



Digital Sovereignty Talks

Food4Thought

Summer 2024

Munich School of Politics and
Public Policy (HfP) · TUM Think
Tank



v1.3

Digital Sovereignty and Soft Power: The Role of Regulation and Auditing

The "Food4Thought" series is our contribution to elevating the discourse on digital sovereignty and its associated challenges. This collection of texts is designed to provoke thought, encourage dialogue among decision-makers, and support informed decision-making in an increasingly complex digital world. Our aim is to provide a platform for the exchange of ideas, thereby creating a guide for shaping a sovereign and collaborative digital future.



Introduction

In today's digital age, trust is a cornerstone for the adoption and success of emerging technologies such as cloud computing and artificial intelligence (AI). Unlike traditional on-premises systems, cloud environments inherently lack physical proximity and control, requiring a higher level of trust. This trust is fundamentally based on auditable standards that act as a "trust wrapper" for these technologies. Furthermore, the establishment of this trust is critical to the enhancement of digital sovereignty, ensuring that nations retain control and influence over their digital infrastructure and data. In addition, the development and enforcement of these standards contribute to a nation's soft power, projecting its influence and setting global benchmarks in digital governance.

Cloud Needs Trust Because It Is Not On-Premises

The nature of cloud computing - where data and services are hosted off-site - presents unique challenges. Users need to trust that their data is secure, that their privacy is protected, and that services will remain available and reliable. Unlike on-premises solutions, where physical control and direct oversight provide a sense of security, cloud environments require users to rely on the security measures and integrity of external providers. This dependency makes trust a critical factor in maintaining digital sovereignty, ensuring that nations can confidently leverage cloud technologies without compromising their control over critical data and systems.

Trust Is Built on Auditable Standards

Robust and auditable standards are essential to building this trust. These standards provide a framework that can be independently verified through auditing, ensuring that the necessary security controls and measures are in place. Auditing acts as a trust wrapper, providing assurance that cloud providers adhere to strict security and operational protocols. This is particularly important in areas such as AI, where transparency and accountability are paramount. With auditable standards in place, countries can ensure that their digital environments are secure and compliant, strengthening their digital sovereignty.

Creating Standards for Emerging Fields

Developing standards in emerging areas requires a collaborative approach. It involves input from auditors who understand what aspects can be audited; technologists who can implement the necessary security controls such as device control, application control, encryption management, and security awareness training; policymakers who shape the regulatory landscape; and regulators who enforce compliance. This multidisciplinary collaboration

ensures that the standards are both practical and comprehensive. By integrating the expertise of multiple stakeholders, these standards become robust frameworks that support a nation's digital sovereignty by maintaining high levels of security and trust.

Standards Must Be Verifiable

For standards to be effective, they must be verifiable. The C5 (Cloud Computing Compliance Criteria Catalogue) in Germany is a good example. Developed by the German Federal Office for Information Security (BSI), the C5 framework outlines clear, auditable criteria for cloud security, providing a transparent and reliable benchmark for cloud providers. Such frameworks are essential for maintaining trust and compliance in cloud environments. Auditable standards like C5 empower nations to ensure the security of their digital infrastructures, further strengthening their digital sovereignty by allowing them to dictate and enforce their security protocols.

Consensus on Auditable Standards

Building consensus around these auditable standards is critical. Consensus ensures that standards are widely accepted and implemented, thereby increasing overall confidence in the technology. It involves an ongoing dialogue among all stakeholders to refine and update the standards, ensuring that they keep pace with technological advances and emerging threats. Consensus-driven standards not only build trust, but also unify different sectors around common security practices, strengthening a nation's digital sovereignty.

Developing Soft Power through Regulatory Ecosystems

Soft power refers to a country's ability to influence others through non-coercive means, such as cultural or ideological appeal. In the realm of digital technology, countries like Germany can develop soft power by establishing a robust regulatory ecosystem with evolving standards such as C5. When regulators like the BSI enforce these standards and auditors verify compliance, they set a global benchmark. This not only enhances national security but also positions Germany as a leader in digital governance, influencing global practices and standards. In this way, Germany not only secures its digital environment but also projects its influence globally and strengthens its digital sovereignty.

In conclusion, building trust in emerging technologies such as cloud computing and AI depends on the interplay between regulation and auditing. By developing and enforcing auditable standards through a collaborative approach and fostering consensus, we can create a secure, reliable, and sovereign digital environment. This approach not only addresses immediate security concerns but also lays the foundation for sustainable innovation and trust in the digital age. Ultimately, such confidence-building measures are fundamental to enhancing

digital sovereignty, allowing nations to maintain control over their digital infrastructures and assert their influence in the global digital economy. Moreover, by leading in the development and enforcement of these standards, nations like Germany can extend their soft power by setting benchmarks that influence global digital governance practices.

Authors

Philipp Müller

Sofie Schönborn