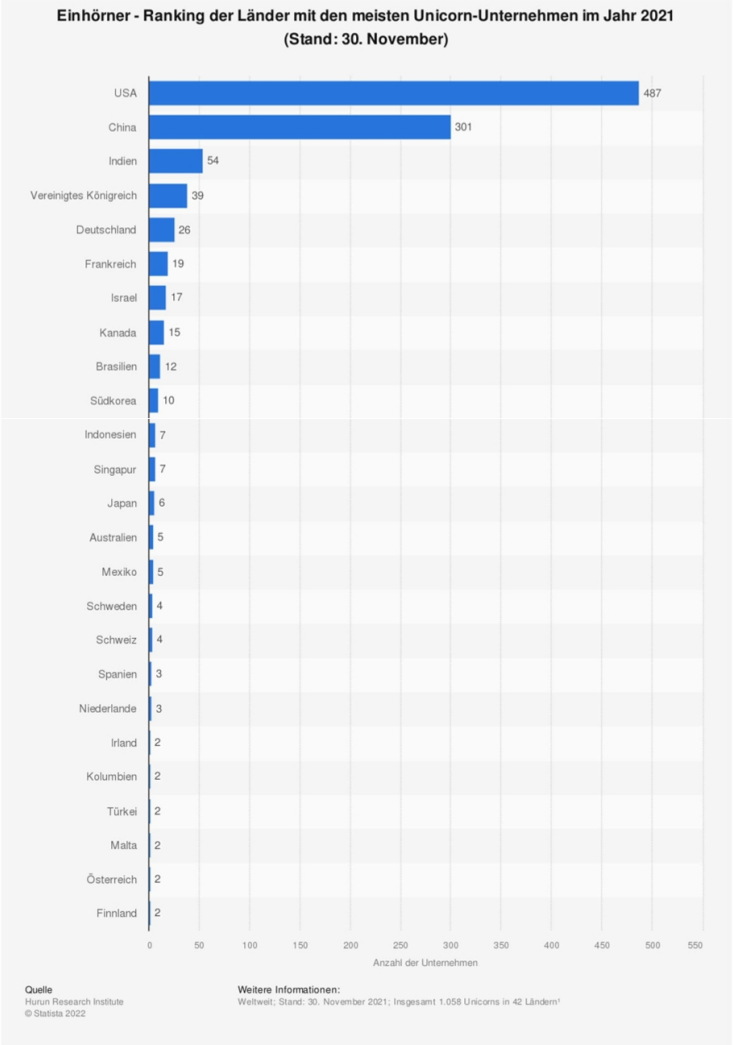
F30) Mit wem sollte ich mich Ihrer Meinung nach sonst noch zum Thema digitale Souveränität unterhalten?

Universität der Bundeswehr München, Lehrstuhl Wirtschaftsinformatik,
Institut für Schutz und Zuverlässigkeit

Abbildung 37: Leitfaden dritte Fallstudie (13/14)

Martha Klare 19.10.2022

Anhang



Universität der Bundeswehr München, Lehrstuhl Wirtschaftsinformatik,
Institut für Schutz und Zuverlässigkeit

Abbildung 38: Leitfaden dritte Fallstudie (14/14)

Fragenliste zum Papier
How Blockchain and Artificial Intelligence influence Digital Sovereignty

Nr.	Themenkomplex	Fragetyp	Frage	Antwortmöglichkeit
1.	Demographie	geschlossen	In welchen Branchen /Sektoren ist Ihr Unternehmen aktiv?	Einzelhandel, Großhandel, Transport- und Logistik, Unternehmensberatung, Information- und Kommunikation, Öffentliche Verwaltung, Verteidigung, Handel, Finanz- und Versicherungsdienstleistungen, Erbringung von sonstigen Dienstleistungen, Autombilindustrie
2.		geschlossen	Wieviele Mitarbeiter beschäftigt Ihr Unternehmen?	1-99, 100-249, 250-1000, >1000
3.		geschlossen	Welchen Umsatz hatte Ihr Unternehmen im letzten Jahr?	0-50 Mio, 51-100 Mio., >100 Mio.
4.		geschlossen	Was ist Ihre aktuelle Postion im Unternehmen?	Inhaber, Geschäftsführer, Management-Ebene, Abteilungsleiter, Angestellter/ Sachbearbeiter, andere
5.		geschlossen	Welcher Altersgruppe gehören Sie an:	18-24, 25-34, 35-44, 45-59, 60 und älter
6.		geschlossen	Inwieweit hat sich Ihr Unternehmen in den letzten Jahren mit der Einführung neuer Technologien (z.B. KI	gar nicht, wenig, stark, sehr stark

Abbildung 39: Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (1/13)

			oder Blockchain) beschäftigt?	
7.	Digitale Souveränität	geschlossen	Wie stark haben Sie sich mit dem Thema "digitale Souveränität" auseinander gesetzt?	gar nicht, wenig, stark, sehr stark, weiß nicht
8.		geschlossen/ offen	Welche der folgenden Begriffe machen für Sie digitale Souveränität aus?	Unabhängigkeit bei der Wahl von IT-Produkten (gar nicht, wenig, stark, voll und ganz, weiß nicht) Selbstbestimmtheit bei der Wahl von Lieferanten/Dienstleistern (gar nicht, wenig, stark, voll und ganz, weiß nicht) Entscheidungsfreiheit beim Umgang mit Daten (z.B. ausländische vs. inländische Cloud-Dienste) (gar nicht, wenig, stark, voll und ganz, weiß nicht) Transparenz der eigenen IT-Architektur (gar nicht, wenig, stark, voll und ganz, weiß nicht) Einhaltung rechtlicher Rahmenbedingungen (z.B. DSGVO)

Abbildung 40: Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (2/13)

				(gar nicht, wenig, stark, voll und ganz, weiß nicht) Beteiligte mit ähnlichen staatlichen Werten (z.B. demokratische Länder) (gar nicht, wenig, stark, voll und ganz, weiß nicht) Einsehbarkeit von Quellcode (z.B. Open Source vs. lizensiert) (gar nicht, wenig, stark, voll und ganz, weiß nicht) Stärkung der IT-Sicherheit (gar nicht, wenig, stark, voll und ganz, weiß nicht)
9.		geschlossen	Wie hoch ist der Stellenwert für digitale Souveränität in Ihrem Unternehmen?	gar nicht vorhanden, niedrig, hoch, sehr hoch, weiß nicht
10.		geschlossen	Wie groß würden Sie das Interesse Ihres Unternehmens für digitale Souveränität einschätzen?	gar nicht, ein wenig, stark, sehr stark, weiß nicht
11.		geschlossen	Würden Sie Ihr Unternehmen als digital souverän bezeichnen?	gar nicht, ein wenig, stark, sehr stark, weiß nicht
12.		geschlossen/ offen	Was ist der Grund, dass sie Ihr Unternehmen als (besonders) digital souverän erachten? (Mehrfachauswahl	Datenhoheit, Transparenz, eigene Systeme, festgelegte Verantwortlichkeiten, vorhandenes

Abbildung 41: Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (3/13)

			möglich)	Entscheidungskonzept, andere
13.		geschlossen/ offen	Was ist der Grund, dass Sie den aktuellen Stand der Souveränität als niedrig einstufen? (Mehrfachauswahl möglich)	geringe Datenhoheit, wenig Transparenz, keine eigenen Systeme, keine festgelegten Verantwortlichkeiten, kein vorhandenes Entscheidungskonzept, andere
14.		geschlossen/ offen	Mit welchen der folgenden Mittel hat Ihr Unternehmen in der Vergangenheit seine digitale Souveränität gestärkt? (Mehrfachauswahl möglich)	Einführung von KI-Systemen zur Steuerung und Überwachung, Einführung von Blockchain zur Schaffung von Sicherheit, Transparenz und Effizienz, Betreiben herstellerunabhängige r Module (z.B. uneingeschränkte Kompatibilität von Software), Mitgestaltung von IT-Lösungen durch Zusammenarbeit mit Dritten (z.B. andere Unternehmen), Aufsetzen einer Strategie zur Stärkung der digitalen Souveränität (z.B. mit einem Anforderungskatalog), Aufbau eigener Kompetenzen (z.B. Weiterbildung der Mitarbeiter), Aufbau

Abbildung 42: Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (4/13)

				eigener Systeme, andere
15.		geschlossen/offen	Sehen Sie in Zukunft die Möglichkeit mit folgenden Mitteln die digitale Souveränität zu stärken? (Mehrfachauswahl möglich)	Einführung von KI-Systemen zur Steuerung und Überwachung, Einführung von Blockchain zur Schaffung von Sicherheit, Transparenz und Effizient, Betreiben herstellerunabhängiger Module (z.B. uneingeschränkte Kompatibilität von Software), Mitgestaltung von IT-Lösungen durch Zusammenarbeit mit Anbietern, Aufsetzen einer Strategie zur Stärkung digitaler Souveränität (z.B. mit einem Anforderungskatalog), Aufbau eigener Kompetenzen (z.B. Weiterbildung der Mitarbeiter), Aufbau eigener Systeme, andere
16.		geschlossen/offen	Was sind ihrer Meinung nach Hindernisse für Ihr Unternehmen, um digital souveräner zu werden? (Mehrfachauswahl möglich)	Finanzierung oder Mehrkosten, fehlende IT-Strategie, fehlende IT-Infrastruktur, fehlende Zuständigkeiten, Informationsdefizite, Abhängigkeit zum

Abbildung 43: Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (5/13)

				Anbieter, fehlendes Fachwissen, fehlendes Interesse, andere
17.		geschlossen	Wie sehr hat Ihr Unternehmen in der Vergangenheit bei der Beschaffung neuer Technologien darauf geachtet, dass diese digital souverän sind?	gar nicht, kaum, ein wenig, sehr, weiß nicht
18.		geschlossen	Ordnen Sie das Unternehmen innerhalb der Branche in Bezug auf souveränes Agieren ein?	Schieberegler: gar nicht, wenig, stark, sehr stark
19.		geschlossen	Empfinden Sie digitale Souveränität als Risiko für Ihr Unternehmen? (z.B. Effizienzverlust / Mehrkosten)	Schieberegler: gar nicht, wenig, stark, sehr stark
20.		geschlossen/offen	Welche der folgenden politischen Rahmenbedingungen würden für Ihr Unternehmen eine Möglichkeit darstellen, um digital souveräner zu agieren? (Mehrfachauswahl möglich)	Entwicklung einer nationalen Datenstrategie, Förderung der Interoperabilität, Förderung von Forschung&Entwicklung, Ausbau von Kooperationen mit EU-Ländern, Weiterbildungsangebote (z.B. zur Förderung des Bewusstseins), Open-Data-Strategien, Schaffung investionsfreudiger Rahmenbedingung (z.B. Steuersenkung), andere
21.		geschlossen	Wird die Bestimmungsfreiheit	ja, nein, weiß nicht

Abbildung 44: Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (6/13)

			Ihres Unternehmens durch die Konkurrenz eingeschränkt? (z.B. Wahl des Lieferanten/Dienstleisters)	
22.		geschlossen	Können Sie sich vorstellen, Daten/Informationen zur Steigerung der Transparenz der Wertschöpfungskette mit konkurrierenden Unternehmen zu teilen?	ja, nein, weiß nicht
23.		geschlossen	Wie wichtig ist Ihrem Unternehmen die Datenhoheit (Schutz der Informationen/Daten) im Zusammenhang mit digitaler Souveränität?	gar nicht, ein wenig, stark, sehr stark, weiß nicht
24.		geschlossen/offen	Welche Bereiche in Ihrem Unternehmen würden Sie als (bereits) digital souverän bezeichnen? (Mehrfachauswahl möglich)	Finanzwesen, Materialwirtschaft, Vertrieb, Personalwesen, Einkauf, Disposition, weiß nicht, Sonstige
25.	Blockchain	geschlossen	Wie sehr sind Sie mit dem Thema Blockchain vertraut?	gar nicht, wenig, stark, sehr stark
26.		geschlossen	Welche der folgendenden Charakteristika einer Blockchain sind Ihnen bereits vertraut? (Mehrfachauswahl möglich)	Fälschungssicherheit/ Integrität, dezentrale Speicherung der Daten, Transparenz, Ausfallsicherheit, Verzicht auf einen zentralen Vermittler oder Treuhändler, Vermeidung zentraler

Abbildung 45: Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (7/13)

				Datenhoheit, keine davon
27.		geschlossen	Welche der folgenden Einsatzmöglichkeiten von Blockchain sind Ihnen bereits bekannt? (Mehrfachauswahl möglich)	Kryptowährungen (z.B. Bitcoin), Verwalten von Echtzeitzertifikaten, Erfassung von Sensordaten, Automatisierung von (unternehmensübergreifenden) Prozessen (z.B. Smart Contracts), Verwalten von Eigentums-/ Urheberrechten, Verwalten von Grundbucheinträgen, Verwaltung von Identititäten, Rückverfolgbarkeit von Produkten, keine davon
28.		geschlossen	Wie hoch schätzen Sie die Eintrittswahrscheinlichkeit der folgenden Kriterien ein, weshalb ein Einsatz von Blockchain scheitern könnte?	Mehrkosten (sehr niedrig, niedrig, mittel, hoch, sehr hoch) fehlende Standards (sehr niedrig, niedrig, mittel, hoch, sehr hoch) fehlende Infrastruktur (sehr niedrig, niedrig, mittel, hoch, sehr hoch) fehlendes Fachwissen in Unternehmen (sehr niedrig, niedrig, mittel, hoch, sehr

Abbildung 46: Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (8/13)

				hoch) fehlendes Interesse (sehr niedrig, niedrig, mittel, hoch, sehr hoch) rechtliche Bedenken (sehr niedrig, niedrig, mittel, hoch, sehr hoch) Bedenken hinsichtlich erfolgreicher Implementierung (sehr niedrig, niedrig, mittel, hoch, sehr hoch)
29.		geschlossen	Existieren in Ihrem Unternehmen bereits ein oder mehrere Projekte in Verbindung mit Blockchain?	keine, theoretisch geplant, praktisch geplant, praktisch umgesetzt, weiß nicht
30.		geschlossen	Denken Sie, dass es mit Hilfe von Blockchain möglich ist, digital souverän zu agieren?	gar nicht, wenig, stark, sehr stark, weiß nicht
31.		geschlossen/ offen	Für welche Zwecke könnten Sie sich vorstellen Blockchain einzusetzen, um digital souveräner zu agieren? (Mehrfachauswahl möglich)	um Datenaustausch mit anderen Unternehmen transparenter gestalten zu können, um einen technologischen Vorteil ggü. Konkurrenten zu generieren, um Unveränderbarkeit der Daten zu gewährleisten, zur

Abbildung 47: Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (9/13)

				Produktnachverfolgung, andere
32.	Künstliche Intelligenz	geschlossen	Wie sehr sind Sie mit dem Thema KI vertraut?	gar nicht, wenig, stark, sehr stark
33.		geschlossen	Welcher der folgenden möglichen Charakteristika der KI sind Ihnen bereits bekannt? (Mehrfachauswahl möglich)	Transparenz, Effizienzsteigerung, eigenständig agierendes System (Autonomie), "Mensch als Maschine" (z.B. Chatbot), maschinelles Lernen, Adaptivität (z.B. individuelle Lernumgebung), keine davon
34.		geschlossen	Welche der folgenden Einsatzmöglichkeiten von KI sind Ihnen bereits bekannt? (Mehrfachauswahl möglich)	optische Inspektion (z.B. Qualitätssicherung), Fehler- oder Prozessanalyse, Prozessautomatisierung, Robotik, vorausschauende Datenanalyse, Mustererkennung und -analyse, Sprachsteuerung, Chatbots, Computerspiele, Texterkennung, smarte Systeme, keine davon

Abbildung 48: Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (10/13)

35.		geschlossen	Wie hoch schätzen Sie die Eintrittswahrscheinlichkeit der folgenden Kriterien ein, weshalb ein Einsatz von KI scheitern könnte?	Mehrkosten (sehr niedrig, niedrig, mittel, hoch, sehr hoch) fehlende Standards (sehr niedrig, niedrig, mittel, hoch, sehr hoch) fehlende Infrastruktur (sehr niedrig, niedrig, mittel, hoch, sehr hoch) fehlendes Fachwissen in Unternehmen (sehr niedrig, niedrig, mittel, hoch, sehr hoch) fehlendes Interesse (sehr niedrig, niedrig, mittel, hoch, sehr hoch) rechtliche Bedenken (sehr niedrig, niedrig, mittel, hoch, sehr hoch) Bedenken hinsichtlich erfolgreicher Implementierung (sehr niedrig, niedrig, mittel, hoch, sehr hoch)
36.		geschlossen	Existieren in Ihrem Unternehmen bereits ein oder mehrere Projekte in Verbindung	praktisch geplant, prakt

Abbildung 49: Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (11/13)

			mit KI?	
37.		geschlossen	Denken Sie, dass es mit Hilfe von KI möglich ist, digital souverän zu agrieren?	gar nicht, wenig, stark, sehr stark, weiß nicht
38.		geschlossen	Die Forschung beschäftigt sich mit einer Weiterentwicklung des maschinellen Lernens, genannt "Federated Learning", ist Ihnen diese Technologie bekannt?	ja, nein
39.	Filterfrage	geschlossen	Inwieweit denken Sie, dass Federated Learning dabei unterstützen kann die digitale Souveränität in ihrem Unternehmen zu steigern?	gar nicht, ein wenig, stark, sehr stark, weiß nicht
40.		geschlossen	Würden Sie Federated Learning als einen Lösungsansatz für digitale Souveränität sehen?	ja, nein, weiß nicht
41.		geschlossen/ offen	Für welche Zwecke könnten Sie sich vorstellen KI einzusetzen, um digital souveräner zu agieren? (Mehrfachauswahl möglich)	um Prozesse transparenter zu gestalten, um Prozesse einfach und verständlicher zu gestalten, um Prozessabläufe zu optimieren, um große Datensätze zu verwalten, um das Verständnis hinter System offen zu legen (z.B. Einsehbarkeit des Quellcodes), um

Abbildung 50: Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (12/13)

				Kommunikation transparenter und einfach zu gestalten, um die Wahl von Lieferanten/Dienstleistern/Services zu kontrollieren und zu optimieren, um die Autarkie bei Entscheidungen zu stärken, andere

Abbildung 51: Fragenliste zur Umfrage im Papier »How Blockchain and Artificial Intelligence Influence Digital Sovereignty« (13/13)

Interviewleitfaden zum Papier
Digital Sovereignty: Affordances in Open Source Projects

Eine kurze Einführung
Digitale Souveränität beschreibt das Ziel, dass Individuen, Unternehmen und staatliche Institutionen in der Lage sein sollten ihre Funktionen und Ideen in der digitalen Welt selbstbestimmt und sicher umsetzen zu können. Für Unternehmen bedeutet das, einen Balance-Akt zwischen mehr Unabhängigkeit und ausgewählten Kooperationen mit vertrauenswürdigen Partnern zu schaffen. Ein Beispiel: Es ist herausfordernd mit Monopolisten wie Microsoft über faire Preise und Konditionen, z.B. für Office, zu verhandeln. Auch die BWI nimmt sich gegenwärtig vor, von solchen Monopolisten unabhängiger zu agieren.
Open Source als eine zentrale Voraussetzung der Digitalen Souveränität
Ein zentrales Element zur Stärkung digitaler Souveränität sind Open Source Software. Da bei Open Source Software in der Regel Bestandteile (Bibliotheken, etc.) von einer Community frei zugänglich bereitgestellt werden, gibt es geringere Abhängigkeit von einzelnen Marktteilnehmern. So wird vermutet, dass man eine Reduktion von Vendor-Lock-Ins erreichen kann. Vendor-Lock-Ins entstehen, wenn es Unternehmen durch Wechselbarrieren (z.B. wegen Kostenvorteilen) erschwert wird, den Anbieter oder dessen Produkt zu wechseln.

Ziel dieser Erhebung
Ich will herausfinden, wo in Projekten bereits Erfolge ersichtlich sind, um Vendor-Lock-Ins zu reduzieren oder wo der „Schuh drückt“.

Deine Einschätzung ist gefragt: Was müssten wir tun, um das Ziel zu erreichen?
Allgemeine Antwort:
What should we do more of:
What should we do less of:
What should we start doing:
What should we stop doing:
What should we keep doing:

Abbildung 52: Interviewleitfaden zum Papier »Affordances in Open Source Projects«

Fragenliste zum Papier
Digital Sovereignty and Digital Transformation Practice Recommendation for the Software Life Cycle Process

Thema	***Antwortoption***
Alter	*jünger als 30; 31-41; 42-52, älter als 52*
Branche	*Branche: Automobilsektor, Marketing, Consulting, Forschung, Sonstiges (bitte eingeben)*
Zugehörigkeit	*Privater Sektor, öffentlicher Sektor*
Position	*Praktikant, Werkstudent, Specialist/Product Owner, Manager/Teamleiter, Senior/Project Manager, Head of/Abteilungsleiter, Director, C-Level*
Einordnung von Erfahrung	• *Erfahrung: Software-Entwicklung (sehr viel, viel, wenig, sehr wenig, gar keine)* • *Erfahrung: Software-Einkauf (sehr viel, viel, wenig, sehr wenig, gar keine)* • *Erfahrung: Software Lifecycle Management (sehr viel, viel, wenig, sehr wenig, gar keine)* • *Erfahrung: Digitale Souveränität (sehr viel, viel, wenig, sehr wenig, gar keine)* • *Erfahrung: Digitale Transformation (sehr viel, viel, wenig, sehr wenig, gar keine)*
Software-Einführung	*Systematische Einführung…* • *basierend auf Strategie und Anforderungen, z.B. durch Unternehmensmanagement, Produktmanagement, etc. (ja/nein)* • *Bei akuten Anforderungen aus den jeweiligen Fachbereichen (ja/nein)* • *auf Basis von Kundenanforderungen (ja/nein)* • *Durch Externe (Auditoren, Berater) initiiert (ja/nein)*
Sofware-Management	*nicht etabliert* *in Arbeit* *etabliert*
Sofware-Life-Cycle-Prozess	*nicht eingeführt* *eingeführt*
Software-Probleme	**4 Nennungen möglich**
Verständnis von digitaler Souveränität	**offene Antwort möglich**
Verständnis von digitaler Transformation	**offene Antwort möglich**

Abbildung 53: Interviewleitfaden zum Papier »Digital Sovereignty and Digital Transformation Practice Recommendation for the Software Life Cycle Process« (1/4)

Herausforderungen im Kontext digitaler Souveränität und digitaler Transformation	*Für digitale Souveränität:* • *Hohe Komplexität bei der Umstellung vorhandener Systeme und Prozesse* • *Fehlende Entscheidungsfreiheit bei der Wahl von IT-Produkten* • *Hohe Kosten* • *Abhängigkeit zu externen Lösungen* • *Technologieakzeptanz von Mitarbeitern* • *Fehlende digitale Kompetenzen* • *viele Risiken* • *Hohe Unsicherheiten* • *Fehlende technologische Standards* • *Zeit* • *Personelle Ressourcen* • *Kontrolle über eigene Daten* • *Transparenz* • *Entscheidungskonzepte* • *Zuständigkeiten* • *Regulierung* • *Strategie* • *Weiterbildungen* *Für digitale Transformation:* • *Hohe Komplexität bei der Umstellung vorhandener Systeme und Prozesse* • *Fehlende Entscheidungsfreiheit bei der Wahl von IT-Produkten* • *Hohe Kosten* • *Abhängigkeit zu externen Lösungen* • *Technologieakzeptanz von Mitarbeitern* • *Fehlende digitale Kompetenzen* • *viele Risiken* • *Hohe Unsicherheiten* • *Fehlende technologische Standards* • *Zeit* • *Personelle Ressourcen* • *Kontrolle über eigene Daten* • *Transparenz* • *Entscheidungskonzepte* • *Zuständigkeiten* • *Regulierung* • *Strategie* • *Weiterbildungen*
Priorisierung von Themen für digitale Souveränität	*Kosten, Komplexität, Entscheidungsfreiheit, Abhängigkeiten, Technologieakzeptanz, Digitale Kompetenzen,*
Priorisierung von Themen für digitale Souveränität	*Transparenz, Strategie, Weiterbildungen, Regulierungen, Entscheidungskonzepte, personelle Ressourcen,*
Maßnahmen für	*Für digitale Souveränität:*

Abbildung 54: Interviewleitfaden zum Papier »Digital Sovereignty and Digital Transformation Practice Recommendation for the Software Life Cycle Process« (2/4)

digitale Souveränität und digitale Transformation	• *Regelmäßige Schulungen* • *Sicherheitsbeauftragte* • *Beauftragung/Zusammenarbeit mit externen Dienstleistern* • *Sicherheitsmanagementsystem* • *Risikoanalysen* • *Risikobeauftragte* • *Verschlüsselung* • *Backups* • *Vertrauenswürdigkeit in Informationssystemen* • *Daten schützen und gleichzeitig nutzen* • *Verständnis und Beherrschung von Schlüsseltechnologien/ technologischen Standards* • *Strategische Partnerschaften im digitalen Raum nutzen/ technologische Vielseitigkeit* • *Analyse von Kosten und Nutzen bei der Auswahl von IT-Systemen* • *Kontrolle über Software sicherstellen/ Wahlfreiheit* • *Abhängigkeitsmanagement in der Lieferkette* • *Resilienz* *Für digitale Transformation* • *Regelmäßige Schulungen* • *Sicherheitsbeauftragte* • *Beauftragung/Zusammenarbeit mit externen Dienstleistern* • *Sicherheitsmanagementsystem* • *Risikoanalysen* • *Risikobeauftragte* • *Verschlüsselung* • *Backups* • *Vertrauenswürdigkeit in Informationssystemen* • *Daten schützen und gleichzeitig nutzen* • *Verständnis und Beherrschung von Schlüsseltechnologien/ technologischen Standards* • *Strategische Partnerschaften im digitalen Raum nutzen/ technologische Vielseitigkeit* • *Analyse von Kosten und Nutzen bei der Auswahl von IT-Systemen* • *Kontrolle über Software sicherstellen/ Wahlfreiheit* • *Abhängigkeitsmanagement in der Lieferkette* • *Resilienz*
Priorisierung von Themen für digitale Souveränität und digitale Transformation	*Vermittlung von Datenkompetenz, Schulungen zu Datensicherheit/Datenschutz, Schaffung von Akzeptanz/Mindset, Prozessverständnis und Veränderungsbereitschaft, Umgang mit neuen Technologien erlernen*
Strategie für digitale Souveränität und digitale Transformation	*Meinem Unternehmen fehlt eine Strategie für Digitale Souveränität* *Meinem Unternehmen fehlt eine Strategie für Digitale Transformation*

Abbildung 55: Interviewleitfaden zum Papier »Digital Sovereignty and Digital Transformation Practice Recommendation for the Software Life Cycle Process« (3/4)

digitale Souveränität und digitale Transformation	• *Regelmäßige Schulungen* • *Sicherheitsbeauftragte* • *Beauftragung/Zusammenarbeit mit externen Dienstleistern* • *Sicherheitsmanagementsystem* • *Risikoanalysen* • *Risikobeauftragte* • *Verschlüsselung* • *Backups* • *Vertrauenswürdigkeit in Informationssystemen* • *Daten schützen und gleichzeitig nutzen* • *Verständnis und Beherrschung von Schlüsseltechnologien/ technologischen Standards* • *Strategische Partnerschaften im digitalen Raum nutzen/ technologische Vielseitigkeit* • *Analyse von Kosten und Nutzen bei der Auswahl von IT-Systemen* • *Kontrolle über Software sicherstellen/ Wahlfreiheit* • *Abhängigkeitsmanagement in der Lieferkette* • *Resilienz* *Für digitale Transformation* • *Regelmäßige Schulungen* • *Sicherheitsbeauftragte* • *Beauftragung/Zusammenarbeit mit externen Dienstleistern* • *Sicherheitsmanagementsystem* • *Risikoanalysen* • *Risikobeauftragte* • *Verschlüsselung* • *Backups* • *Vertrauenswürdigkeit in Informationssystemen* • *Daten schützen und gleichzeitig nutzen* • *Verständnis und Beherrschung von Schlüsseltechnologien/ technologischen Standards* • *Strategische Partnerschaften im digitalen Raum nutzen/ technologische Vielseitigkeit* • *Analyse von Kosten und Nutzen bei der Auswahl von IT-Systemen* • *Kontrolle über Software sicherstellen/ Wahlfreiheit* • *Abhängigkeitsmanagement in der Lieferkette* • *Resilienz*
Priorisierung von Themen für digitale Souveränität und digitale Transformation	*Vermittlung von Datenkompetenz, Schulungen zu Datensicherheit/Datenschutz, Schaffung von Akzeptanz/Mindset, Prozessverständnis und Veränderungsbereitschaft, Umgang mit neuen Technologien erlernen*
Strategie für digitale Souveränität und digitale Transformation	*Meinem Unternehmen fehlt eine Strategie für Digitale Souveränität* *Meinem Unternehmen fehlt eine Strategie für Digitale Transformation*

Abbildung 56: Interviewleitfaden zum Papier »Digital Sovereignty and Digital Transformation Practice Recommendation for the Software Life Cycle Process« (4/4)

Universität der Bundeswehr München BWI IT für Deutschland

Fragebogen zum Innovationspotenzial von Sovereign Clouds

Ziel:

- Bewertung von sovereign clouds in verschiedenen Branchen
- Identifikation von Innovationspotenzialen oder Einschränkungen

---

Fragen:

Hintergrundinformationen

- In welcher Position arbeiten Sie?
- Wie lange arbeiten Sie bereits in dieser Position?
- Welche Erfahrungen haben Sie bereits mit dem Thema Sovereign Clouds gemacht? (sehr wenig, wenig, viel, sehr viel)

Einführung:

- Wie betrifft Sie das Thema Cloud im Arbeitsalltag?
- Was verstehen Sie unter dem Begriff >>Sovereign Cloud<<?
- Was motiviert Ihrer Meinung nach die Nutzung des Worts >>sovereign<<?

Deep Dive

- Welche Anwendungsfelder sehen Sie für Sovereign Clouds? (Kontrolle über getrennte Netzwerkereiche, Kontrolle über Zugriffskontrollen, Kontrolle über Datenverlauf, Sonstiges)
- Welche Vorteile sehen Sie bei der Nutzung von den public cloud Angeboten der gängigen Hyperscaler im Vergleich zu Sovereign Clouds? (Betriebliche Unterstützung, Skalierungsmöglichkeiten, Bereitstellung eines Data Centers, Best Practices, Support, Sonstiges)

Praxisperspektive

- Wo würden Sie für ihr Unternehmen die größten Herausforderungen für die **Nutzung** von Sovereign Clouds sehen? (Finden geeigneter Partner/Provider, Robustheit/Resilienz der Sovereign Cloud, Disaster Recovery, Kosten, Mehraufwand, Fachexpertise, Datenmigration, Zugriff auf Internetverbindung, Sonstiges)
- Wo würden Sie für ihr Unternehmen die größten Herausforderungen für die **Einführung** von Sovereign Clouds in der Praxis sehen? (s.o.)
- Bitte ranken Sie. Was ist für Sie der größte wahrnehmbare Mehrwert einer SovereignCloud? (Einhaltung spezifischer gesetzlicher Spezifikationen, mehr Sicherheit der Daten, Umgang mit Komplexität (z.B. bei Vorschriften))

Einschätzung

Durch die Nutzung einer Sovereign Cloud verändert sich offensichtlich die Wettbewerbssituation eines Unternehmens. Es kann Leistungen anbieten, die es vorher nicht anbieten konnte oder die preislich zu teuer gewesen wären. Das Unternehmen geht auch andere Geschäftsbeziehungen ein und teilt Aufgaben anders mit Partnerunternehmen auf. Wir würden nun gerne verstehen, die die Sovereign Cloud die Entwicklungsrichtungen verändert, in die sich das Unternehmen weiterentwickeln kann.

1. *Gewährleistung von mehr IT-Security.*
   - Sind Sie der Meinung, dass Unternehmen nun mit der Einführung einer SC tatsächlich besser geschützt sind gegen…
     - Eindringlinge von außen (z.B. Datenklau, usw.)? (ja, nein)
     - Schwachstellen (ja, nein)
     - Unerwünschte Funktionalitäten bei der Datenverarbeitung (z.B. Möglichkeit eines Mithörens) (ja, nein)

Abbildung 57: Fragebogen zum Papier »Digital Sovereignty through Sovereign Clouds« (1/2)

2. *Schaffung von Resilienz*
   - Sind Unternehmen mit einer SC ihrer Meinung nach nun eher in der Lage…
     - sich schnell von unerwünschten Ereignissen zu erholen? (ja, nein)
     - schnell auf Probleme zu reagieren? (ja, nein)
3. *Digitale Supply Chain*
   - Sind Unternehmen mit einer SC ihrer Meinung nach nun in der Lage mehr Kontrolle über ihre digitale Supply Chain zu erreichen? (ja, nein)
   - Wird die digitale Supply Chain durch die Wahl vertrauenswürdiger Provider ihrer Meinung nach sicherer? (ja, nein)
4. *Entwicklung von Kernkompetenzen.*
   - (Wo) bietet ihr Unternehmen eigene Expertise im Kontext von SC an? (ja, nein)
   - Bitte ranken Sie. Wo würde sich ihr Unternehmen bei der Nutzung einer SC am ehesten auf andere Kompetenzen verlassen? (Technologiekompetenz, Fachkompetenz, Sicherheit&Datenschutz)
5. *Zugang zu Kunden.*
   - Welche neuen Kunden/Märkte werden durch die Nutzung erschließbar? (Kunden im public sector, Kunden im private sector)
   - Welche neuen Werteversprechen kann Ihr Unternehmen diesen Kunden machen? (mehr Kontrolle über Daten, Stärkung digitaler Fähigkeiten und Wertevorstellungen Europas, nachhaltige Lösung, hohe Usability, hohe Standardisierung bei gleichzeitiger Interoperabilität, Sonstiges)
   - Welche Werteversprechen kann es NICHT mehr machen, durch Einschränkungen der Sovereign Cloud?
6. *Umgang mit Konkurrenz.*
   - Ist Ihr Unternehmen durch die Wahl beschränkt bei der Expansion (z.B. in asiatische Märkte)? (ja, nein)
   - Wie verändert sich die Position Ihres Unternehmens, d.h. mit wem muss es jetzt konkurrieren im Unterschied zu vorher?
7. *Technologieoffenheit.*
   - Werden Technologien und Services Ihrer Meinung nach mit der SC langsamer eingeführt? (ja, nein)
   - Wie schwer ist es, die Entscheidung für die Cloud rückgängig zu machen? (gar nicht schwer, eher schwer, eher leicht, sehr leicht)
   - Welche Möglichkeiten bestehen für Ihr Unternehmen, auf Preisveränderungen bei den Cloudanbietern zu reagierten? (wir haben gar keinen, eher wenig, viel, sehr viel Handlungsspielraum)

Ausblick

- Glauben Sie, dass es in Zukunft mit der SC…
  - Weniger Aufwände gibt hinsichtlich Cybersicherheit? (ja, nein)
  - Einfacher ist mit politischen Problemen umzugehen? (ja, nein)
  - Einfacher ist mit geopolitischen Veränderungen umzugehen? (ja, nein)
- Glauben Sie, dass die Einführung von SC die Wettbewerbsfähigkeit von Unternehmen langfristig einschränkt? (ja, nein)

Abbildung 58: Fragebogen zum Papier »Digital Sovereignty through Sovereign Clouds« (2/2)