# Digitale Souveränität – Wie kann das gelingen ?

Ulrike Lechner

Juni 2025,
IKT-Sicherheitskonferenz Dornbirn



gefördert durch
dtec.bw

Finanziert von der Europäischen Union
NextGenerationEU

# LIONS & CONTAIN


dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Funded by the European Union
NextGenerationEU


Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
FKZ 13N16581-13N16587

Bundesministerium Finanzen

SIFO.de

KIRAS Sicherheitsforschung

FFG Forschung wirkt.
FKZ FO999902707

# Digitale Souveränität

Time to 'reclaim sovereignty'

## Von der Leyen receives Charlemagne Prize as Frieden calls for stronger Europe

| Update: 29.05.2025 17:43 | 4 Comment(s)

Europe must become technologically and digitally sovereign, said Chancellor Merkel in her speech on the occasion of the German EU Council Presidency. The concept of digital sovereignty is not very clear-cut. In a policy brief, Falk Steiner and Viktoria Grzymek explain the underlying problems and discuss what digital sovereignty can mean in concrete terms: A better awareness and control of dependencies in central

## Defense giants want von der Leyen to boost made-in-Europe tech

European industrial and tech firms want the EU's backing to reduce reliance on the U.S.

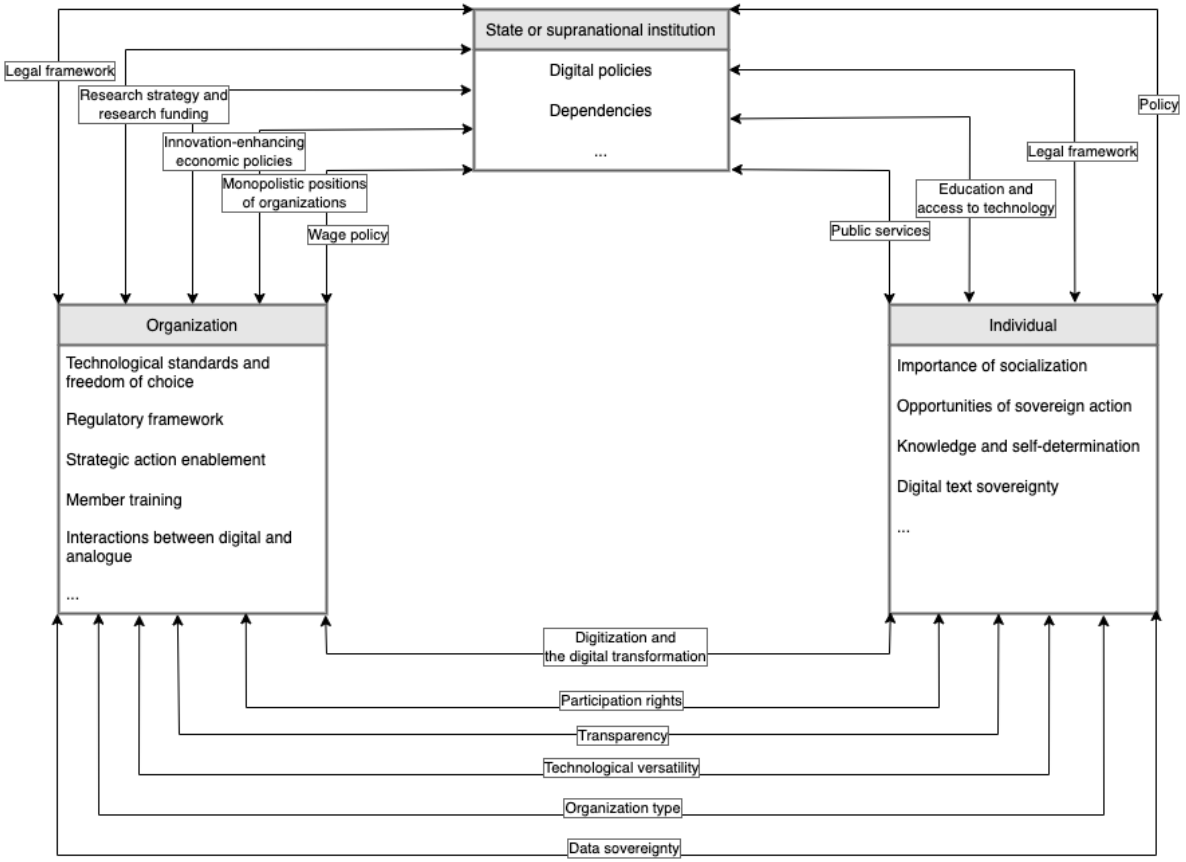
In a letter to European Commission President Ursula von der Leyen and tech sovereignty chief Henna Virkkunen released on Monday, the companies said Europe needs to be "more technologically independent across all layers of its critical digital infrastructure."

Signatories want "Buy European" requirements for governments to increase demand for homegrown tech and a "sovereign infrastructure fund" to support investments in more capital-intensive industries like microchips and quantum technology.

# Sicherheit in der guten alten Zeit – Die Burg zu Burghausen

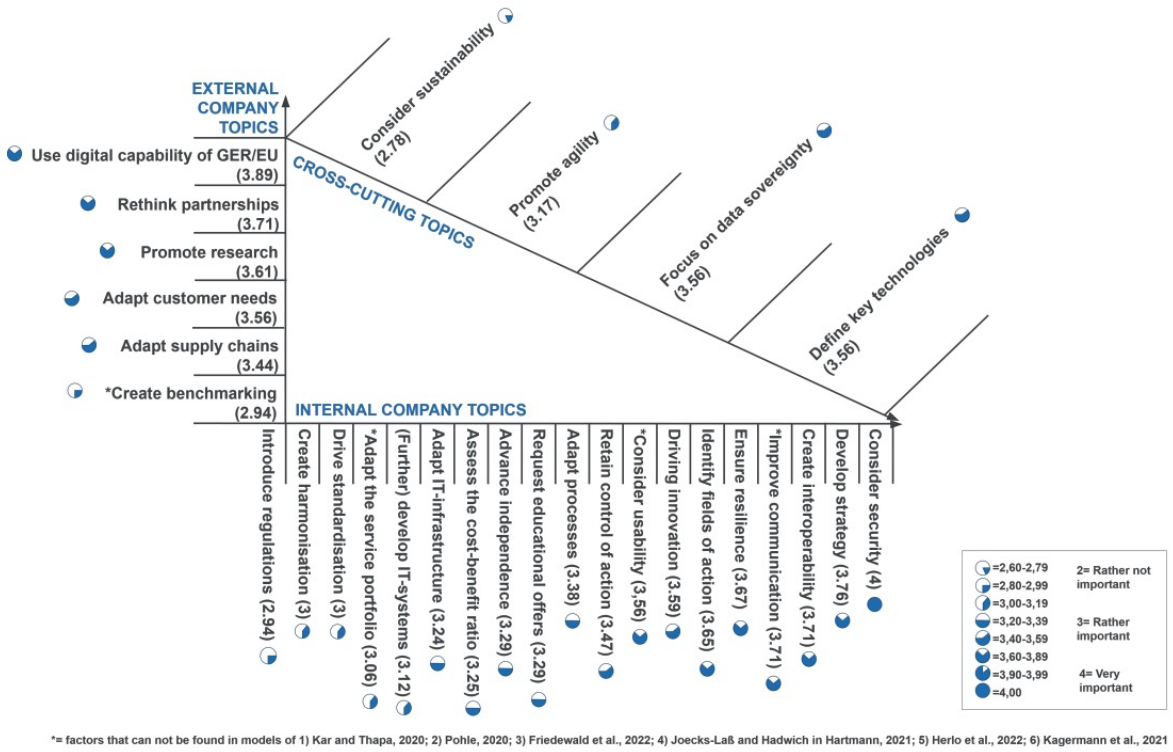
(Quelle: Martin Falbisoner, Digital Commons)

# Das LIONS´ Modell Digitaler Souveränität




*(Maximilian Greiner, Manfred Hofmeier, Razvan Hrestic, Ulrike Lechner, & Thomas Wendeborn, CRITIS 2022)*

# Digitale Souveränität aus Sicht der IT-Beratung: Das DISMIC Modell




*= 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

*(Martha Klare & Ulrike Lechner, ICSOB 2023)*

# Affordanzen als Wegweiser zu Digitaler Souveränität

| Cluster | Affordance | Exact solution | Explanation | Impact |
|---|---|---|---|---|
| Open Source Project No. 1: Messenger | | | | |
| Standardizing Affordances | Standards and guidelines | Standards and guidelines for matrix (Matrix.org Foundation) | Matrix.org 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) |
| Basic Affordances | Know how | Cryptography know how (Vector Informatik GmbH) | Vector Informatik GmbH offers cryptography know how. 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 test know how (Secusmart GmbH) | Secusmart GmbH is the company responsible for penetration tests within the project. The six-monthly test is intended to ensure that security weaknesses in Messenger are detected quickly. They are also responsible for proposing mitigation measures, which the project team will then implement. | Project work (speed) |
| | Testing software | Eggplant (Keysight Technologies) | Keysight Technologies 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 | | Jira (Atlassian) | With Jira, Atlassian 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) |
| | Project management tools | Confluence (Atlassian) | Atlassian 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) |

James Gibson first analyzed in 1986 how an object can be perceived and used differently by various living beings. His definition: *"The affordances of the environment are what it offers the animal, what it provides or furnishes, either for good or ill"*

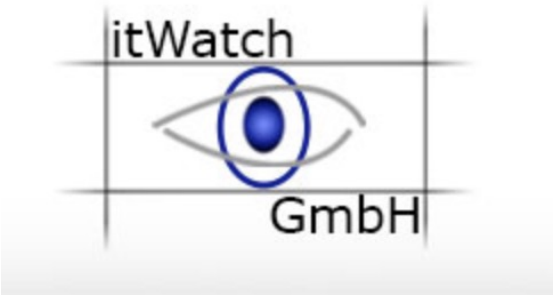
In psychology, where the term 'affordance' originates, it is increasingly understood as the possibility of perceiving actions through objects in the environment.

| 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 | MongoDB is a modern database management solution from MongoDB, 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) |

*(Martha Klare & Ulrike Lechner, ICSOB 2024)*

# Gestaltung Digitaler Souveränität - Der LIONS Demonstrator

- Design Science with
  - Scenario
  - Demonstrator
  - Evaluation by informed argument

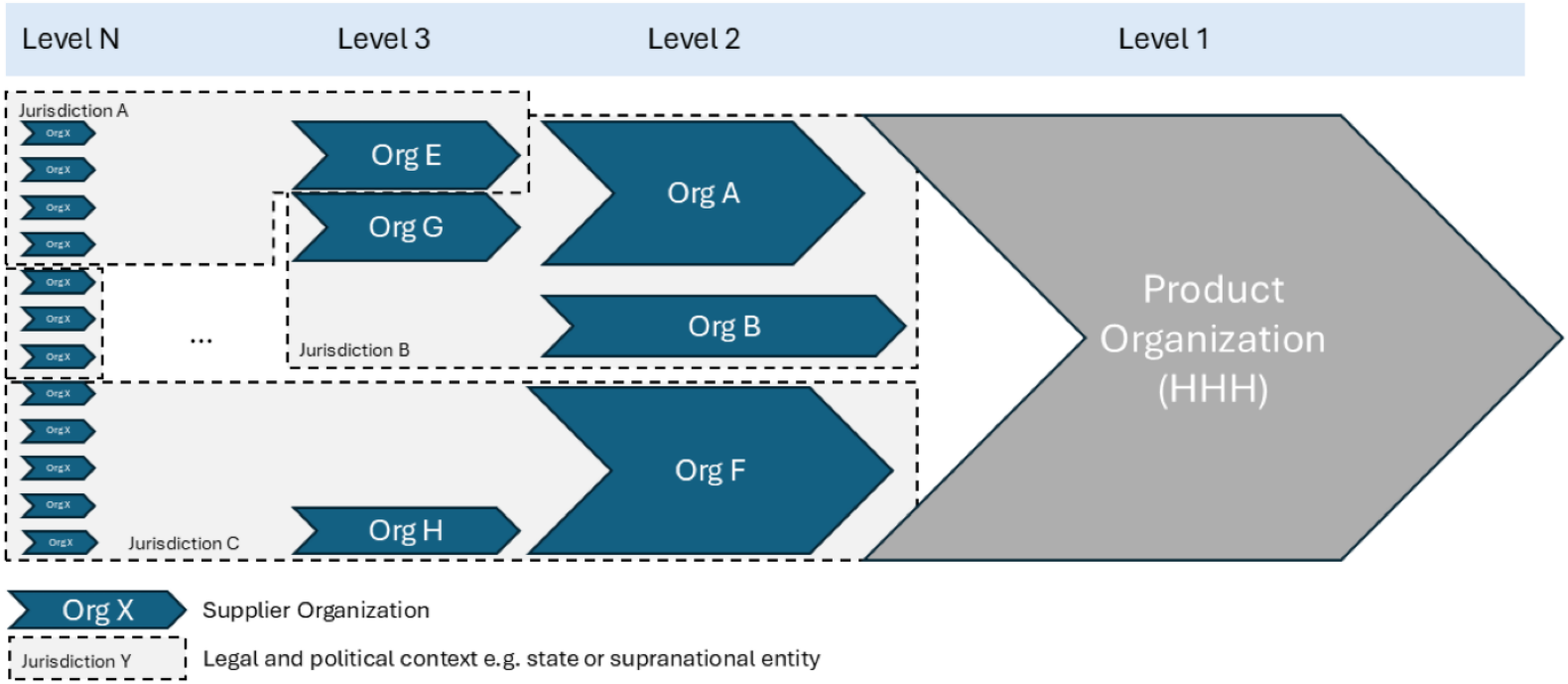



This research was carried out in cooperation between the research teams and a small IT software company specialized in products and services with high level of security risks as part of a larger research project.

# Digital Sovereignty from a Supply Chain Management and Procurement Perspective

- **RQ1:** How can digital sovereignty be **quantified and measured**?
- **RQ2**: What **factors influence** digital sovereignty at the organizational level?
- **RQ3**: What are **specific risks** in the digital supply chain and how to mitigate them?
- **RQ4**: How can the **use of blockchain technology** contribute to digital sovereignty goals and which other trade-offs does it offer?
- **RQ5**: Which **choices of strategy** are possible when considering their effects on digital sovereignty?

# Das Senar: Der kleine Staubsaugerrobter und die Supply Chain



# Die Risiken im Szenar

**Risk 1**: Key components in the supply chain depend on **few or even single suppliers**.

Risk 2: **Key components in the supply chain are not well understood or checked** by the producing organization because of missing capabilities or personnel (e.g., skills, specific qualifications, etc.).

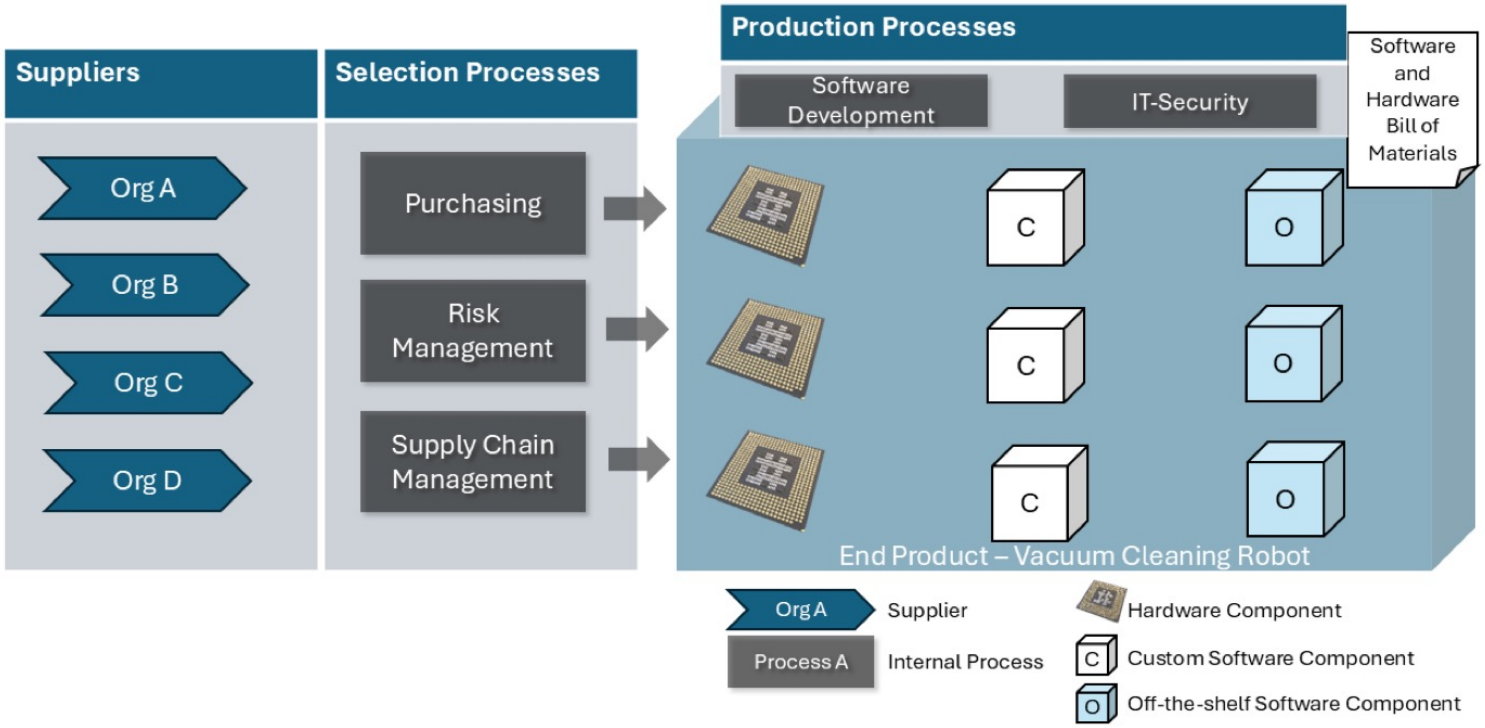
Risk 3: **Gathering data e.g. the full bill of materials for software and hardware components** or security findings **is difficult or time-consuming** to gather across systems and thus not used as a decision basis for the product itself.

Risk 4: When **data** is available, it is usually **difficult to anonymize and prepare for usage for the entire supply chain or even outside it**. Information e.g. about a compromised component is thus not conveyed in a timely manner. Also nobody else outside the data producing organization may use the data to e.g. gain and share insights that might help improve the product.

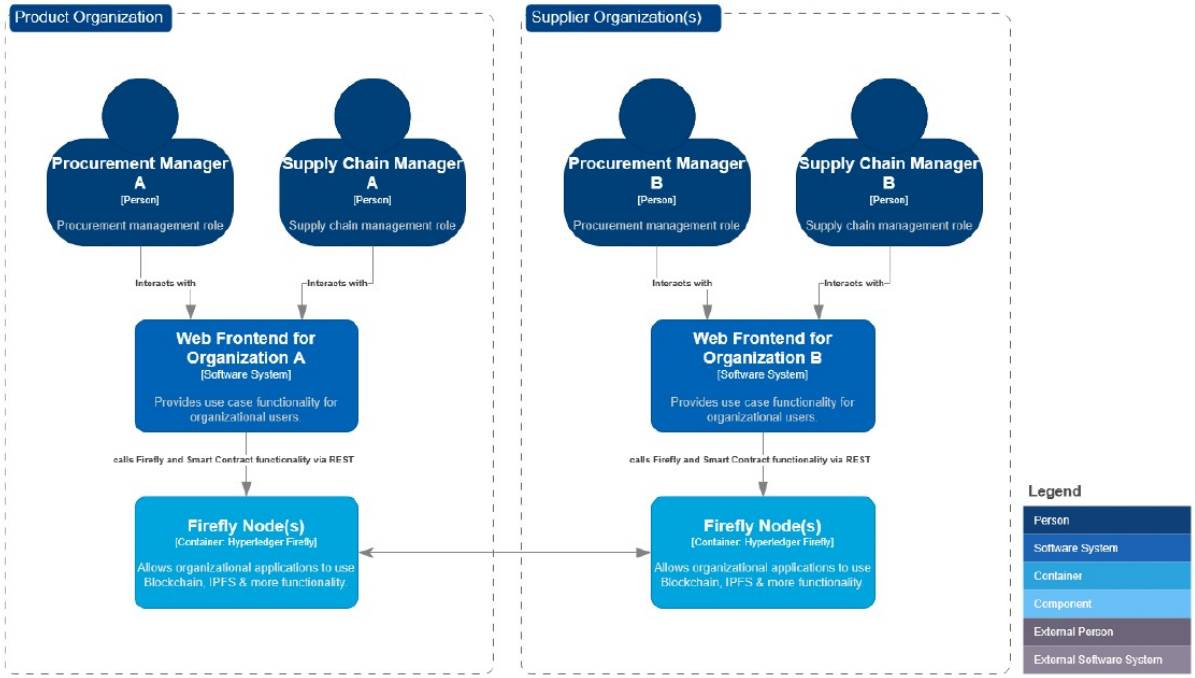
Risk 5: When suppliers do not get data on e.g. how they rank in good security practices compared to others, they do not have as much **incentive to improve their practice**. This can lead to overall less secure products of lower quality.

Risk 6: Global supply chains are affected by **global crises and geopolitical tensions**. Should a component become unavailable because of e.g. technology embargo, bankruptcy, sabotage etc. and there is no alternative, the entire product availability is at stake.

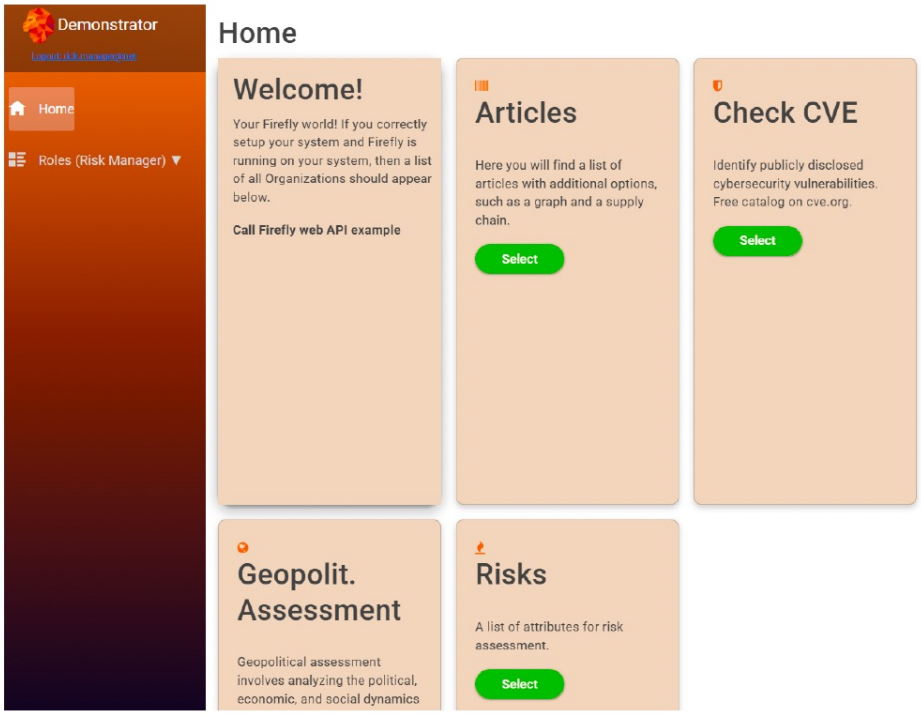
# Überlegungen zu Risiken und Souveränität



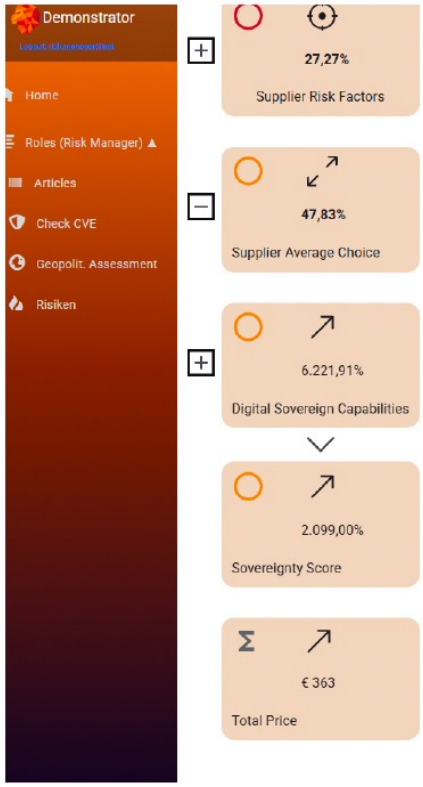
# Blockchain Konsortium für Souveräne Informationsflüsse

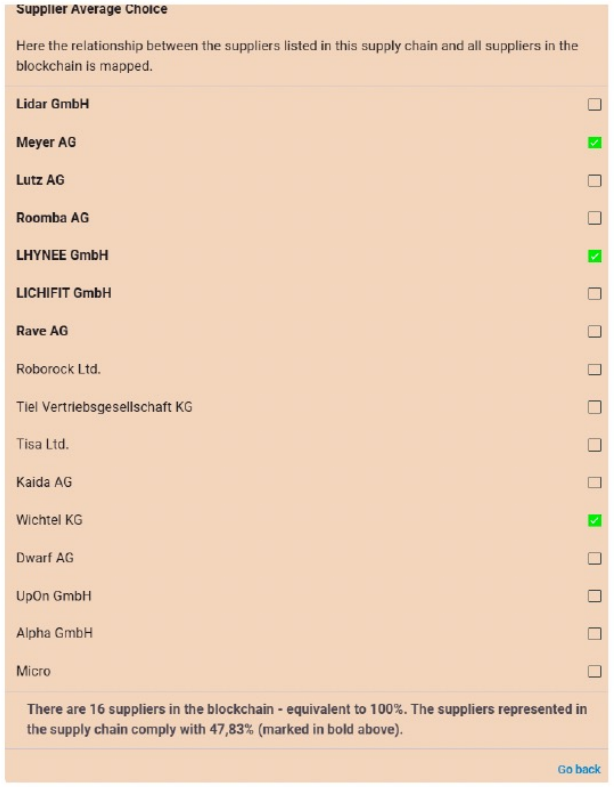


# Der Demonstrator – Die Hauptseite

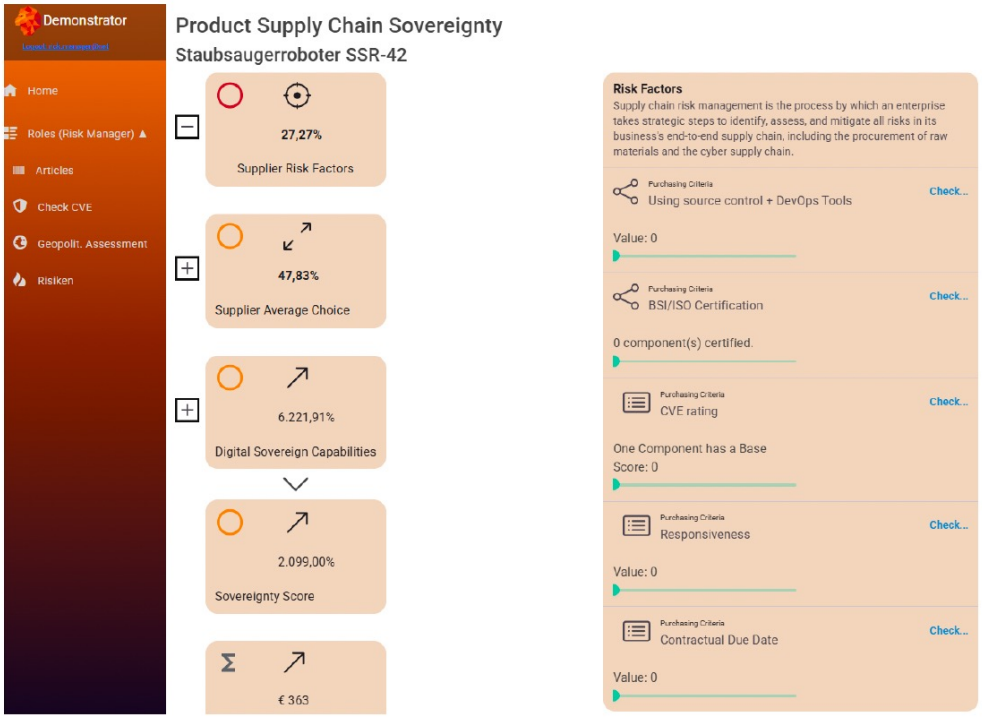


# Supplier Sovereignty Screen

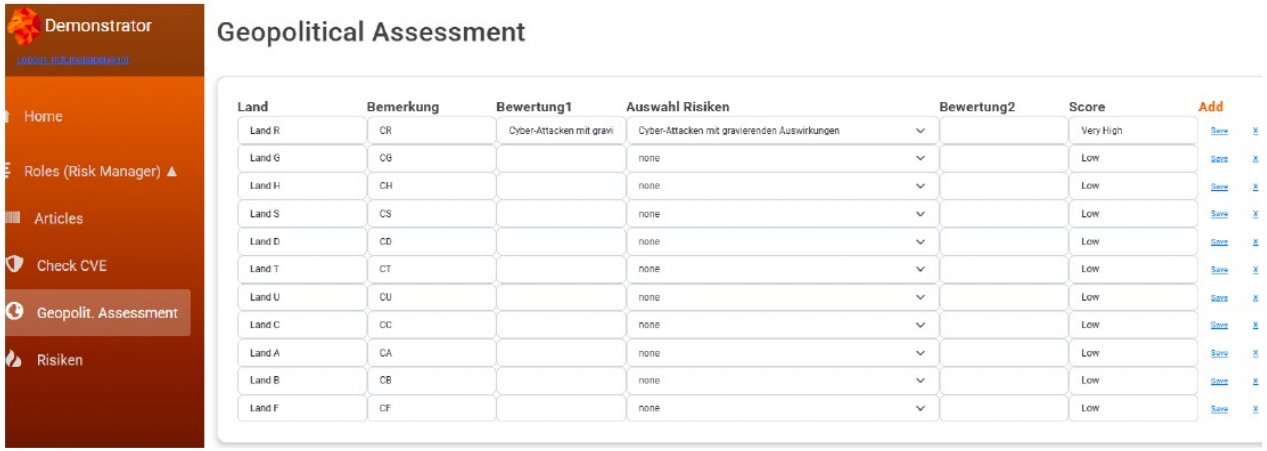


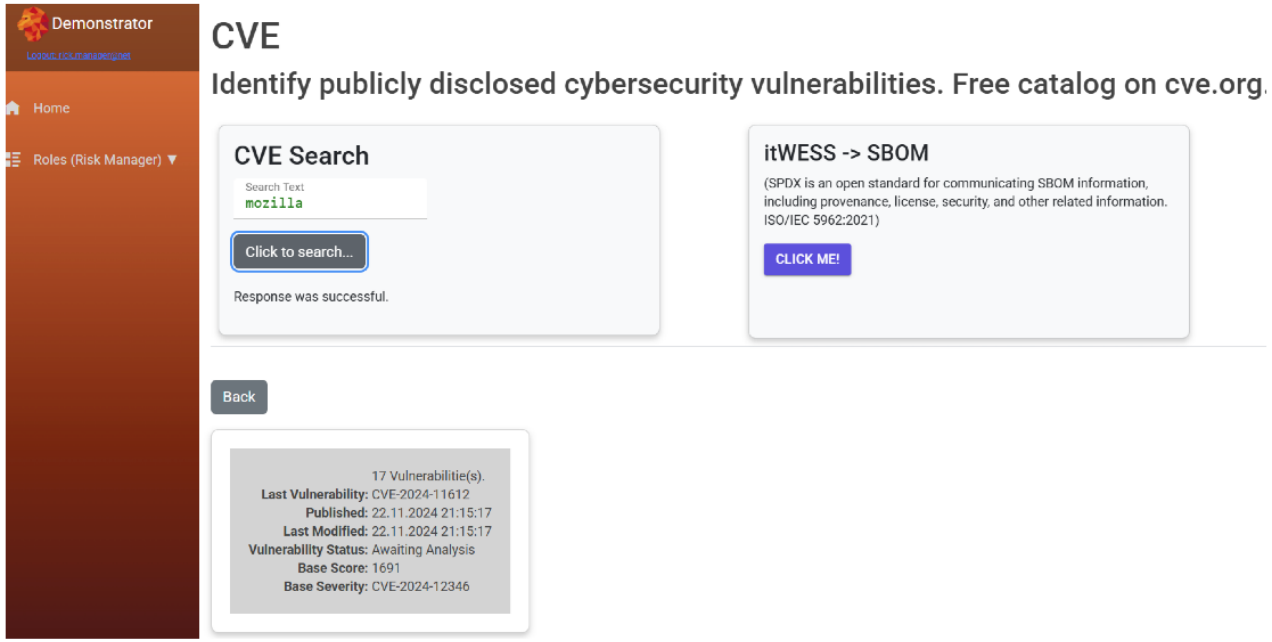
# Supply Sovereignty Dashboard



# Bewertung der Geopolitischen Lage



# CVE Bewertungsscreen



# Quantifizierung Digitaler Souveränität

$$\frac{\text{Supplier Risk Factor} \times \text{Supplier Average Choice} \times \text{Digital Sovereign Capabilities}}{3}$$

$$\frac{\text{number of available suppliers per component}}{\text{total number of suppliers}}$$

# Digitale Souveränität – Resilienz und das Bewusstsein durch Serious Games


Eine Frage der Sicherheit

**Scared? Prepared? Toward a Ransomware Incident Response Scenario**

Maximilian Greiner, Judith Strussenberg, Andreas Seiler, Stefan Hofbauer, Michael Schuster, Damian Stano et al.
**Pages 289-320**

Operation Raven

# Referenzprozess – Sicherheit, Resilienz und Digitale Souveränität im Geschäftsmodell

**Schritt 2: Erste Maßnahmen**

**Stakeholder:** (7)

- IT Abteilung
- Kritische Anbieter
- Benutzer
- Unternehmen
- Kollegen

**Schlüsselaktivitäten:** (5)

- Dokumentation beginnen (Was wurde bemerkt, an wen welches Gerät übergeben, etc.)
- Gerät mit Strom versorgen
- Security Abteilung benachrichtigen
- Handy abgeben bei der IT
- PIN bereitstellen
- Zugänge sperren (Mobile ID, M365, Cloud, Banking, etc.)
- Gerät vom Netzwerk nehmen
- Backups identifizieren

**Ressourcen:** (6)

- Kontakt zu IT (Ansprechpartner vorhanden) sowie Kontaktkanäle zu den kritischen Anbietern
- In Incident Response geschulte IT Abteilung

**Wertversprechen:** (2)

- Begrenzung des Schadens

**Kommunikation** (3)

- Kommunikation mit der IT Abteilung → Incident Beschreibung; Verfügbarkeit von Backups (privat und in der Firma) → Sperrung von Konten für kritische Dienste
- Kommunikation mit kritischen Diensten (Bank) → Sperrung von Konten

**Kommunikationskanäle:** (4)

- Persönlicher Kontakt
- Telefonisch (mit Alternativgerät)
- Online

**Interne / externe Kunden (Zielgruppe)** (1)

- Ich selbst

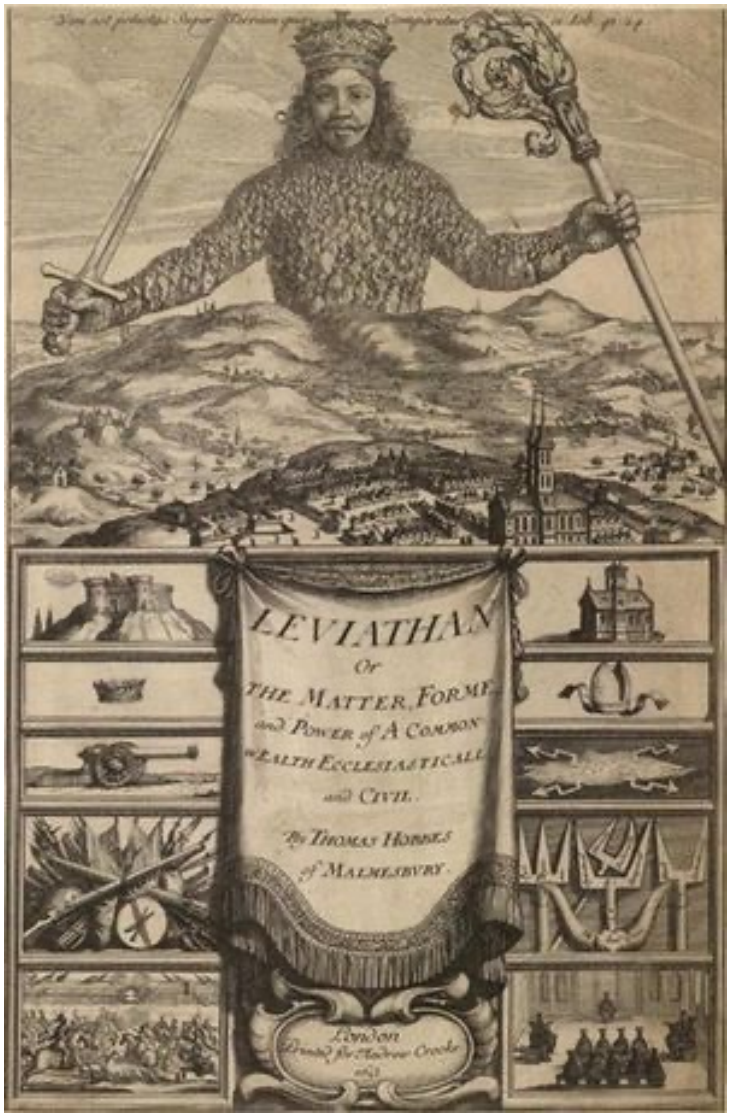
**Hypothesen:** (9)

- Ransomware ist im wesentlichen auf dem persönlichen Gerät oder den persönlichen Diensten

**Endzustand:** (8)

- Das persönliche Gerät ist bei der IT Sicherheit

# Digitale Souveränität - Eine bewusste Entscheidung!




Thomas Hobbes - Leviathan

# Digitale Souveränität – Ihre Entscheidung!



- Digitale Souveränität ist eine Entscheidung des Einzelnen.
- Digitale Souveränität ist eine Chance, die im Dialog genutzt wird.
- Digitale Souveränität kann gestaltet, gebaut, gemanagt werden. Digitale Souveränität braucht Bewusstsein für IT-Sicherheit, Resilienz, Risiken und Verpflichtungen und Handlungsoptionen.
- Sicherheit, Resilienz und Digitale Souveränität sind und brauchen ein Geschäftsmodell.



# Danke für Ihre Aufmerksamkeit

Kotakt
Prof. Dr. Ulrike Lechner
ulrike.lechner@unibw.de