



Digital Sovereignty Talks

Food4Thought: Digital Sovereignty in a Multipolarized World

February 2025

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



v2.0

Digital Sovereignty in a Multipolarized World

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.

Authors

Philipp Müller

Sofie Schönborn

Contributors

Tim Würfl

Anastasiia Tyshenko



Executive Summary

Europe stands at a crossroads in a rapidly evolving “multipolar” world, where technology underpins both security and prosperity. The Munich Security Report 2025 highlights that competing power centers now jostle for influence in areas such as AI, quantum computing, and cybersecurity—domains in which the EU’s engineering expertise, strong data-protection ethos, and regulatory savvy could become major assets. However, participants at our Digital Sovereignty Talks stressed that Europe must do more than tout moral leadership: it must focus on concrete “control points” where it can excel, standardize non-critical layers to maximize efficiency, and invest in an inclusive talent pipeline. Well-targeted regulation can drive innovation, but only if existing rules are streamlined and combined with agile public-private cooperation. Equally crucial is social cohesion: strengthening civic and digital education, creating avenues for foreign graduates to integrate, and embedding “public interest technology” approaches can help unite diverse communities against disinformation and cyberattacks.

These strategies reinforce each other. When the EU builds on credible technical capabilities—especially in cybersecurity and AI—its stance in global tech deals improves, and its cross-border partnerships can better reflect European values of freedom, security, and justice. Civic resilience benefits, too: citizens better equipped with digital skills are less vulnerable to disruptive misinformation, and more likely to support forward-looking projects like sustainability-driven research or AI-based governance. Ultimately, a model of “federated innovation”—combining local experimentation with principled guardrails—positions Europe as a confident rule-shaper rather than a rules-taker. Harnessing Europe’s diversity, regulatory tradition, and democratic heritage can turn a fracturing world order into an opportunity for leadership, ensuring that digital sovereignty is anchored in shared prosperity, societal cohesion, and respect for fundamental rights.

Introduction

According to the Munich Security Report 2025, today's global power shifts - and the polarization that accompanies them - have deepened the sense of "multipolarization". As influence is redistributed to a growing number of actors, states compete for technological and economic primacy. In this environment, digital sovereignty is more than a buzzword; it has become a cornerstone of national security, resilience, and the ability to shape the global order.

In this essay, we share reflections and findings from our unofficial Munich Security Conference side event, "Digital Sovereignty Talks"—a breakfast held at the TUM Think Tank and co-organized with DriveLock— where participants from academia, industry, and government gathered to discuss Europe's digital path forward. The underlying question was whether, in a world dominated by new power centers, Europe still has the operational, normative, and economic heft to secure its digital ecosystem while remaining true to democratic values.

Several participants noted that trust—the foundation of secure partnerships—is eroding, especially between Europe and increasingly assertive global players. This breakdown is forcing Europeans to prove that they can effectively protect their data flows, infrastructures, and digital supply chains, lest outside observers dismiss them as lacking capacity. Compounding this pressure, major powers are adopting more authoritarian approaches to harness technology for strategic gains, while Europe is itself fragmented on many pressing policy issues. As some attendees argued, this begs the question: *Does democracy retain sufficient weight to influence digital and geopolitical norms in an era of multipolarization?*

Yet there is a counterpoint: Europe's inherent strengths remain underutilized. From long life expectancies to deep reserves of societal capital and tourism, the continent's comparative advantages could fuel a more strategic global role. The challenge, however, is that one cannot rely on the so-called "Brussels Effect" without the economic might and digital innovation necessary to enforce rules on the international stage. As one participant put it, Europeans may have been "playing chess in a ring full of martial arts fighters"—and must adapt accordingly.

Against this backdrop, digital sovereignty is about more than data privacy or cybersecurity; it is about building the operational and technological resilience to negotiate confidently in a fluid and sometimes confrontational environment. During our breakfast discussions, we therefore framed digital sovereignty through the lens of **capacity to act** in four interrelated dimensions: (1) **operational excellence**, (2) **deal-making**, (3) **societal resilience**, (4) and **world-shaping**.

We hope these perspectives will inform policymakers as they seek to secure Europe's digital future in a rapidly transforming multipolar landscape.

(1) In light of heightened power competition and rising cyber threats, what strategies can governments and firms adopt to bolster their operational excellence in digital systems and infrastructures – thereby maintaining Europe’s competitiveness and security?

A recurring theme in our conversations was that Europe cannot be self-sufficient in every layer of technology—nor can it afford to cede significant ground to more assertive players. The way forward, participants suggested, hinges on adopting a layered approach: identify and secure critical “control points” where European leadership is possible or necessary, while standardizing and collaborating more broadly in less critical areas to streamline costs and combat fragmentation.

First, many argued for **focusing on high-impact domains such as advanced cybersecurity, next-generation computing, and key AI applications**, where Europe can realistically compete at a world-class level. By zeroing in on these segments, the region can leverage its engineering strengths and shared data protection principles to create pockets of excellence that reinforce trust with global partners. In turn, less strategic layers—where vertical lock-ins may pose fewer risks—can be standardized and outsourced in ways that avoid diluting vital resources.

Second, participants underscored the imperative of **strengthening the digital talent pipeline**, both for industry practitioners and regulators. Attracting top researchers, developers, and entrepreneurs will require policy measures like streamlined visas, tax incentives, and robust upskilling programs. Equally important, authorities who shape or enforce digital regulations need deeper technical knowledge. Whether overseeing AI-enabled services or managing internet-of-things (IoT) risks, regulators who understand core technologies are better positioned to align policies with operational realities.

A third concern revolved around **Europe’s current regulatory environment**, which—though motivated by consumer protection and competitiveness—risks becoming entangled in overlapping directives. Attendees called for enhanced regulatory coherence to prevent confusion in the marketplace and enable firms to innovate without excessive administrative burdens. Crucially, any consolidation of existing frameworks should continue to embed “security by design,” ensuring that each stage of the digital supply chain meets high standards of data protection and resilience. Only then, participants stressed, will Europe retain the global credibility to export its rules-based approach and hold its own against powers like the U.S. and China.

Finally, operational excellence depends on **deeper public-private collaboration**. Several participants described an evolving landscape where governments and industry could form

joint bodies—not just to coordinate crisis responses but also to identify and address upcoming technological shifts. High-level orchestration of public procurement programs, co-funded pilot projects, and cross-border industrial partnerships can amplify Europe’s core strengths in research, infrastructure, and innovation. Participants emphasized that co-investment and risk-sharing are critical, especially when confronting fast-moving sectors like AI, quantum computing, or advanced encryption.

Taken together, these insights point toward a handful of concrete takeaways. Europe should **pinpoint and protect its high-stakes technological layers**, ensuring local excellence and sovereignty where it truly counts. It must **cultivate a talent-driven environment** across both industry and regulation, aligning policy so that emerging expertise does not drain away to foreign tech hubs. Further, **achieving greater coherence in Europe’s digital regulations** will reduce complexity for innovators and safeguard security. Most importantly, **public-private partnerships** should be deepened through ongoing dialogue, shared investments, and proactive cross-border coalitions. By embracing these strategies, Europe can sustain a robust digital ecosystem capable of meeting the challenges of a multipolar technological era.

(2) Considering the growing importance of technology as a lever of global power, how should states and private actors approach cross-border tech deals and data governance agreements to ensure mutual benefit and maintain strategic autonomy?

Participants emphasized that while Europe’s strengths—like high-quality manufacturing, robust cybersecurity capabilities, and a principled regulatory framework—offer distinct advantages, they must be channeled into a coherent value proposition. To persuade international partners to adopt or invest in European solutions, stakeholders need to identify and articulate the region’s competitive edges, such as trusted data-management expertise or well-trained engineering talent. This means governments and private actors alike should systematically determine **where Europe excels** and communicate those areas compellingly in any negotiation involving data governance or technology transfer.

A key element of deal-making success is also tied to a thriving local ecosystem. By strengthening the domestic market for innovative technology—often through strategic public procurement and dedicated “technology missions”—Europe can foster a pipeline of competitive companies that command global credibility. One suggestion was to align public procurement rules with broader ambitions to nurture local champions, thereby using the state’s purchasing power to cultivate an environment conducive to advanced R&D and entrepreneurial risk-taking. Major stakeholders in industry, research, and government could

co-design flagship initiatives, focusing on challenges that require high-tech responses, such as smart mobility or AI-driven sustainability. These targeted missions would not only incentivize domestic development but also serve as beacons to attract foreign expertise and investors.

Another crucial factor, discussed by nearly all participants, is the need to **bridge Europe's digital skill gap**. While some pockets of excellence exist, a significant portion of the population—and many policymakers—remain insufficiently versed in cutting-edge digital issues. Embedding computer science and data literacy throughout educational systems is vital to forming a broad base of digital-savvy professionals, regulators, and citizens. Some attendees noted that external macro trends, including uncertainties in the U.S. visa regime, could open a “window of opportunity” for Europe to attract high-skilled migrants who might otherwise seek careers in North America, further boosting the region's talent pool.

Moreover, participants saw **regulation not merely as a compliance mechanism** but as a potential driver of innovation. Well-framed requirements—especially those highlighting data privacy or cybersecurity—can push firms to adopt leading-edge solutions, sometimes favoring domestic providers. By translating Europe's regulatory commitments into tangible incentives, policymakers could foster the local adoption of emerging technologies while simultaneously shaping global standards. The caveat, however, is ensuring that Europe does not overwhelm industries with a patchwork of overlapping directives. Instead, officials need to move from passive rulemaking to **agenda-setting**, tying regulatory clarity to forward-looking domains—such as AI governance or zero-trust cybersecurity architectures—and using those rules as leverage in global tech deals.

Overall, participants concluded that **defining Europe's strategic assets, strengthening the domestic market, upgrading digital literacy, and using regulation as an innovation catalyst** would significantly bolster the region's deal-making capacity. When Europe leads with clear priorities, invests in nurturing local champions, and showcases its commitment to data trustworthiness and security, it can better align cross-border tech deals with both mutual economic benefit and essential European values—ultimately ensuring that strategic autonomy is not an afterthought, but an inherent outcome of proactive engagement on the global stage.

(3) Which political investments, governance models, and technologies support the strengthening of societal resilience in a multipolar digital age?

Participants repeatedly underscored that Europe's digital sovereignty rests not just on technical prowess or market share but on the social fabric that underpins these capabilities. Societal trust, in turn, hinges on inclusive education, forward-looking governance models, and technology policies that prioritize civic empowerment. To maintain resilience against disinformation, protect critical infrastructure, and foster an engaged public, Europe must embrace both structural reforms and cultural shifts.

A first line of action, many suggested, is **broadening and deepening civic and technological education**. While participants recognized that Germany's and Europe's universities attract international talent, they argued that overall investment in lifelong learning remains too narrow. From AI literacy in secondary schools to continuous upskilling programs in the workforce, governments and industry alike need to scale initiatives that equip citizens with the knowledge to navigate—and shape—emerging digital trends. Moreover, expanding political education can help counter fragmentation and reduce susceptibility to extremist narratives or disinformation campaigns.

Institutional structures must also adapt to the evolving digital landscape. This includes **aligning administrative language and processes with a global reality**: many international graduates lose motivation to remain in Europe because they face barriers such as job postings in local languages and limited opportunities to integrate. By internationalizing job markets, governments and employers can retain highly qualified individuals who reinforce societal resilience through their expertise and perspective diversity.

In parallel, **public-private collaboration** emerged as a key enabler. Participants asked how democratic values and the public interest could be baked into joint endeavors between the public sector and technology firms—an emergent approach sometimes referred to as “public interest technology.” Such a model may for example entail co-developed AI applications focused on solving social challenges, coupled with transparent governance structures that keep democratic accountability at the forefront. By creating shared platforms for civic engagement—where industry shares data responsibly and the public sector ensures democratic oversight—Europe can develop technologies aligned with core societal objectives, from equitable healthcare to trustworthy information ecosystems.

Finally, technology itself, if implemented with an ethos of security-by-design and user empowerment, can further bolster resilience. By setting robust standards for data protection

and interoperability, Europe may foster an environment in which smaller civic-tech players thrive, helping citizens distinguish reliable sources from disinformation. Institutions could also fund research on “civic machines”—digital solutions aimed explicitly at strengthening public discourse, preserving elections’ integrity, and bridging social divides. These tools, aligned with strong data protection frameworks, would operate within a rules-based system that places human rights and transparency at the center.

Overall, the discussions highlighted that **strengthening societal resilience is not a single intervention** but a web of complementary measures. By investing in ongoing education at every level, adopting more inclusive hiring practices to retain global talent, institutionalizing public-private cooperation for democratically guided technology, and setting strict standards that promote civic-driven innovation, Europe can help ensure that its societies remain cohesive, diverse, and well-informed—even in a world where digital threats and rapid change are the new norm.

(4) In what ways can digital sovereignty empower nations—and alliances of nations—to proactively shape tomorrow’s digital rules, norms, and values, and how might this help address potential fractures in the broader international order?

Participants noted that Europe has a significant opportunity to exert leadership precisely because of its commitment to openness, democracy, and a relatively decentralized political landscape. While some argued that Europe’s federal structures and slower-moving legislative processes hinder the region’s agility, many saw flexibility as an untapped strength: it allows regional or local innovations to flourish, with only core standards—such as data privacy, cybersecurity requirements, and fundamental rights—set at a more centralized level. This dual model of strategic centralization and operational decentralization was repeatedly highlighted as a unique alternative to the more uniform systems of competing powers.

At the same time, discussants stressed the need for **fast yet principled action**. Specifically, they questioned whether “old” administrative approaches—where each country or federal entity individually negotiates digital standards—remain tenable in a multipolar world. A pan-European “heat map” of competencies and needs could help identify where to pool resources for maximum impact, whether in AI ethics, cross-border data flows, or quantum research. Once key priorities are fixed, Europe could deploy a consistent “Maslow’s hierarchy of needs”—ensuring basic digital infrastructure, safeguarding security, and cultivating a well-educated society prepared to pioneer next-generation solutions.

Another thread emphasized that *values-based innovation* can shape global digital rules without sacrificing Europe's democratic principles. By "gardening" innovation—letting smaller pilots experiment, then scaling successful solutions—Europe can maintain robust quality standards ("quality over price") yet remain agile. This approach requires rethinking regulation as a tool to encourage responsible tech rather than merely a mechanism to limit risk. Sometimes, participants argued, no additional regulation is precisely the impetus needed for rapid experimentation—so long as public oversight remains intact to ensure fairness and accountability.

Overall, attendees agreed that **digital sovereignty's real power lies in forging cohesive alliances** among governments, industry, and civil society—alliances that explicitly incorporate European values of openness, human rights, and public interest. Such partnerships could serve as a magnet for global talent and a bulwark against authoritarian or one-size-fits-all digital regimes. Done right, Europe's capacity to shape an inclusive, rules-based digital environment can help stitch together the international order—rather than watching it further fragment along competing spheres of influence.

Conclusion

The Munich Security Report 2025 describes how "multipolarization"—the redistribution of power across an increasingly diverse set of global actors—demands that Europe rethink the fundamentals of its security, economy, and governance. Nowhere is this more pressing than in the digital sphere, where the continent's ability to protect its infrastructure, negotiate global tech agreements, fortify societal trust, and project shared values all shape Europe's future.

Across the four dimensions we examined—**operational excellence, deal-making capacity, societal resilience, and shaping our world**—Europe has a chance to build on genuine strengths. Its formidable engineering talent, robust data-protection ethos, and proven regulatory creativity can act as pillars of a more confident digital sovereignty strategy. At the same time, participants repeatedly underscored that sovereign capabilities cannot be achieved in isolation: the success of any initiative depends on deepening cooperation between national governments, the European Commission, industry, academia, and civil society.

- 1. Operational Excellence:** By focusing on core "control points," standardizing selectively, and co-investing in talent and R&D, Europe can maintain a leading edge in critical areas like cybersecurity and AI.
- 2. Deal-Making Capacity:** Strategic alignment of public procurement, industry consortia, and regulatory goals helps the EU engage in tech partnerships from a position of strength.

3. Societal Resilience: Sustainable digital autonomy requires comprehensive civic and technological education, inclusive labor markets, and “public interest AI”—all predicated on trust and democratic oversight.

4. Shaping Our World: Europe’s openness and democratic character can become a magnet for global talent and an alternative model to centralized, top-down digital regimes. By balancing agile local experimentation with principled guardrails, the EU can export values-based rules that enrich—not fragment—the international order.

In short, a truly *European* approach to digital sovereignty recognizes the region’s unique mix of diversity and cohesion. If Europe resolves to identify its strategic technological priorities, empower public-private collaboration, and embed both flexibility and accountability into its governance, it can help to unify a fracturing global environment. Rather than resorting to isolationism, European leaders—and the broader ecosystem of innovators and citizens—have the tools to shape a multipolar age in ways that safeguard common values and sustain long-term prosperity.