



Fundamentals

DIGITAL SOVEREIGNTY

👤 Dr. Esther Görnemann

Weizenbaum Institute

<https://orcid.org/0000-0003-3958-2493>

Version: 📅 6/25/2024

Cite as Görnemann, E. (2024). Digital Sovereignty (Fundamentals series). Berlin: Weizenbaum Institute.

Compact overview Digital Sovereignty

Sounds good, means a lot. What is digital sovereignty, beyond political rhetoric?

1.1 Objects of digital sovereignty

1.2 Actors of sovereignty

The great awakening. Why do we want to become digitally sovereign?

2.1 Cyberspace sovereignty

The multi-stakeholder governance ideal - Governing with the wisdom of the many

2.2 The walled gardens of the proprietary internet

2.3 The power of platforms

Surveillance capitalism - The business with data

2.4 Mass surveillance and cyber espionage

The NSA affair

Political and industrial espionage

2.5 Isolation and seclusion

The splinternet: Authoritarian states seal themselves off

Isolationist tendencies in the EU

2.6 Geo-economical dependencies

The semiconductor industry

Politicization and trade war

2.7 Cyberattacks and hybrid threats

Ways into the self-determined future. How do we become digitally sovereign?

3.1 Legislation as a value-oriented instrument of governance

3.2 Basic conditions of digital sovereignty

Individual self-determination through digital competencies

Democratic self-determination through participation and inclusion

Extensive cybersecurity

Key technologies in research and development

3.3 Digital sovereignty at the data layer

Data protection

Data economy

Cloud infrastructure

3.4 Digital sovereignty at the code layer

Digital Sovereignty

Open-source software

Platform regulation

3.5 Digital sovereignty at the physical layer

Extensive infrastructure development

Reduction of supply risks

Outlook

What does sovereignty mean? A historical excursion



Digital espionage – the NSA affair



What is a microchip?



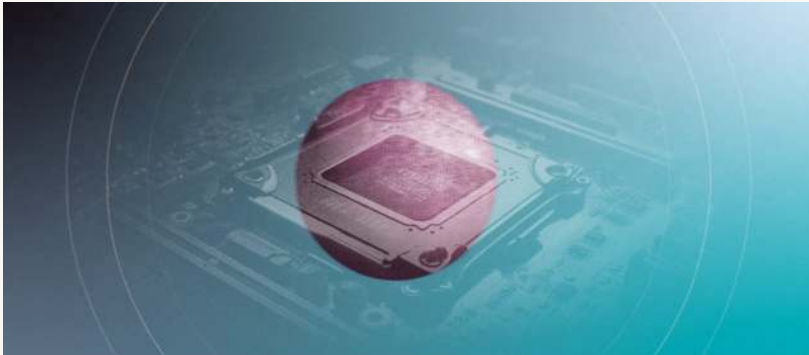
Glossary

References

COMPACT OVERVIEW DIGITAL SOVEREIGNTY

The term “digital sovereignty” has become an integral part of current political discourse. Across party lines and administrative levels, there is consensus: Being digitally sovereign is desirable and important. However, it often remains unclear what it actually means to be digitally sovereign and how this desirable state should be achieved. Nearly every digital policy measure could be justified and rhetorically polished with the goal of digital sovereignty. Still, digital sovereignty is more than a meaningless buzzword. It allows us to experience the political dimensions of digital infrastructures in many facets. It clarifies the political dimensions of digital infrastructures and points us towards the scopes of action in which we ourselves can shape our digital future in a self-determined way. To illustrate digital sovereignty in its entirety, this compact overview addresses **three central questions**.

Sounds good, means a lot. What is digital sovereignty, aside from political rhetoric?



We scrutinize the political discourse on digital sovereignty and find answers to the question of **who** is supposed to become sovereign **over what**. We then establish the historical connection to the notion of state sovereignty, and establish that both terms, although they have somewhat divergent meanings, inform and give context to one another.

[Jump to chapter](#)

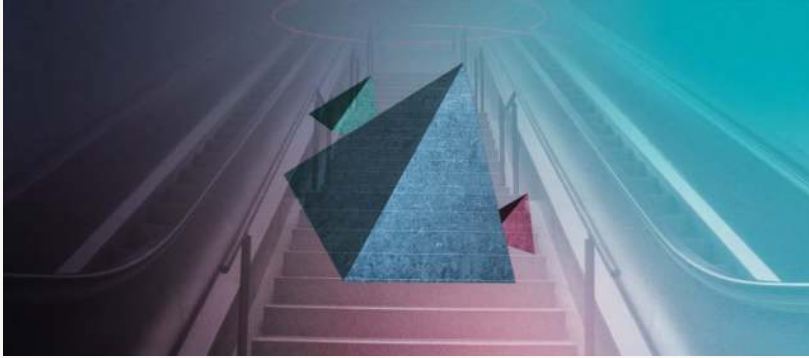
The great awakening. Why do we want to become digitally sovereign?



The last 30 years of internet history have provided many legitimate reasons to view “the digital” as a challenge to the sovereignty of public institutions, companies, individuals and collective movements. We recapitulate **seven important events** and developments that have fueled the call for digital sovereignty and raise fundamental questions about the distribution of power and creative authority in the digital age.

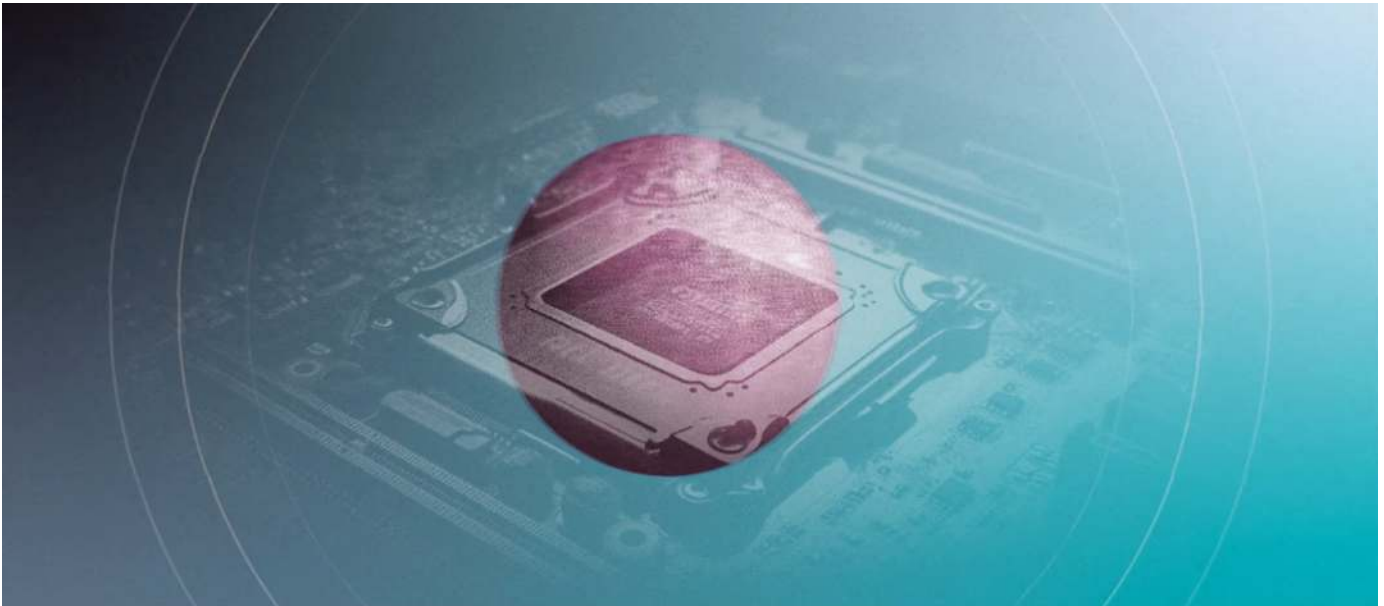
[Jump to chapter](#)

Ways toward a self-determined future. How do we become digitally sovereign



The digital sovereignty of various stakeholders can be promoted through different **government interventions**. In the EU and Germany, this involves, among other things, digital competency, infrastructure expansion, data policy, platform regulation, key technologies and cyber security. Ideally, the measures discussed should fit together like pieces of a puzzle.

[Jump to chapter](#)



SOUNDS GOOD, MEANS A LOT. WHAT IS DIGITAL SOVEREIGNTY, BEYOND POLITICAL RHETORIC?

"We must strengthen our digital sovereignty," declared German Chancellor Olaf Scholz at the re:publica conference in 2022 [1]. "What we need now in every sector, for every innovation, are European solutions and European sovereignty," demanded French President Emmanuel Macron two years earlier; the pursuit of digital sovereignty has become a central political project of his presidency [2].

"We must strengthen our digital sovereignty"

Olaf Scholz 2022

We encounter calls for digital sovereignty at many levels of German and European politics, in party programs, strategy papers from ministries, in the EU Commission, the Council of Europe, in security authorities, among internet activists and in business associations. However, as ubiquitous as the term may be, its actual meaning usually remains unclear. Actors from the domains of politics, industry and civil society are calling for different, sometimes even contradictory measures under the banner of digital sovereignty. Apparently, we are dealing with a political *high-value word* [3]. Digital sovereignty is an undisputed consensus term: No matter which digital policy one advocates, no one can say that they don't care about digital sovereignty. Those who call for it can rhetorically enhance their policy agenda and link it to higher ideals without making concrete, verifiable promises. At times, high-value words are used in such an inflationary way and in so many contexts that they are in danger of being completely stripped of their meaning and becoming meaningless empty phrases.

Even in research, a uniform definition of the term does not exist [4][5][6]. In general, the demand for digital sovereignty involves an idea of more autonomy,

freedom of choice, co-determination and control over “the digital” [4][5]. Let’s try to concretize this vague idea. We can do this by defining the object of sovereignty (“*what* do we want to become sovereign over?”) and the corresponding actor (“*who* is supposed to become sovereign here?”) more precisely.

1.1 Objects of digital sovereignty

What exactly “the digital” is that we want more sovereignty over can vary greatly, depending on whether we are talking about resource dependencies, skills shortages, digital education or platform regulation, for example. In somewhat simplified terms, digital technologies and infrastructures can be represented on three layers, which together form the technology bundle: the physical layer, the code layer and the data layer [4][7][8]. Virtually every digital application we use is based on a combination of IT components on these three layers.

To write an email, we need several devices (physical layer). We compose it via a user interface, behind which there are a number of programmed software components (code level) and finally send it by routing the message to the recipient via various servers and internet nodes using defined standards and protocols (data level).

Digital sovereignty can be conceived at each of these layers by asking to what extent they can be shaped in a *self-determined* or at least *fairly independent* manner. At each technology layer, the desired freedom of choice and design extends across the entire service chain, that is, from research and development through production, marketing and operation to self-determined and secure usage [9].

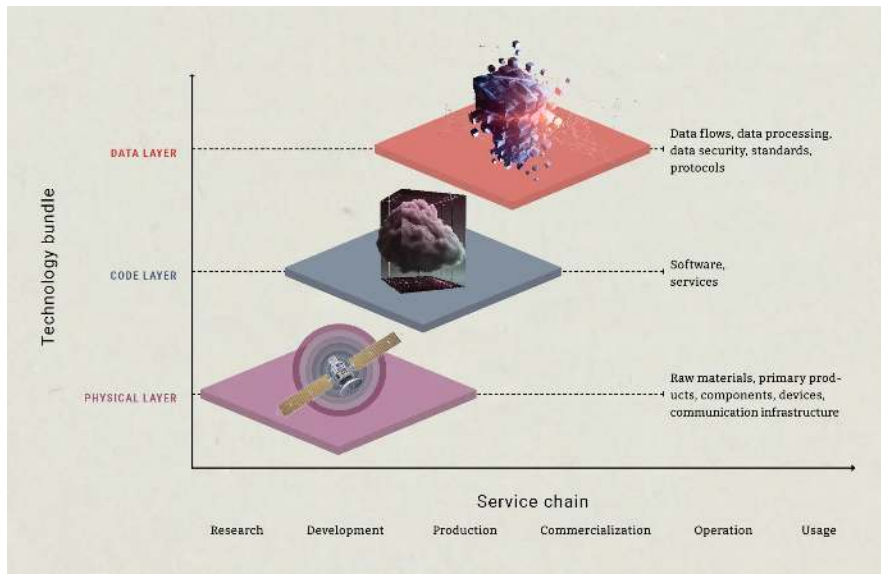


Diagram of technology layers with data, code, and physical layers, and their associated value chain

However, it is neither possible nor sensible to become “self-sufficient” (completely independent) in all these areas. Rather, it may be sufficient to create scope for decision-making so that there is a choice between several alternatives. In any case, certain dependencies cannot be avoided. In Europe, for example, there are no significant deposits of the rare earths needed for the production of important technological components. Dependence on the import of such resources is therefore inevitable. There are also dependencies that are not inevitable but have simply grown over many years, such as the

dominance of U.S. companies in cloud computing. Efforts to free oneself from such dependencies or to reduce them are also referred to as “acts of resistance” to digital forms of hegemony [6]. After all, the struggle for digital sovereignty also reveals the continuation of a race for economic, political and military dominance in the world. In addition to physical territories such as land, water, air and space, digital space has become another arena for geostrategic power struggles [10].

1.2 Actors of sovereignty

There is a lack of clarity in the discourse on digital sovereignty, particularly with regard to the question of whose sovereignty should be strengthened. The circle of “sovereign actors” is often interpreted very broadly in political and academic discourse. For example, it can refer to the digital sovereignty of individual countries or groups of countries, such as Germany [9], the EU [11] or the Global South [12]. The focus is also often placed on social sub-sectors or organizations, be it public administration [13], academia [14], private companies [15], civil society [16] or individuals [17]. We will return to these actor groups in the third chapter because political measures to increase digital sovereignty are usually aimed at specific actor groups and each group has different ways of expanding and utilizing its scopes of action for shaping the digital space.

However, the wide variety of actors discussed today has only grown over time. When the term sovereignty was first used in the digital context around 30 years ago, its meaning was still very much based on the understanding of state theory, which clearly focused on the state as the sovereign actor. This understanding is expressed in the Charter of the United Nations. By signing the Charter, the now 193 member states have committed themselves to *respect the sovereignty of other states*. In this regard, the UN Charter deals with two essential concepts of sovereignty; namely, internal sovereignty and external sovereignty.

External sovereignty

External sovereignty refers to the prohibition of the use of force and the *territorial integrity* of states guaranteed by it. UN member states expressly declare that they will refrain from any use of force or threat of force against other states. Wars of aggression are not compatible with the UN Charter, and even propaganda for wars of aggression is explicitly prohibited. If a state is attacked, it has the right to defend itself. The external sovereignty of a state is given if its territorial integrity is preserved.

Internal sovereignty

Internal sovereignty refers to self-determined internal organization: Each state has “*the right freely to choose and develop its political, social, economic and cultural systems*” [18]. Sovereign states are therefore free to decide, for example, whether they pursue a social market economy or a centrally planned economy, whether a one-party system or a democratic republic governs, or whether they grant secular power to the church. A state is internally sovereign if it can decide on its internal affairs in a self-determined and independent manner.



Since 1945, the United Nations has built on the promise to uphold the sovereignty of all states.

[View source](#) ↗

In-depth text

What does sovereignty mean?
A historical excursion



THE GREAT AWAKENING. WHY DO WE WANT TO BECOME DIGITALLY SOVEREIGN?

Over the past 25 years, digitalization has transformed vast areas of society. Leisure activities, interpersonal communication, media consumption, administrative processes and even entire professional groups have shifted to the digital space. There were profound upheavals that raised new questions about autonomy, control and the distribution of power between different interest groups. Over the course of time, there were a number of events in the context of which the notion of sovereignty was used and re-interpreted time and time again, until digital sovereignty finally became a political high-value word that, while omnipresent, has an enormous range of meanings and is rarely defined.

In this chapter, we recapitulate *seven central developments* in the history of the internet in the context of which sovereignty was mentioned and which changed how digital sovereignty was interpreted. On the one hand, this explains why the term has become so ambiguous over time. But it also shows that along the entire value chain of digital infrastructures, the power and design interests of various groups clash and need to be negotiated. In the third part of this compact overview, we will look at how this can ultimately succeed and how perceived grievances are addressed.

2.1 Cyberspace sovereignty

People have been talking about sovereignty for many centuries, and one thing has always remained the same: it is tied to a territorial concept. State sovereignty always refers to a defined, physically existing area that determines the *borders of the national territory*. However, digital space – often referred to as “cyberspace” in the 1990s – is not a physical territory in this sense, as there is simply no fixed geographical and political frame of reference as with a

national territory. The question therefore arose early on as to whose national territory cyberspace belonged to, if any.

In the mid-1990s, this was referred to as “cyberspace sovereignty” by the technical community and in the academic and journalistic debate. The dominant narrative was that cyberspace was a new sphere of human activity that was fundamentally different in nature from everything that had gone before. People were convinced that it would be difficult or even impossible to regulate or control it with existing legal instruments. Laws, it was commonly assumed, were only valid within defined territorial boundaries — outside these boundaries they were neither enforceable nor did they have legitimacy [23]. One of the most daring claims was that cyberspace, with its cross-border, global networking and decentralized organization, was so exceptional that it needed *its own sovereignty*, similar to a separate nation state. This vision of cyberspace as an independent space with decentralized government is embodied by internet pioneer John Perry Barlow. In 1996, he wrote the “Declaration of Independence of Cyberspace,” which is most impressively presented by himself.



John Perry Barlow, internet pioneer



The multi-stakeholder governance ideal - Governing with the wisdom of the many

Initially, “governing” the internet mainly meant taking technical decisions, for example, in the development of standards and data protocols. The internet was to become a quasi-neutral structure in which information could be transported freely and openly from one end of the world to the other and to which all people would have equal access. In line with the ideals of freedom and openness, the multi-stakeholder governance model had become established for decision-making. Ideally, anyone who spent time on the internet would also be able to participate in its development [24]; that is, not only governments, but also the private sector, the technical community and civil society. In accordance with the principles of inclusion, transnational cooperation and consensus-building, decisions concerning the technical development of the internet were therefore made jointly by many different stakeholders [25].

Towards the end of the 1990s, the commercialization of the internet began, which was accompanied by a rapid increase in the number of users, available applications and retrievable content. The existing “governance system” of the internet — maintenance and regulation of technical structures based on collective decision making — was not suitable for ensuring that available

content and applications complied with local legislation. State intervention and regulation was therefore increasingly seen as necessary in order to shape the internet in accordance with national legal concepts [26][27]. Thus, at the level of applications and content on the internet, state regulatory measures increasingly prevailed, while at the level of technical infrastructures, standards and protocols, non-governmental organizations still “govern” based on multi-stakeholder governance processes.

2.2 The walled gardens of the proprietary internet

The commercialization of the internet ultimately led to more state intervention in the internet. But it also meant increasing private sector intervention in the design of technology. Precisely because the internet was able to develop freely and organically over many years and was not created on the initiative of commercial companies, it allowed radically new forms of cooperative value creation [28]. Open-source methods, in which internationally dispersed groups of people wrote code and software together, often free of charge, played a special role. Such collaborations were only possible because the internet was an “open platform”: it was not built for a specific, commercial purpose, but as an open, creative space that was constantly being changed and developed by its users.

Jonathan Zittrain [28] illustrates the effects of commercialization on this creative freedom with a comparison of the Apple II from 1977 with the first iPhone, which came onto the market 30 years later. Similar to the internet, the Apple II was also a changeable platform that virtually invited hobby programmers but also companies to develop new programs and functions. Any individual contribution that complied with a basic set of rules (such as a programming language or certain internet protocols) was generally acceptable and was shared and developed further as desired. Many of the programs created in this way contributed greatly to the market success of Macintosh computers.



Apple II, 1977

The iPhone, on the other hand, symbolizes the advance of the digital in the form of “sterile,” pre-programmed devices and services. It is no longer possible to change view or even change the program code. Programs to be installed are pre-selected in app stores or installed directly on the smartphone by default. Security updates for older devices are discontinued at will. While the computer and internet revolution was once driven by innovative design freedom, the proprietary version of the digital world is now an aesthetic world of “walled gardens” [29]. This world may be easy to use, well-designed and convenient, but it is woven into a network of commercial control and restriction. This version of the digital goes hand in hand with a severe loss of digital self-determination and significantly restricts creative freedom. In light of this, industry associations such as the Open Source Business Alliance (OSBA) have been arguing for years that the path to digital sovereignty will increasingly be paved by the use and further development of open source software and open standards, especially in public administration [30].



iPhone, 2007

2.3 The power of platforms

The accelerating commercialization of the internet since the late 1990s has provided compelling reasons to view the digital ecosystem as a challenge to state sovereignty. For many years, the U.S. tech giants – above all Alphabet, Amazon, Meta, Apple and Microsoft – were able to build up almost unrivaled power. As platform companies, they gradually integrated more and more applications and services into a core platform. Their infrastructures became ubiquitous communication and organizational tools in everyday private life as well as in countless companies and in public administration [31]. The platforms often benefited from the “network effect” [32], the principle whereby a network becomes more valuable the more members it has. For example, once a social network has reached a critical mass of members, the number of users increases exponentially until competitors can hardly compete and a monopoly almost inevitably forms.



Prof. Dr. Jeanette Hofmann

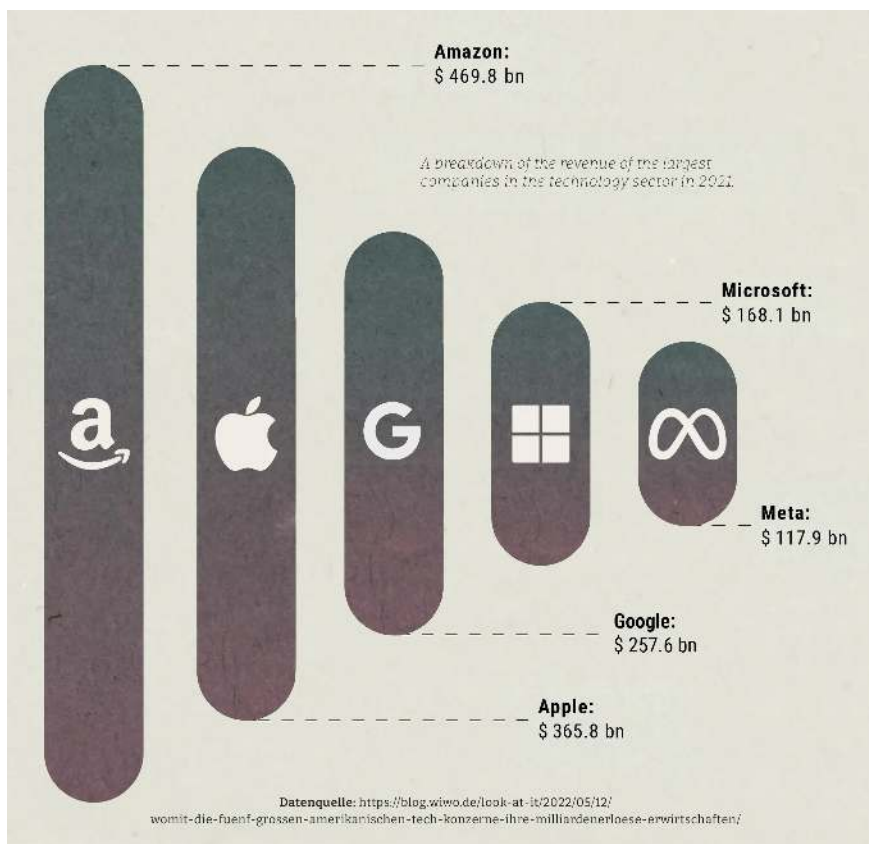
Principal Investigator of the research group "Technology Power and Domination" at the Weizenbaum Institute.

"The economic theory of network effects states that the value of an infrastructure such as the telephone network increases with the number of connected people and objects. Expanding infrastructures therefore create a more or less uncoerced compulsion to connect to them." (2020)

[Go to profile ↗](#)

Platform companies offer essential technical infrastructures and services on the internet that private individuals, companies and public services rely on. They provide content and communication channels, shape public spaces and operate marketplaces over whose competitive conditions they have a decisive influence. This means that a small number of large American companies have far-reaching scopes of action and regulatory competence, not only over technical infrastructures but also over the socioeconomic conditions and processes that take place within them [33]. Platform companies are therefore often referred to as being “quasi-sovereign” in the digital space [18].

The dominance of platforms poses a market risk for Europe because it threatens to distort competition and jeopardize economic stability and innovation [31]. Platform companies have more or less exclusive access to the enormous amounts of data produced within their structures. This data gives them a direct advantage over their competitors. However, large amounts of data are also a prerequisite for developing key technologies such as artificial intelligence [15]. On a regular basis, the disadvantages that arise for European companies due to the dominance of platform companies are seen as a restriction of their scope of action and thus their digital sovereignty [7][15].



Revenues of the largest Tech companies in 2021, showing Amazon, Apple, Microsoft and Meta.

One-sided dependence on foreign-controlled companies is also seen as a potential security threat. Governments can use platforms as political leverage and pressure against those who are dependent on them. The U.S. government demonstrated this in the trade conflict with China in 2019, for example, when the Department of Commerce forced Google by decree to cease all business with Huawei [35]. This is another reason why the one-sided dependence on platform companies is seen by politicians as a challenge to digital sovereignty [30][31]. Finally, the dominance of platform companies is also reflected in their relationship with their users, whose data has become the raw material of

lucrative digital products and whose individual digital sovereignty has been significantly weakened as a result [15][37].

Surveillance capitalism - The business with data

For many years, large platforms have been increasingly turning to lucrative advertising to finance their free services. It became clear early on that advertising can be implemented particularly effectively on the internet, due to the ability to personalize and target it. To this end, user data is systematically collected, enriched and analyzed in the background. *Demographics, consumer behavior, social contacts, interests and preferences, personality, life situation, location* – the more detailed the findings, the better individually tailored advertising measures can be presented at the right time, in the right place and in the right context. The enormous market value of the platforms is therefore based to a substantial degree on their ability to predict and effectively influence future (consumer) behavior. While users have become increasingly transparent in the context of these business models, the industry behind them has remained comparatively opaque. In this context, we speak of “information asymmetry” – a situation in which two contracting parties do not have the same information. If future behavior is deliberately manipulated on the basis of unequal information, information asymmetry also results in power asymmetry [38]. The fact that such power asymmetries can also have potentially harmful consequences for democracy was discussed intensively in 2018 in connection with the Cambridge Analytica scandal [39][40].

Harvard economist Shoshana Zuboff sees these systems of surveillance capitalism as an *attack on individual digital sovereignty* because they undermine the autonomous ability of individuals to act and make decisions [37]. Especially when citizens’ self-determined ability to act is undermined in the context of democratic processes (such as elections and referendums), this can also be understood as an encroachment on the internal sovereignty of the state, which is at least enabled by platforms. In November 2019, Zuboff was at the Humboldt Institute for Internet and Society (HIIG) in Berlin to talk about the age of surveillance capitalism.



2.4 Mass surveillance and cyber espionage

Lucrative data-based business models offered companies a strong incentive to collect more and more data about users and infer further insights from it. However, the availability of such detailed information is also an incentive for other actors, not least for the police and security authorities, to use it for their own purposes [41].

The new convergence of commercial surveillance and security agencies was revealed in 2013 in an unprecedented leak by U.S. intelligence officer Edward Snowden. The extensive digital surveillance that Snowden uncovered is considered one of the key events that led to digital sovereignty becoming a demand in European politics. The understanding of sovereignty under international law includes the self-determination of domestic organization, meaning that no one has the right to interfere with it. However, if another state – in this case the USA – secretly operates systematic, broad-based surveillance programs that specifically target political institutions, this can certainly be seen as an encroachment on state sovereignty.

Not least, the discourse on digital sovereignty is also about the digital self-determination of individuals and civil society. Individual data sovereignty – that is, the “targeted, informed provision of one’s own data” [42] – is directly undermined by the mass surveillance of communication data without cause.

The NSA affair



The documents leaked by Snowden prove that the secret services of Western countries, particularly the USA, are engaged in extensive global surveillance. Doubts about their credibility were unequivocally dispelled by the European Court of Justice in two judgments. In 2015, the highest judges confirmed that “the NSA and other United States security agencies” access personal data “in the course of a mass and indiscriminate surveillance and interception” [43].

In-depth text

Digital espionage – the NSA affair

Political and industrial espionage

The NSA affair also showed that one task of the secret services was to conduct *industrial espionage*. This became known as early as 2001, when a committee of the European Parliament looked into “Echelon,” a global interception system of the Five Eyes, which intercepted global satellite communications [54]. The committee’s report suggested that the intelligence network was specifically eavesdropping on the communications of companies. Foreign companies were spied on in order to give American companies a competitive advantage. With the information obtained, U.S. companies were able, for example, to beat their European competitors to patent applications [55][56], or outmaneuver them in negotiations [57][58]. The Snowden leaks show that industrial espionage was still one of the NSA’s strategic missions 10 years later [59]. In addition to Russia and China, Germany and France were also among the NSA’s target countries. The mission was to prevent any advance in critical technologies that would give these countries military, economic or political advantages.

NSA documents also describe years of systematic and targeted eavesdropping on top politicians – including Angela Merkel [60] – and political institutions. The political targets reportedly included the headquarters of the United Nations [61], the International Atomic Energy Agency [62] and, by means of a cyberattack on the Belgian company Belgacom, presumably also the European Commission, the European Council, the European Parliament and NATO [63].

2.5 Isolation and seclusion

In authoritarian states such as China or Russia, the advance of networked communication was perceived as a threat to the existing political order [5]. China was one of the first countries to respond with a strategy of maximum technical isolation and control. Russia followed suit a few years later. In doing so, the Chinese government relied on its typical interpretation of national sovereignty as a non-interference principle. In essence, no other country should interfere in Chinese affairs, and China would not interfere in the affairs of other states (for example, in armed conflicts). This sovereignty rhetoric was already used by China in the early 2000s. After the NSA affair in 2013, it was applied more to the digital context and became a further interpretation of digital sovereignty, which in its radical implementation is far removed from the European understanding. In this context, digital (or cyber-) sovereignty means subjecting data flows and digital infrastructures as completely as possible to national control.

weapons.
 2. Threats posed by foreign space and counter-space systems: China and Russia
 Accepted Risks:
 a. Weapons and force developments in: Saudi Arabia, and India
 b. Threats posed by foreign space and counter-space systems: India and France.

OSD J. MISSION: Emerging Strategic Technologies: Preventing Technological Surprise.
 Focus Areas: Critical technologies that could provide a strategic military, economic, or political advantage: high energy lasers, low energy lasers, advances in computing and information technology, directed energy weapons, stealth and counter-stealth, electronic warfare, robotics, space and remote sensing, cyber-a-spies, nanotechnology, emerging materials. The emerging strategic technology threat is expected to come mainly from Korea, China, India, Japan, Germany, France, Korea, Brazil, Singapore, and Sweden.
 Accepted Risks: Technological advances and/or basic S&T development on a global basis elsewhere.

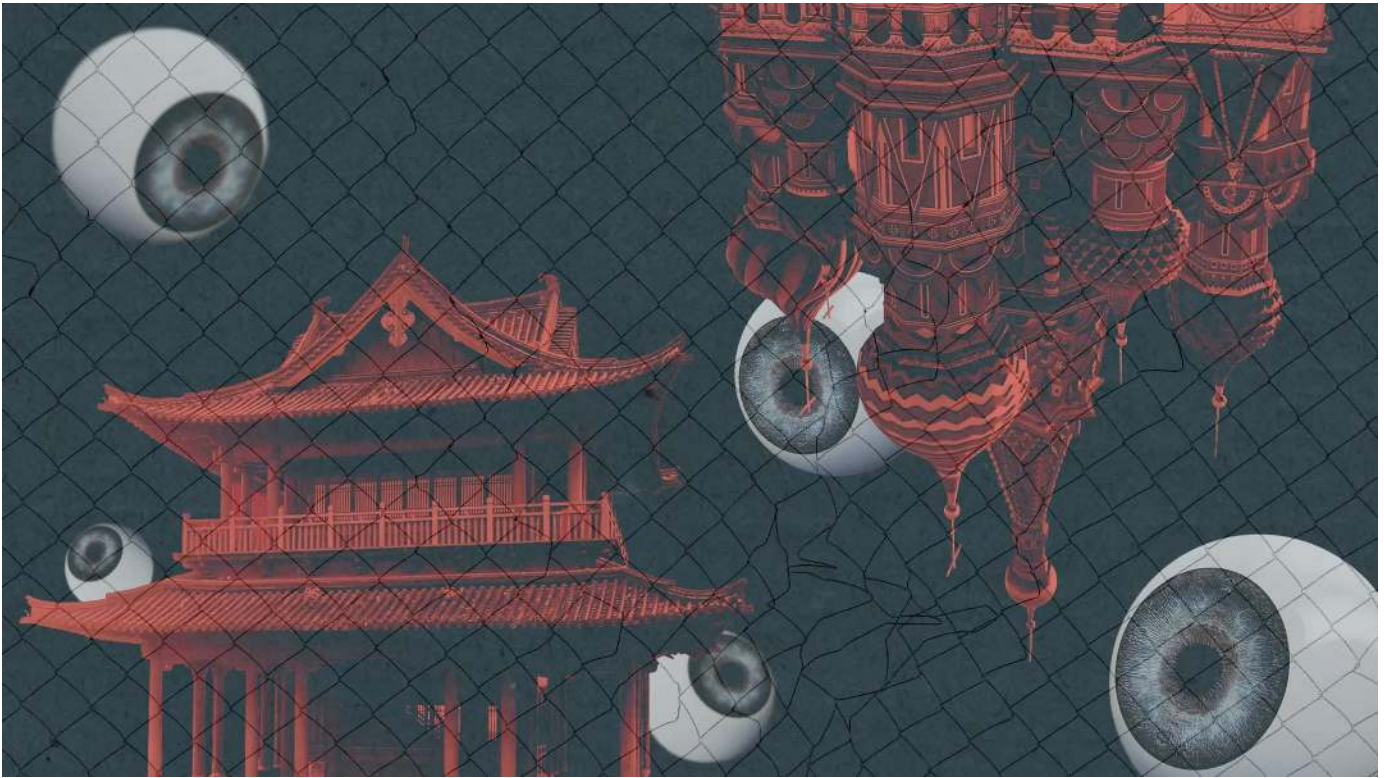
OSD K. MISSION: Foreign Policy Includes Intention of Nations and Multinational Organizations: Ensuring Diplomatic Advantage for the U.S.
 Focus Areas: Policies, objectives, programs, and actions on the part of governments or multilateral organizations that could affect U.S. interests in Asia, Africa, Europe, Middle East, and Western Hemisphere.

Leaked NSA documents: Even among allies, industrial espionage serves the purpose of securing military, economic and political advantages

New York Times

[View source ↗](#)

The splinternet: Authoritarian states seal themselves off



In response to the NSA affair, China was one of the first countries in the world to declare “cyber sovereignty” as the goal and principle of its digital policy measures in 2015. In his opening speech at the Global Internet Conference in 2015, China’s President Xi Jinping declared that, in the spirit of state sovereignty, each country should be allowed to pursue its own regulatory approaches on the internet [64]. No one should intervene in the cyber sovereignty of another country, interfere in the internal affairs of other states via digital channels or support cyber activities that undermine the national security of another country [65]. China sees digital sovereignty primarily as a way not only to maintain national security and protect the country from cyber threats and economic espionage [5] but also to support the local economy by giving preferential treatment to Chinese companies [65]. The situation is similar in Russia, where digital sovereignty is equated with greater state control over the digital space and, in particular, over data traffic on Russian territory [65]

An important part of this strategy is *data localization* [66], which provides that data should only be stored, transferred and processed within national borders and legal jurisdictions. To this end, it is necessary to gain control over the essential technical infrastructures of the internet or to locate them on one’s own national territory. Technically, this is implemented, for example, with national data infrastructures, local data centers, national routing, national e-mail services and a national internet backbone infrastructure [67].

The structures created also offer new opportunities for systematic surveillance and censorship of the population. In Russia, for example, since 2019, internet service providers are required by the Sovereign Internet Law to install network equipment which allows for more effective traffic monitoring and blocking of unwanted content. In China, since 2019, the Internet Domain Name Regulations have ensured that any cross-border data traffic that has not

previously been explicitly approved by the censorship authorities is blocked. For example, if a foreign-registered news portal wants to be available in China, it will have to censor itself [68].

Isolationist tendencies in the EU

After the NSA affair, arguments for greater technical isolation were also voiced in Western countries, for example in the discussion about Schengen routing [69]. The declared aim was to strengthen protection against espionage activities by foreign intelligence services in the Schengen area. The Schengen routing would have had the welcome side effect that European companies, especially Deutsche Telekom, could have benefited from this implementation [70]. However, the idea was soon discarded, because data traffic is just too globally networked, actual benefits would be too small, and the danger of a “splinternet” – an internet fragmented into many isolated areas on the basis of geographical and commercial boundaries – was too great [48][49]. Yet, even a decade after the NSA affair, similar arguments for the localization of essential technical infrastructures within the EU are still being made in the debate about digital sovereignty, for example, in the context of the European data infrastructure project Gaia-X [73].



Prof. Dr. Thorsten Thiel

Associated researcher at the Weizenbaum Institute

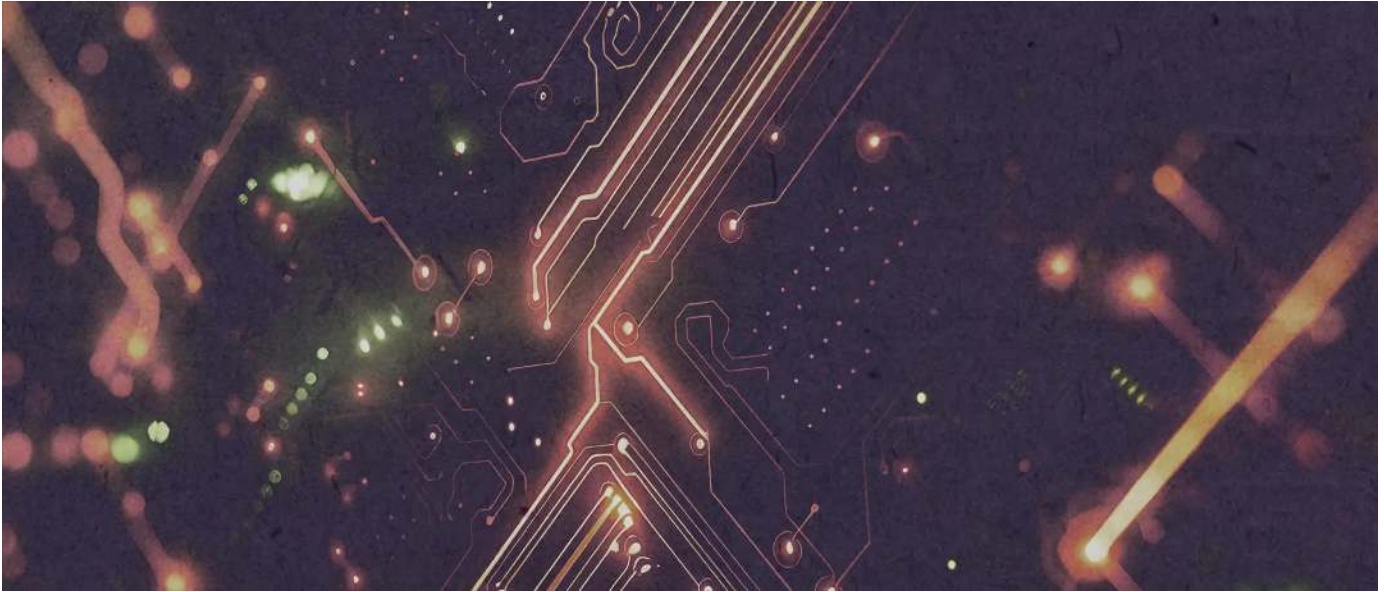
“In the wake of the Snowden revelations, Schengen routing was a political push to further nationalize data traffic in order to prevent U.S. services from gaining access to communications that take place exclusively between nationals of a region – in this case, the region of those European countries that have joined the Schengen Agreement.” (Thiel, 2014)

[Go to profile ↗](#)

2.6 Geo-economical dependencies

Especially at the EU level, the debate about digital sovereignty is often about freeing oneself from economic dependencies. The digital industry is characterized by dependencies like hardly any other branch of industry. Those who master essential components or services are in a position to put pressure on other states, while those who are dependent on individual suppliers or countries make themselves susceptible to blackmail. Such economic dependencies are very prominently discussed in the discourse on digital sovereignty because they diminish the ability – especially of European industry – to act in an independent and self-determined manner. Digital sovereignty (in this context often referred to as “strategic autonomy” [74]) means reducing structural dependence on digital technologies, components and intellectual property from abroad in order to secure availabilities, create choice, and, last but not least, strengthen one’s own economic competitiveness [31].

The semiconductor industry



Microchips – electronic components based on semiconductors – are a particularly essential component of digital infrastructures. They provide the basis for a wide range of modern devices, from smartphones to computers, televisions, cars, industrial robots, weapons systems and medical devices.

The semiconductor industry in particular is characterized by extraordinary dependencies. After all, the astonishing advances in microelectronics have only been possible because companies have become extremely specialized over time. Instead of offering all steps from circuit design to testing and assembly from a single source, it made more and more economic sense to specialize in a core business, which was then scaled accordingly. In Silicon Valley, companies such as AMD, Broadcom and Qualcomm increasingly focused on high-margin work steps such as the design of blueprints and circuit designs. Large contract manufacturers emerged in Taiwan, such as TSMC, the world market leader in the production of logic and high-performance chips, which are used, for example, in artificial intelligence [79]. Microchips are based on globally distributed, fragmented supply chains and highly complex production processes. Thousands of work steps are meticulously intertwined, refined and specialized over decades. No country in the world would currently be able to develop and manufacture a sufficient amount of microchips on its own.

Decades of technology-driven globalization have created complex risk cascades [31]. If the availability of even one essential component fails, entire industry branches threaten to collapse. It would take decades and enormous investments to rebuild production capacities in one's own country. From a pure economical perspective, this would be illogical and inefficient. Yet, in the semiconductor industry, market-based logics have long lost their impact because trade relations have politicized over the years.

Politicization and trade war

Governments have recognized that it is specifically the reliance on foreign-sourced microchips that makes them vulnerable. Semiconductor products are essential for many industries and products, and their availability is already uncertain due to fragile supply chains without fall-out options. In addition,

In-depth text

What is a microchip?

there have been several supply disruptions in recent years, some with dramatic consequences; for example, when an unexpectedly high demand for computers collided with border closures and lock-downs during the Covid-19 pandemic. Efforts to free oneself from these dependencies are seen as a path to digital sovereignty [7].

The global semiconductor industry has become the arena of international geopolitics and an instrument for exerting targeted influence on other states [9]. There has long been a power struggle between the U.S. and China for political, economic and military supremacy in the world, which has plunged the two nations into an open trade war. Of course, there are similar efforts in Europe, they just have not been particularly successful so far. The USA and China are competing with each other in key technologies such as artificial intelligence, autonomous weapons systems, and quantum computers – all fields of technology in which high-performance chips are used. In the chip industry, competition developed for patents, manufacturing equipment and skilled workers. Both countries massively subsidize their domestic semiconductor industry. At the same time, they increasingly sanctioned each other with import tariffs and export restrictions in order to gain economic advantages and prevent knowledge transfer. But the semiconductor industry just cannot be relocated quickly. American high-performance chips are still predominantly manufactured in Taiwan, which is why the U.S. is particularly concerned by China's ambitions to take over the Taiwanese peninsula. This could give China not only insights into production processes but potentially even control over the export of microchips to the US.

2.7 Cyberattacks and hybrid threats

The topic of cybersecurity has also entered the debate on digital sovereignty, as security agencies in particular see a high level of cyber security as a prerequisite for the digital sovereignty of civil society, economy, science, and the state [80]. They all can only independently and safely exercise their role in the digital world if they can rely on secure technologies and the respective digital competences for the secure handling of technology.

However, digital infrastructures are susceptible to sabotage and are targeted by hackers driven by both profit motives and political interests. Cyberattacks are becoming more frequent, especially on government institutions and on small and medium-sized enterprises, which are often less resilient than large companies. The threat level is assessed by German authorities as *“higher than ever before,”* with the focus of current waves of attacks on ransomware [81]. A ransomware attack is a form of digital blackmail. Attackers exploit security vulnerabilities to penetrate and encrypt systems. Often the only way to regain the data is to pay a ransom [81]. Ransomware attacks also frequently target critical government infrastructures, such as healthcare systems or supply infrastructure (such as the Colonial Pipelines).



On this topic, we recommend the business book of the year 2022 by Prof. Chris Miller. **Chip War – The Fight for the World's Most Critical Technology**

[🔗 Prof. Chris Miller](#)



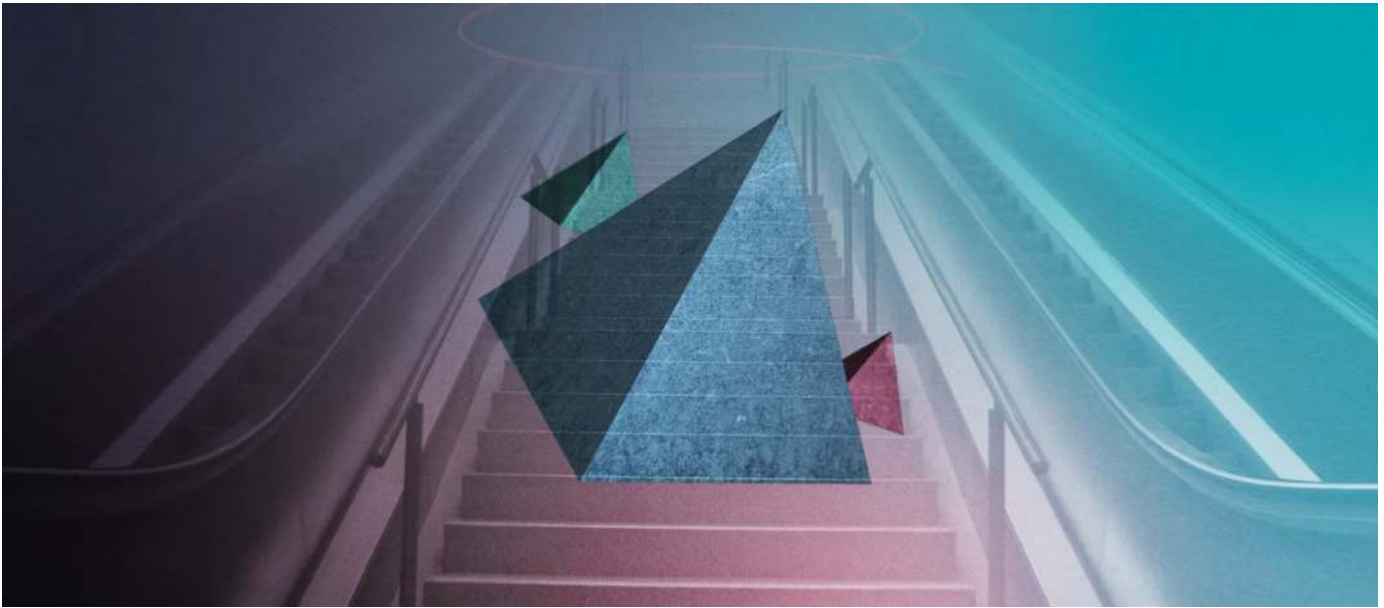
Global cyberattacks in real-time

Kaspersky, 2024

[View source](#)

In addition to cyber-attacks, the discourse on digital sovereignty also frequently addresses the danger of hybrid threats. These involve the deliberate spread of disinformation and propaganda, which can undermine democratic processes and lead to unrest. In a study, the EU Commission outlined the acute danger posed by disinformation and targeted propaganda: Hybrid threats jeopardize “human rights, the rule of law, democratic processes, national sovereignty, and geopolitical stability” [82]. The digital influence through disinformation and propaganda consequently leads to a growing mobilization potential among European citizens, particularly in susceptible environments such as among right-wing extremists, conspiracy theorists, and individuals who delegitimize the state.

The EU considers it a part of digital sovereignty that EU citizens are free from intentional external influence in the digital space and can make self-determined decisions [83]. We have encountered a similar aspect in the context of data economy in a slightly different form (see chapter 2.3.): Whether corporations manipulate consumer behavior for profit or foreign actors spread disinformation to create public unrest, in both cases digital structures are used to deliberately influence (individual or public) opinion and (individual or collective) behaviors. Digital sovereignty can be interpreted here as the ability to make self-determined decisions in the digital space free from external influence [83].



WAYS INTO THE SELF-DETERMINED FUTURE. HOW DO WE BECOME DIGITALLY SOVEREIGN?

The political discussions surrounding digital sovereignty in the EU revolve around various policy areas that can be seen as building blocks to strengthen digital sovereignty [84]. In the following, we will explore the options for action of various groups of actors. Civil society, the economy, science, and public administration all have the opportunity to gain digital sovereignty themselves. Additionally, lawmakers can support them in this endeavor through targeted political measures. Here, the EU plays the important role of balancing the sometimes-conflicting interests of different actor groups. But which priorities does the EU set in its digital policy agenda, and what principles it is guided by in doing so?

3.1 Legislation as a value-oriented instrument of governance

Ideally, digitization should meet the needs of society across all actor groups [85]. Therefore, the EU strategically aims to orient its digital policy towards “European values” and to create technological and regulatory structures that uphold these values.

Margrethe Vestager, who initiated numerous judicial proceedings against U.S. tech giants as EU trade commissioner, emphasizes the goals of the European digital strategy [86].

Three things become clear here: First, competitiveness is a key concern of the EU, and it clearly pursues its own economic interests with its digital policy. Second, Vestager cites the security and fundamental rights of EU citizens as guiding principles of the European digital agenda, but also emphasizes that regulations are only employed where these values are threatened. This can be understood as a distinction from the sovereignty ambitions of authoritarian states, which often seek to enforce greater control over their own society in the digital realm (see chapter 2.5).

Thirdly, Vestager mentions that European standards have worldwide implications. She thereby alludes to the “*Brussels Effect*.” Given the considerable size and attractiveness of the European market, EU regulatory measures often have a strong impact on companies and governments outside the EU. They have an incentive to follow European regulatory approaches if they want to do business in the EU [87]. It is also argued that the EU, in its role as a “*global regulatory hegemon* [87]”, intervenes in the sovereignty of other countries.



Simon Schrör

Since 2022 leader of the research group “Norm Setting and Decision Processes” at the Weizenbaum Institute

“The Brussels Effect refers to the EU creating economic incentives for the adoption of its regulatory approaches beyond the European single market. It effectively becomes a *regulation exporter* and can indirectly exert control over companies and the laws of other governments. Viewed critically, the Brussels Effect can also represent indirect interference in the sovereignty of other, usually smaller, states.” (2024)

[Go to profile ↗](#)

But which control options do the EU and the German federal government actually utilize to strengthen digital sovereignty? What leeway do civil society, organizations, and institutions themselves have at their disposal to expand their respective scopes of action? We start with the foundations of digital sovereignty, which are of systemic relevance across all actor groups and technology layers: Sufficient education and participation of civil society, comprehensive cybersecurity and development of key technologies. We will then consider the most important options for action along the three layers of the technology bundle: data layer, code layer, and physical layer.

3.2 Basic conditions of digital sovereignty

“By setting the standards, we can pave the way for ethical technology worldwide and ensure that the EU remains competitive along the way. [...] Our rules will intervene [...] when the safety and fundamental rights of EU citizens are at stake.”

Margrethe Vestager, executive vice-president for a Europe fit for the digital age, European Commission, 2021

Digital sovereignty can only be built upon a digitally sovereign civil society. *“Only digitally empowered and capable citizens [...] can be the masters of their own destiny, confident and assertive in their means, value and choices,”* emphasizes the EU Commission [88]. What is frequently referred to as individual digital sovereignty in scholarly literature encompasses digital competency and participation. Digital literacy and competences *enable* civil society to *“act and decide in a conscious, deliberate, and independent manner”* [65]. Meanwhile, opportunities for participation *empower* civil society to engage in digital policy discourse and decisions, as well as directly in the shaping of technology [16].

Individual self-determination through digital competencies

Let's start with the question of what skills are actually needed to make deliberate and independent decisions in the digital space and thus become somewhat digitally sovereign. Digital literacy encompasses knowledge and skills across all layers of the technology bundle.

🔧 Technical proficiency

First and foremost, it is important to be able to use technology in general. Digitally competent persons will be able to handle various IT components—end devices, important applications, and internet services—and know both how and for what purposes to use them [42][89]. They will also have enough prior knowledge to be able to “make comprehensive and qualified decisions about the release, collection, storage, use, and processing of their own data” [42].

📺 Media proficiency

Once a person can operate technology, it becomes necessary to also be able to use and assess the media accessed in the digital space. This means the ability to effectively search for information [42][89] and to judge the quality and credibility of sources and communication partners by critically questioning them [90][16][42].

🔒 IT security

Among the essential competencies of digitally sovereign individuals, the ability to minimize security risks is regularly counted [80], not least because effective self-protection also protects other users [42]. This includes, for example, being able to effectively protect oneself against data loss, identity theft, malware, and phishing.

⚖️ Legal certainty

Not infrequently, at least a basic level of legal certainty is mentioned as part of digital literacy [42]. This includes knowing one’s own rights (e.g., regarding data protection) and being able to assert them. Legal certainty also means knowing the rights of others in the digital space and accordingly being able to act in compliance with the law. This includes copyright and criminal law (for example, regarding digital bullying, defamation, and stalking) [42].

📊 Impact assessment

Digital literacy also involves knowledge about the possible consequences of use for oneself and for others. This can include knowledge about the health effects of IT use such as sleep deprivation or concentration disorders [42] or a deeper understanding of the societal, economic, and state power interests in the digital space [6].

For the European Commission, digital education and skill development are among the top priorities of the European digital policy until 2030 [89]. It is the foundation for enabling the civilian population to critically and consciously engage with technologies and assess the impact of digital transformation on society and the environment [90]. A lack of digital skills can result in social exclusion and significant disadvantages in society, the labor market, and the education system [91]. Conversely, businesses and public administration rely on digitally competent workers to remain competitive in the long term,

highlighting the importance of skills development in civil society for other actor groups as well.

Public educational offerings provide a framework for individual competence acquisition and can help adapt competence development to future needs (such as those of the job market) [16]. In light of this, the Federal Ministry of Education and Research launched an “education offensive” in 2021. This initiative aims to better equip schools with technology, develop digital learning tools, and help education professionals earn relevant (digital) qualifications. For vocational and continuing education, digital training measures are being developed, and freely available educational materials are being disseminated [92]. The Federal Ministry for Family Affairs, Senior Citizens, Women and Youth also focuses on the autonomy of older people. For example, low-threshold, age-specific educational offerings for seniors are being developed [17]. In 2023, the Federal Ministry of the Interior and Community introduced the Digital Driver’s License: a comprehensive educational offering, combined with the opportunity to test one’s own digital skills at various difficulty levels and obtain a certificate upon successful completion [93].

Democratic self-determination through participation and inclusion

Digital competencies help us to navigate the digital space individually self-determined. However, they are also a helpful – if not necessary – prerequisite for actively participating in political and technical shaping processes in the digital world [16]. Participation means becoming democratically self-determined, influencing political decisions in the interest of society, and shaping technologies. The democratic agency of civil society in the digital space can be actively promoted by the state.



Dr. Bianca Herlo

Leader of the research group “Design, Diversity and New Commons” at the Weizenbaum Institute

“People need to be empowered for individual and democratic self-determination in order to also be able to positively influence the cultures, practices, and visions of organization, governments, and civil society with their digital skills and thus contribute to sustainable digital sovereignty” (2023).

[Go to profile ↗](#)

For this, it is first necessary that there is transparency about important political and economic decision-making processes, such as in regulation or in the development of technical standards. Only then can citizens understand and participate in these processes. Representatives of civil society can (and should) actively accompany these standardization processes [94][95], or even be involved in the development of governmental strategies, such as those for building digital sovereignty [85]. These are effective approaches to ensure that public interests are represented early and effectively.

The state can actively promote the democratic participation of civil society by holding committee meetings publicly, communicating procedures in advance, setting adequate deadlines, and inviting citizens to participate in advisory committees or in the drafting of legislative proposals. Participation formats can

also be designed digitally and with low barriers to entry (for example, numerous NGOs demand the establishment of a central publication and participation platform) [96].

Extensive cybersecurity

As the second basic condition for digital sovereignty, strong emphasis is placed on the security and resilience of digital infrastructures [15][97]. Cybersecurity is considered a fundamental requirement for societal life, economic processes, and the protection of critical infrastructure [99]. Strategies and measures to enhance IT security are formulated at both the European and national levels in response to a high level of threat. At the end of 2020, the European Commission presented the new EU Cybersecurity Strategy [100]. Central to this is the plan to address cyber threats across borders, in a coordinated manner, and in close collaboration. The package of measures aims to enforce a uniformly high level of security and resilience of digital infrastructures across the EU. In addition to specific requirements for national cybersecurity strategies and governmental structures, cooperation groups facilitate strategic collaboration on cybersecurity in Europe. National points of EU countries and act as clear points of contact. In the event of acute crisis situations, they should be able to coordinate operational responses quickly, effectively, and across borders.

Simultaneously, better encryption systems and stronger defense against surveillance [101], as well as increased use of open-source software (see chapter 3.4), are seen as technical means to improve cybersecurity. The introduction of trusted security certificates could lead to greater transparency and increased security awareness among users [99][102]. Targeted government support for research and development in the field of cybersecurity is an effective measure to strengthen IT security in the long term and reduce dependencies in this area as well [103].

Key technologies in research and development

Long-term and forward-looking government support for research and development is not only relevant in the field of cybersecurity. Rather, the promotion of key technologies can be understood as another condition for digital sovereignty, which is significant across all actor groups and technology levels. The EU views key technologies as pillars of future economic value creation. Therefore, many EU measures aim to firmly orient the domestic research and business landscape towards the development of artificial intelligence, quantum technologies, cloud technologies, and semiconductor technologies [97]. This is done partly to reduce economic dependencies in the medium term and strengthen the domestic industry, and partly to shape technologies in line with European values [65]. Concrete measures in recent years have often aimed not only at direct financial support but also at improving the competitive conditions for European providers and lowering market entry barriers [65], for example, by specifically supporting start-up ecosystems [97]. At the same time, research and development partnerships can be strategically expanded both between EU Member States and between private companies and states [65].



The European cybersecurity legislation NIS was comprehensively updated in 2023 after only 6 years to keep up with the fast-moving threat landscape. (European Union, 2013)

European Union, 2013

[View source ↗](#)



Massive funding programs are intended to secure Germany's access to key technologies.

Quantum systems research program, BMBF 2022

[View source ↗](#)

3.3 Digital sovereignty at the data layer



In recent years, the EU has developed a variety of successful data policy measures. At the data level, it is evident that legislators are striving to balance the divergent interests of various stakeholder groups. On one hand, the data of European citizens, companies, and institutions must be adequately protected, and violations of data protection laws must be punished. On the other hand, innovative data-based business models should also be able to develop within the EU, as they are associated with societal and economic benefits.

Data protection

Let's start with the interests and rights of civil society at the data level. A milestone in data protection law is certainly the General Data Protection Regulation (GDPR), which, since its implementation in 2018, significantly strengthens the protection of personal data of EU citizens and gives users more control over their personal data. It is considered one of the strictest data protection standards worldwide and sets standards that have already been adopted by numerous other countries [104]. The ability for users to control data they generate themselves is considered an important feature for their digital sovereignty [84]. The strong data protection law limits the powers of data processing companies and increases consumers' right to information, thus reducing existing information asymmetries (see chapter 2.3) in favor of consumers. The GDPR also ensures users have the ability to transfer their data to other applications, which in turn can lower switching barriers and dependencies from specific service providers.

Data economy

In other regulatory approaches of the EU, a more private-sector, growth-oriented data policy is evident. The European Data Strategy [105] aims to develop a functioning European single market for data while ensuring a high level of data protection. The strategy is primarily based on the Data Governance Act (DGA) 2022 and the Data Act 2024. The DGA lays the groundwork for a trustworthy data exchange model that simplifies data-based collaborations between businesses, academia, public institutions, and civil society. The regulation envisions the establishment of independent, transparent, and trustworthy data marketplaces where data suppliers and buyers can come together. Data can thus easier and more transparently be shared between different sectors. The DGA also aims to encourage altruistic data donations: data donations are facilitated and the access and reuse of donated data is organized in a more unambiguous and transparent manner. The Data Act, on the other hand, stipulates that users must be given access to all data generated by their IoT devices and that this data must also be made available to third parties at the request of the user [106]. At best, this means that European companies will also be able to access larger volumes of data from which they can create value.

Cloud infrastructure

As part of the “Gaia-X” project, announced in 2019 by the German and French ministries of economics, existing data infrastructures from various sectors will be interconnected to create a common European data ecosystem [107]. The project aims to facilitate cross-sectoral data exchange and integration. Many previously separate data spaces are thus to be linked together. The task is to formulate appropriate rules and standards for cooperative data exchange and compliant data usage, as well as to define and implement the technical requirements for this new data space. The European Commission emphasizes that its data strategy will make the EU more internationally competitive and contribute to stronger economic growth: Big Tech platforms have “a high degree of market power, as they control large amounts of data,” [108] and the European data strategy aims to counteract the dominance of these platform companies over data spaces. The Gaia-X project in particular began with the goal of combating the data hegemony of U.S. and Chinese corporations and strengthening Europe’s own competitiveness based on “sovereign data exchange” [73] (see chapter 3.3). Meanwhile, partners and members of technical working groups of the Gaia-X organization also include major corporations such as Microsoft, Alibaba, Amazon, Google, and Palantir [109]. As providers of cloud services, they will not only be connected to the created data spaces but also contribute their expertise to the development of these infrastructures. However, they have recently faced criticism for deliberately slowing down the project’s workflows [110].

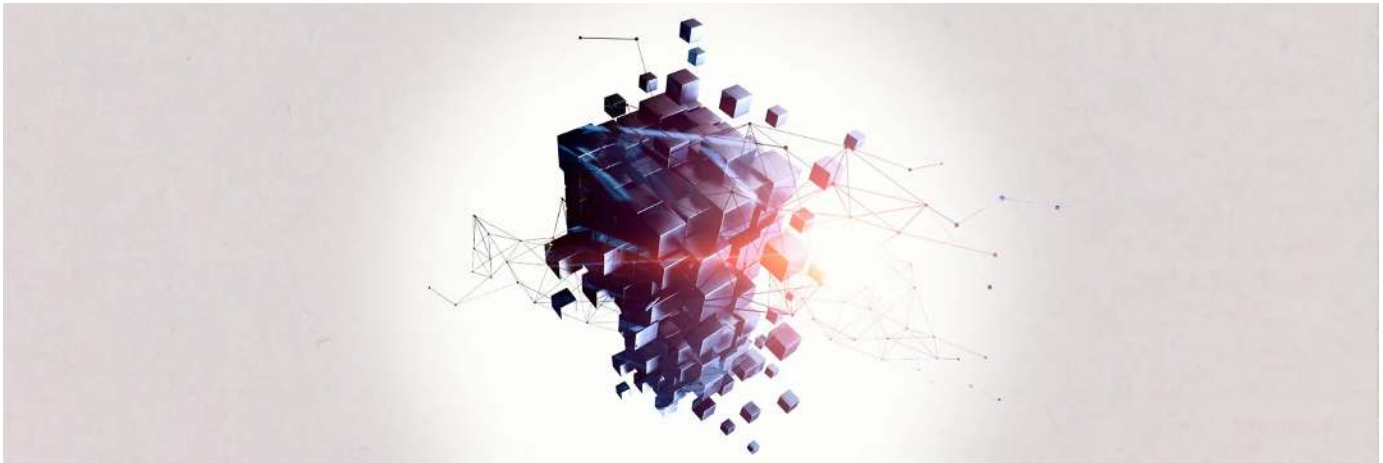


Margrethe Vestager sees the Data Governance Act as an alternative model to the data processing practices of large tech platforms. (European Union, 2020)

European Union, 2020

[View source ↗](#)

3.4 Digital sovereignty at the code layer



Open-source software

At the level of software and applications, the increased use of open-source software is widely emphasized for digital sovereignty. Specifically, the German Federal Ministry of the Interior and Community highlights that the increased use of open-source software fulfills three strategic objectives [111], which apply not only to public administration but also to other societal sectors. The use of open-source software can be considered a lever for all actor groups to strengthen their independence and room for maneuver.

Open-source software provides **options for switching**: on one hand, because it is built more modularly (allowing individual components to be easily exchanged), and on the other hand, because it is more interoperable than proprietary software (open interfaces enable a greater variety of software components to be linked together). The resulting flexibility reduces the dependence on individual software providers. Open-source software guarantees the **ability to co-create**. Since the underlying code is visible and modifiable, it can be better adapted to one's own needs and strengthens potential for collaborations and creative cooperation. If the ability to view, understand, and shape source code has been increasingly restricted by providers of proprietary software, open-source software can rediscover these possibilities. For users – including companies and public institutions – this opens up creative spaces and thus innovation potentials. Ultimately, the use of open-source software also increases **bargaining power** against providers of proprietary software because there are powerful alternatives to their products [111], which are even considered more trustworthy and secure due to their viewability [9].

Platform regulation

The EU aims to enhance individual digital rights to establish greater digital sovereignty and exert stronger control over non-European technology companies, especially platform giants. In response to perceived misconduct by these platform companies in recent years (particularly regarding data privacy, misinformation, and monopolization tendencies), the EU introduced two large-scale new regulations.

Digital Services Act

The Digital Services Act (DSA) aims to better protect the fundamental rights of users in the digital space. Its goal is to “prevent illegal or harmful online activities as well as the spread of disinformation” [112], with particularly strict regulations formulated for very large platforms.

Digital Markets Act

The Digital Markets Act (DMA) aims to level the playing field between particularly powerful companies (“gatekeepers”) and other market participants [113]. Gatekeepers are prohibited from favoring their own products or disadvantaging competing products and providers. Also apps from gatekeepers like Apple or Google must be uninstallable from smartphones.

The regulatory package comprising the DSA and DMA addresses several challenges that are highlighted in the discussion about digital sovereignty. For the civil society actors, digital sovereignty requires effective regulation of disinformation, hate speech, and defamation [95] to ensure that fundamental rights are enforced in the digital space. Through the stricter transparency requirements for personalized advertising and tracking, individual users gain more power to decide whether they want to be shown personalized recommendations and content. Targeted advertising for minors will be entirely prohibited. This is supposed to mitigate the information and power asymmetries between platforms and users and strengthen users’ autonomous action and decision-making.

The DMA also strengthens the digital sovereignty of the economy, as unfair market conditions and business practices by market leaders are effectively limited. This strengthens the opportunities for small and medium-sized enterprises to establish themselves in the development and operation of digital services in the market [113].



Rita Gsenger

Doctoral student in the research group “Normsetting and decision processes” at the Weizenbaum Institute

“Disinformation, illegal content, hate speech and discrimination on platforms can have an impact on social debates and democratic processes and jeopardize the physical and mental well-being of minors in particular. The European Commission is tackling these challenges by holding platforms and search engines accountable. However, the *prospects of success are unclear* and can only be assessed in the coming years” (2024).

[Go to profile ↗](#)

3.5 Digital sovereignty at the physical layer



Physical components play a crucial role in the discourse surrounding digital sovereignty. Of particular focus in policymaking is the expansion of physical IT infrastructure and the strengthening of European research, development, and production capacities.

Extensive infrastructure development

Time and again, the importance of comprehensive expansion of technical infrastructures is emphasized to grant equal access to the digital space and thus enable digital sovereignty for all members of society [90]. Whether it's mobile network coverage or the laying of fiber-optic cables, participation and engagement can only occur for those members of society who have barrier-free access to the digital space [114]. Both the EU and the German federal government demand and actively support improvements in supply coverage. For instance, Germany's "Gigabit Strategy" aims for half of all German households and businesses to have fiber-optic connections by the end of 2025, with "comprehensive, uninterrupted voice and data communication" across the entire country by 2026 [115].

Reduction of supply risks

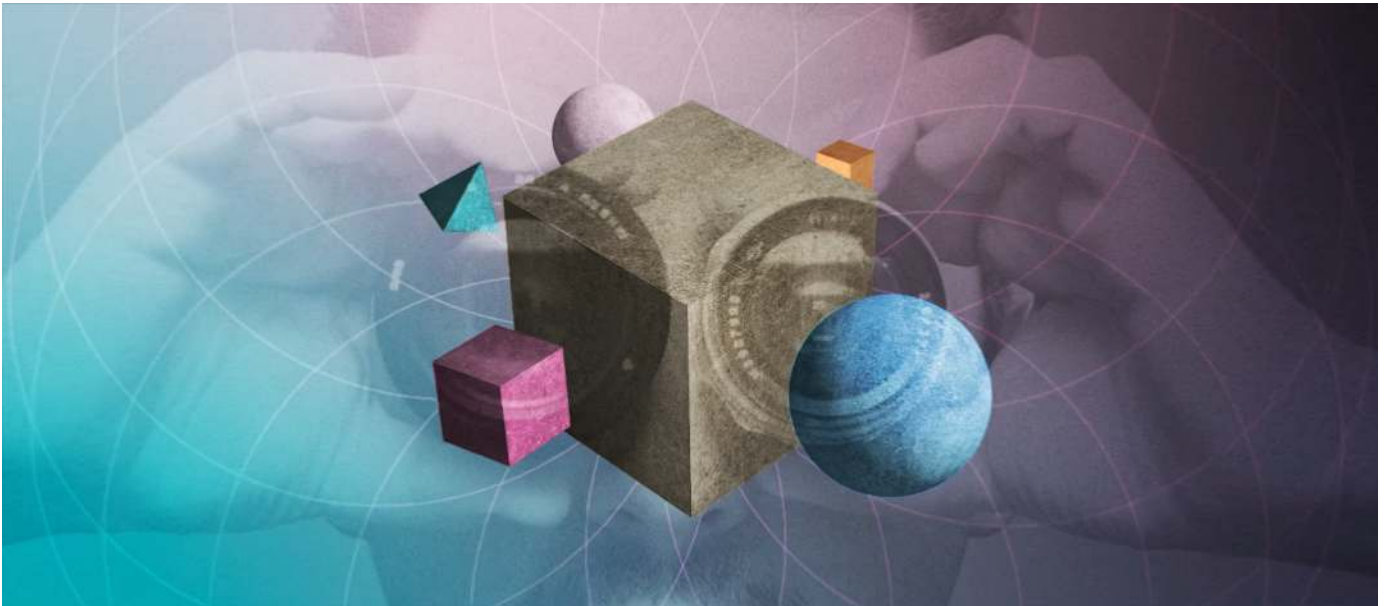
In terms of hardware, the discourse at the EU reduces economic dependencies by expanding domestic production capacities and developing strategic partnerships in procurement. The term "strategic autonomy," frequently used in EU institutions, illustrates that the core ambition is not mere protectionism or even autarky. Rather, it is to create fallback options and choices, at least for essential hardware components. With the European Chip Act, the EU has launched some of the most extensive economic support programs of its digital policy. The Act entails investments in research and development as well as in production facilities within the EU [116]. This strengthens the competitiveness of European providers in this market and ensures the reduction of economic dependencies [9].



EU Commissioner for Internal Market and Industrial Policy Thierry Breton announced massive investment in the European semiconductor industry in 2022. (European Union, 2022)

European Union, 2022

[View source](#) ↗



OUTLOOK

Monopoly structures, surveillance, supply shortages, cyberattacks, disinformation—the challenges could hardly be more diverse. Under the umbrella of high-value-word “digital sovereignty”, they find common ground. They are linked by the fact that the interests and claims to power of different social groups clash in them and have to be negotiated politically. Digital sovereignty basically describes a tug-of-war between various players over sovereignty claims, dependency relationships, decision-making and creative leeway in the digital context. With a spectrum of economic, security and education policy measures, politicians are attempting to strengthen or restrict the scope of action of various players in a targeted manner. The political balancing of conflicting interests will have a decisive impact on the future design of our digital infrastructures.

However, it is difficult to assess to what extent individual measures actually lead to “greater digital sovereignty.” Thus far, there is no approach that makes digital sovereignty measurable in the breadth in which it is politically discussed. Consequently, it is also challenging to determine whether and how strongly individual measures influence digital sovereignty. Evidently, it would be advisable to think about measures at the European level—specifically when it comes to regulatory initiatives and economic promotion—since the EU, as a community, can set much stronger incentives than a government acting alone on a national level. Numerous projects and regulations at the EU level have already proven to be expedient and successful. Nevertheless, most digital policy regulatory measures are still relatively young; time will tell how enforceable and effective they ultimately are.

It is clear that strengthening digital sovereignty requires forward-looking planning and a certain amount of courage and self-assurance to shake up established structures and embark on new paths.

In-depth text

What does sovereignty mean? A historical excursion

In contrast to “digital sovereignty,” the concept of sovereignty is very old. Its interpretation has changed repeatedly over the centuries to reflect the political circumstances of the time.

Principle of territoriality

Initially, we find the term in the teachings of Jean Bodin. The French philosopher used it to describe the absolute authority of the sovereign (here, the French king). Bodin postulated in the late Middle Ages that the king had the highest and final authority *over his state territory*. The sovereign is legitimized neither by a special education nor by voting (free elections were still unthinkable in the 16th century). According to Bodin, a sovereign is not subject to any higher authority, receives his claim to power for life and can pass it on. “*The principle mark of sovereign majesty and absolute power*” consisted above all in the “*right to impose laws generally on all subjects regardless of their consent*” [19].

Social contract

In the mid-17th century, the English philosopher and mathematician Thomas Hobbes experienced massive political unrest as a child during the English Civil War between king and parliament. It was therefore hardly surprising that he described the natural state of mankind as a “behemoth”—a gruesome monster from the Old Testament. In the natural state, he claims, anarchy and chaos would reign among people. People would have to live in suspicion and in constant fear of dispossession and death. Hobbes was convinced that there could only be one remedy for this state of affairs: a “Leviathan.”

This mythological sea monster symbolizes a sovereign ruler whose punishments are even more terrifying than chaos. For fear of punishment, no one would dare to disobey the laws; peace and trust in order would return. Hobbes was thus the first to envision something like a social contract. The people would voluntarily give up their anarchic freedom to do as they pleased. They would surrender their freedom and self-determination to the sovereign in return for the guarantee that the sovereign would administer justice and enforce laws [20]

Enlightenment and the rule of law

Around a century later, the Age of Enlightenment began in Europe. Montesquieu, a French state theorist, and Jean-Jacques Rousseau, a Swiss scholar, were the ideal harbingers of the French Revolution. They supplemented the concept of sovereignty with aspects of the rule of law, not least to reduce the risk of a monarch becoming an arbitrary despot. In 1748, Montesquieu described various forms of government and explained the basic principles of democracy. These included the fact that in a democracy, the people possess sovereign power by expressing their will in elections [21].



Jean Bodin (16th century)
(François Stuerhelt, PD, via Wikimedia Commons)
[View source](#)



The wise ruler Leviathan defeats the chaos (1651)
(A. Bosse, PD-US, via Wikimedia Commons)
[View source](#)



Baron de Montesquieu, 1728
(PD-US, via Wikimedia Commons)
[View source](#)

Rousseau built on this idea. In 1762, he dared to put forward a thesis that was unheard of at the time: He called for a social contract. Sovereignty—indivisible and inalienable—was held by the people, not the ruler (he spoke of *popular sovereignty*). The people would give themselves a constitution and submit to it. Within the framework of a social contract, the people could delegate the exercise of the law to a ruler, but they would still enact the law and thus remain sovereign [22]. At the time, this principle was the theoretical justification for removing rulers from power by force in revolutions and it is still an integral part of democratic constitutions around the world today.



Jean-Jacques Rousseau, 1753
(PD-US, via Wikimedia Commons)

[View source](#) ↗

In-depth text

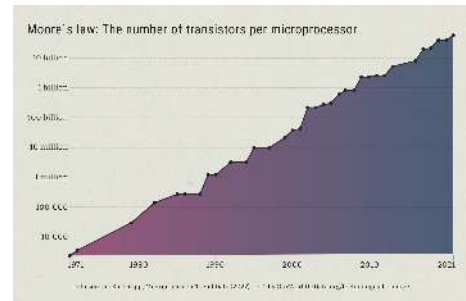
What is a microchip?

Microchips are built on a round plate of semiconductor material (“wafer”) that can be up to 30 centimeters in diameter but is no thicker than one millimeter. The special feature of semiconductor materials is that their electrical conductivity can be controlled in a very targeted manner [75]. For this reason, electronic circuits can be practically “drawn” onto a wafer.

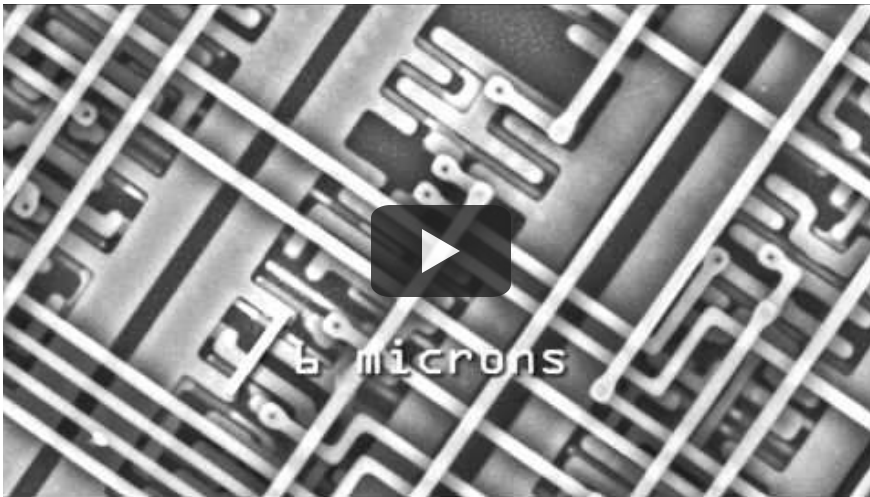
In layers, microscopic circuits are applied to the surface of the wafer by etching tiny areas of the wafer, exposing them to UV light or coating them with other materials. Layer by layer, gossamer three-dimensional structures are created through which electricity can be conducted. Tiny areas in this structure can now be specifically set to the state of “conductive” or “non-conductive.” They are called transistors, and their state corresponds to 1 or 0 in the binary system. When several transistors are connected together, circuits are created that can be used to store data and process commands.

In theory, a transistor only needs to be a few *atoms* wide to function, but the challenge is to technically realize such orders of magnitude. The more transistors are placed on a chip, the more powerful and energy-efficient it is in the end. The chip industry has seen unprecedented progress in this area. Since 1970, the number of transistors on a microchip has doubled every 2 years [76]. One of the most powerful chips currently available accommodates a total of 250 million transistors on an area of 1mm². Here, the smallest applied structures are only a few nanometers wide [77].

It is only with a scanning electron microscope that one can get a realistic picture of the magnitudes of nanotechnology, as shown here in a video with close-ups of the fascinating inner workings of a microchip of roughly 3mm² in size [78].



Moore's Law: Since 1970, the number of transistors per microchip has doubled every two years



In-depth text

Mass surveillance and espionage: The revelations of the NSA Affair

The political explosiveness and the sheer extent of the documents leaked by Edward Snowden was unprecedented. It was a trove of around 17 million classified documents, some of them top secret [44]. They provided evidence of a whole series of intelligence operations through which global data traffic was systematically recorded, stored and analyzed.

Who authorized the NSA to eavesdrop on the whole world?

After the terrorist attacks on the World Trade Center in 2001, the surveillance of digital communication by American security agencies was massively expanded. In particular, the CIA and NSA were scaled up in terms of personnel and equipped with unprecedented budgets. Their declared aim was to identify and monitor terrorist networks and suspicious individuals [45]. Just a few weeks after the attacks, the George W. Bush administration passed the Patriot Act, a law that was uncritically approved by the House of Representatives and the U.S. Senate within just three days. The Patriot Act provided for a drastic restriction of American civil rights and simplified the conditions under which surveillance or searches of persons at home and abroad could be ordered. Last but not least, the Act obliged American companies to grant security authorities access to their servers without the need for a court order. The Patriot Act also granted such access rights to the data of foreign subsidiaries of U.S. companies, even if local legislation in other countries would actually prohibit such disclosure. The FISA Amendments Act of 2008 made surveillance even easier. An issues paper of the European Parliament concludes that in the operational practice of US authorities there is probably no restriction on the intrusion into the privacy of non-US persons [46].

The surveillance programs

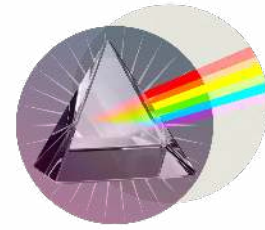
Here you get an insight into just some of the NSA surveillance programs made public by Edward Snowden:

“All data useful to U.S. foreign policy is considered, including explicitly political surveillance of ordinary and lawful democratic activities.”

European Parliament | Directorate-General for Internal Policies of the Union, 2013

PRISM

The PRISM program was designed to systematically collect communications data. User data was recorded directly from the servers of cooperating companies, some of which, according to reports in The Washington Post, were paid to do so [47]. According to the documents, Microsoft, Google, Facebook, Skype, Apple, YouTube, AOL and Paltalk granted the NSA real-time access to all emails, chat histories, videos, photos, audio files, files, data transfers and video conferences of their users. In addition, the intelligence services received personal account data and could reportedly be notified immediately when a target logged in [48].



XKEYSCORE

XKeyscore was considered one of the most far-reaching analysis softwares for information retrieval and data enrichment in the intelligence environment. A presentation by the NSA shows that it could be used in a similar way to a search engine. By entering a unique identifier, such as an e-mail address or IP address, all available data on a target person could be viewed and searched in real time. The available material contained an almost unlimited variety of information, from calls made, email histories, chat logs, messages and activities on social networks to browser histories and search terms entered [49]. The NSA argued that such queries were only used to protect national security and were only accessible to authorized personnel who were subject to regular checks [49]. However, Snowden himself emphasized that the analysts approved for the tool could intercept anyone in the world, at any time, in real time, as long as they had their email address [50]. A purchase agreement [51] between the NSA and the German Federal Intelligence Service and Federal Office for the Protection of the Constitution later confirmed what had previously been denied: German authorities also had access to XKeyscore from April 2013. According to the contract, the user agreement was accompanied by extensive promises to exchange data with U.S. authorities.



BULLRUN

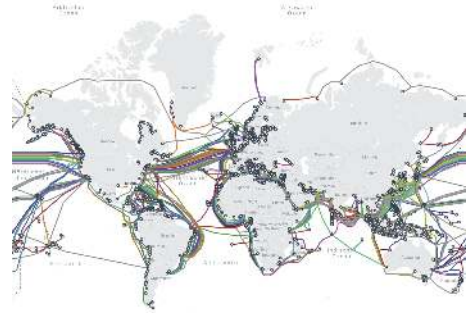
The program Bullrun [46] aimed to break encryption technologies in order to read encrypted communications. Various methods were used in parallel: among other things, it is suspected that the NSA cooperated with providers of IT security products, infiltrated technical committees and influenced them to adopt insecure encryption standards. The systematic installation of “backdoors” in encryption systems is also assumed. Backdoors are deliberate technical vulnerabilities that make systems easier to attack. Their installation may also have been enforced by means of a court order [46].



TEMPORA/UPSTREAM

The Tempora [52] and Upstream [46] programs involved the collection of large amounts of data by tapping directly into undersea fiber optic cables and internet nodes. The mass collection and storage of data was carried out without cause or suspicion. The declared aim of the Tempora program was nothing less than collecting “as much online and telephone traffic as possible” [52]. Vast amounts of data traffic were siphoned off, filtered, stored and analyzed using over 70,000 keywords. Subsequently, content such as recordings of phone calls, emails and metadata were analyzed by secret service employees [53].

In a speech at the Chaos Communications Congress 2019, Rainer Rehak, researcher at the Weizenbaum Institute, recapped Snowden's revelations.



Worldwide network of undersea fiber optic cables

TeleGeography, 2024

[View source](#) ↗



Glossary

open source software - Open source means that the source code on which a software is based can be viewed and modified.

security and resilience - Cyber security means preventing attacks on digital infrastructures from happening in the first place; cyber resilience means being able to "bounce back" quickly and in a coordinated manner in the event of an attack.

Colonial Pipelines - One of the largest oil pipeline systems in the USA, which was shut down for several days in 2021 due to a ransomware attack by Russian hackers.

semiconductors - Semiconductors are materials such as silicon or germanium whose electric conductivity can be precisely controlled

Five Eyes - An established intelligence alliance between the US, UK, New Zealand, Australia, and Canada.

Cambridge Analytica scandal - The British political consulting firm obtained the profile data of millions of Facebook users via controversial channels and used it to calculate individual psychometric profiles (such as personality types) [39]. The buyers of this profile data in 2016 included the Republican U.S. Senator Ted Cruz and the then presidential candidate Donald Trump, whose campaign teams allegedly used the profiles for tailored, individualized election advertising [40].

disinformation - False or misleading information that is deliberately and intentionally disseminated to cause public harm.

References


- [1] "A.-L. Schlitt, dpa, and AFP, „Olaf Scholz: "Wir müssen unsere digitale Souveränität stärken", Die Zeit, Hamburg, June 9, 2022. (German only)" <https://www.zeit.de/politik/deutschland/2022-06/republica-bundeskanzler-olaf-scholz-digital-zeitenwende>
- [2] "E. Macron and N. Zennström, „Il est temps pour l'Europe d'avoir sa propre souveraineté technologique !", ÉLYSÉE, Paris, December 9, 2020. (French only)" <https://www.elysee.fr/emmanuel-macron/2020/12/09/il-est-temps-pour-leurope-davoir-sa-propre-souverainete-technologique>
- [3] "E. Felder, „Anmassung in der politischen Sprache - Nicht nur ein Merkmal sogenannter populisten", Sprachreport, issue 2, 2017. (German only)" <https://pub.ids-mannheim.de/laufend/sprachreport/pdf/sr17-2.pdf>
- [4] "G. Falkner, S. Heidebrecht, A. Obendiek and T. Seidl (2024), "Digital sovereignty—Rhetoric and reality", Journal of European Public Policy, 31(8), pp. 1–22." <https://doi.org/10.1080/13501763.2024.2358984>
- [5] "J. Pohle and T. Thiel, „Digital sovereignty", Internet Policy Review, 9(4), 2020." <https://policyreview.info/concepts/digital-sovereignty>
- [6] "S. Couture and S. Toupin, „What does the notion of "sovereignty" mean when referring to the digital?", New Media and Society, 21(10), pp. 2305–2322, 2019." <https://journals.sagepub.com/doi/abs/10.1177/1461444819865984>
- [7] "H. Kagermann, K.-H. Streibich, and K. Suder, „Digital Sovereignty - Status Quo and Perspectives", National Academy of Science and Engineering, 2021." <https://en.acatech.de/publication/digital-sovereignty/download-pdf?lang=en/>
- [8] "A. Chander and H. Sun, „Sovereignty 2.0", Vanderbilt Journal of Transnational Law, 55(2), pp. 283–324, 2022." <https://scholarship.law.vanderbilt.edu/vjtl/vol55/iss2/2/>
- [9] | "R. M. Kar and B. E. P. Thapa, „Digitale Souveränität als strategische Autonomie", Kompetenzzentrum Öffentliche IT, 2020. (German only)" <https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t+als+strategische+Autonomie++Umgang+mit+Abh%C3%A4ngigkeiten+im+digitalen+Staat>
- [10] "X. Jin, B. W. Wah, X. Cheng, and Y. Wang, „Significance and challenges of big data research", Big data research, 2(2), pp. 59–64, 2015." <https://www.sciencedirect.com/science/article/abs/pii/S2214579615000076>
- [11] "L. Floridi, „The Fight for Digital Sovereignty", Philosophy and Technology, 33(3), pp. 369–378, 2020." <https://link.springer.com/article/10.1007/s13347-020-00423-6>
- [12] "R. A. Pinto, „Digital sovereignty or digital colonialism?", Sur - International Journal on Human Rights, 15(27), S. 15–27, 2018." <https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/>
- [13] "IT Planning Council, „Stärkung der digitalen Souveränität der öffentlichen Verwaltung. Eckpunkte – Ziele und Handlungsfelder", 2020. (German only)" https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-losungen/eckpunktpapier-digitale-souveranitaet.pdf?__blob=publicationFile&v=2
- [14] "German Science and Humanities Council, „Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum", Cologne, 2023. (German only)" https://www.wissenschaftsrat.de/download/2023/1580-23.pdf?__blob=publicationFile&v=11
- [15] "BMWi (Federal Ministry for Economic Affairs and Energy), „Schwerpunktstudie Digitale Souveränität", 2021. (German only)" <https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.html>
- [16] "B. Herlo, A. Ullrich, and G. Vladova, „Sustainable Digital Sovereignty: Interdependencies Between Sustainable Digitalization and Digital Sovereignty", Weizenbaum Institute for the Networked Society, Berlin, Working Paper 32, 2023." <https://www.ssoar.info/ssoar/handle/document/86849>
- [17] "Federal Foreign Office, „German Government's fourteenth Human Rights Report", 2020." <https://www.auswaertiges-amt.de/blob/2422644/3f981cf30f610babfd16d0eb63ee542c/201202-mrb-14-download-data.pdf>
- [18] "United Nations, „Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations", 1970." https://treaties.un.org/doc/source/docs/A_RES_2625-Eng.pdf
- [19] "J. Bodin, The six Books of the Republic, Vol. I–III, p.222, Munich: Beck, 1981."
- [20] "T. Hobbes and M. Dießelhorst, Leviathan: First and second part, bibliographically supplemented edition 2018, [reprint] 2023. Ditzingen: Reclam, 2018."
- [21] "C. L. de S. de Montesquieu, The Spirit of Law, bibliographically supplemented edition 2011 [reprint] 2023. Ditzingen: Reclam, 2011."
- [22] "J.-J. Rousseau, H. Brockard, and E. Pietzcker, The Social Contract, bibliographically supplemented edition 2020, [reprint] 2023. Ditzingen: Reclam, 2020."
- [23] "D. R. Johnson and D. Post, „Law and Borders: The Rise of Law in Cyberspace", Stanford Law Review, 48(5), pp. 1367–1402, 1996." <http://firstmonday.org/ojs/index.php/fm/article/download/468/824>
- [24] "J. Hofmann, „Multi-stakeholderism in Internet governance: putting a fiction into practice", Journal of Cyber Policy, 1(1), pp. 29–49, 2016" <https://www.tandfonline.com/doi/full/10.1080/23738871.2016.1158303>
- [25] "W. Hoxtell and D. Nonhoff, „Internet Governance: Past, Present and Future", Konrad-Adenauer-Stiftung e.V., 2019." <https://www.kas.de/de/einzeltitel/-/content/internet-governance-past-present-and-future>
- [26] "C. M. Glen, „Internet Governance: Territorializing Cyberspace?", Politics & Policy, 42(5), pp. 635–657, 2014." <https://onlinelibrary.wiley.com/doi/abs/10.1111/polp.12093>
- [27] "J. Pohle and T. Thiel, „Digitale Souveränität - Von der Karriere eines einenden und doch problematischen Konzepts", in Der Wert der Digitalisierung: Gemeinwohl in der digitalen Welt, C. Piallat, Hrsg., Bielefeld: transcript Verlag, 2021, pp. 319–340. (German only)" <https://www.econstor.eu/bitstream/10419/241996/1/Full-text-chapter-Pohle-et-al-Digitale-Souveranitaet.pdf>
- [28] "J. Zittrain, The Future of the Internet-And How to Stop It. New Haven & London: Yale University Press & Penguin UK, 2008." https://dash.harvard.edu/bitstream/handle/1/4455262/Zittrain_Future of the Internet.pdf
- [29] "T. Berners-Lee, „Long live the web", Scientific American, 303(6), pp. 80–85, 2010." <https://www.scientificamerican.com/article/long-live-the-web/>

- [30] "T. Bendig, P. Ganten, P. Krosta-Hartl, R. Neuburger, T. Schauf, „Manifesto for Digital Sovereignty“, Open Source Business Alliance - Bundesverband für digitale Souveränität e. V., 2021." <https://osb-alliance.de/wp-content/uploads/2022/06/Manifesto-for-Digital-Sovereignty-1.pdf>
- [31] "M. Mayer und Y.-C. Lu, „Illusionen der Autonomie? Europas Position in den globalen digitalen Abhängigkeitsstrukturen“, SIRIUS – Zeitschrift für Strategische Analysen, 7(4), pp. 390–410, 2023. (German only)" <https://www.degruyter.com/document/doi/10.1515/sirius-2023-4005/html>
- [32] "J. Hofmann, „Digitale Kommunikationsinfrastrukturen“, in Handbuch Digitalisierung in Staat und Verwaltung, T. Klenk, F. Nullmeier, G. Wewer, Hrsg., Wiesbaden: Springer VS, 2020, pp.147-157. (German only)" <https://link.springer.com/book/10.1007/978-3-658-23668-7#bibliographic-information>
- [33] "U. Dolata, „Internet – Platforms – Regulation: Coordination of Markets and Curation of Sociality“. SOI Discussion Paper 2020-02, 2020." https://www.sowi.uni-stuttgart.de/dokumente/forschung/soi/soi_2020_2_Dolata.Internet.Platforms.Regulation.pdf
- [34] "C. G. Katz, „One Map to Rule Them All: Google Maps and Quasi-Sovereign Power in International Legal Disputes“, Hastings Science and Technology Law Journal, 14(1) p. 67, 2023." https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1121&context=hastings_science_technology_law_journal
- [35] "ZEIT Online, „Android: Google setzt Geschäftsbeziehungen zu Huawei aus“, Die Zeit, Hamburg, 20. Mai 2019. (German only)" <https://www.zeit.de/digital/2019-05/android-update-huawei-lizenz-google-alphabet-usa>
- [36] "BMWi (Federal Ministry for Economic Affairs and Energy) and Digital Summit Focus Group „Digital Sovereignty“, „Digitale Souveränität im Kontext plattformbasierter Ökosysteme“, Report, 2019. (German only)" https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/p2-digitale-souveraenitaet-plattformbasierter-oekosysteme.pdf?__blob=publicationFile&v=4
- [37] "C. Tsalikis, „Shoshana Zuboff on the Undetectable, Indecipherable World of Surveillance Capitalism“, Centre for International Governance Innovation, 2019." <https://www.cigionline.org/articles/shoshana-zuboff-undetectable-indecipherable-world-surveillance-capitalism/>
- [38] "S. Zuboff, „Big other: Surveillance Capitalism and the Prospects of an Information Civilization“, Journal of Information Technology, 30(1), pp. 75–89, 2015." <https://journals.sagepub.com/doi/epdf/10.1057/jit.2015.5>
- [39] "C. Cadwalladr and E. Graham-Harrison, „How Cambridge Analytica turned Facebook ‚likes‘ into a lucrative political tool“, The Guardian, March 17, 2018." <https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm>
- [40] "P. Lewis and P. Hilder, „Leaked: Cambridge Analytica's blueprint for Trump victory“, The Guardian, March 23, 2018." <https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory>
- [41] "C. Fuchs and D. Trottier, „Towards a theoretical model of social media surveillance in contemporary society“, Communications, 40 (1), pp. 113-135, 2015." <https://westminsterresearch.westminster.ac.uk/item/96vw5/towards-a-theoretical-model-of-social-media-surveillance-in-contemporary-society>
- [42] "G. Goldacker, „Digitale Souveränität“, Kompetenzzentrum Öffentliche IT, Report, 2017. (German only)" <https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souveränität>
- [43] „Schrems I“ - Opinion of Advocate General Yves Bot. Case C-362/14 Maximilian Schrems v. Data Protection Commissioner, 2015." <https://curia.europa.eu/juris/document/document.jsf?jsessionid=BBBF0523A2E66910286E86768266614E?text=&docid=168421&pageIndex=0&doclang=EN>
- [44] "D. E. Sanger and E. Schmitt, „Snowden Used Low-Cost Tool to Best N.S.A.“, The New York Times, February 8, 2014." <https://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html>
- [45] "B. Gellmann and G. Miller, „Black budget' summary details U.S. spy network's successes, failures and objectives“, Washington Post, August 29, 2013." https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_print.html
- [46] "C. Bowden, „The US surveillance programmes and their impact on EU citizens' fundamental rights“, European Parliament, PE 474.405, 2013." [https://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT\(2013\)474405_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf)
- [47] "C. Timberg and B. Gellman, „NSA paying U.S. companies for access to communications networks“, Washington Post, Mai 17, 2023." https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html
- [48] "M. Kremp, K. Lischka, and O. Reißmann, „Projekt Prism: NSA spioniert weltweit Internet-Nutzer aus“, Der Spiegel, June 7, 2013. (German only)" <https://www.spiegel.de/netzwelt/netzpolitik/projekt-prism-nsa-spioniert-weltweit-internet-nutzer-aus-a-904330.html>
- [49] "G. Greenwald, „XKeyscore: NSA tool collects ‚nearly everything a user does on the internet‘“, The Guardian, July 31, 2013." <https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>
- [50] "L. Poitras and G. Greenwald, „NSA whistleblower Edward Snowden: ‚I don't want to live in a society that does these sort of things‘ – video“, The Guardian, June 9, 2013." <http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video>
- [51] "ZEIT Online, „NSA hilft Verfassungsschutz: XKeyscore – das Dokument“, Die Zeit, Hamburg, August 26, 2015. (German only)" <https://www.zeit.de/digital/datenschutz/2015-08/xks-xkeyscore-vertrag>
- [52] "E. MacAskill, J. Borger, N. Hopkins, N. Davies, and J. Ball, „GCHQ taps fibre-optic cables for secret access to world's communications“, The Guardian, June 21, 2013." <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>
- [53] „Abhörskandal: Auch britischer Geheimdienst späht Daten aus“, Handelsblatt, June 22, 2013. (German only)" <https://www.handelsblatt.com/politik/international/abhoerskandal-auch-britischer-geheimdienst-spaht-daten-aus/8391120.html>
- [54] "G. Schmid, „Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)“, European Parliament, Temporary Committee on the ECHELON Interception System, July 11, 2001." https://www.europarl.europa.eu/compa/temppcom/echelon/pdf/rapport_echelon_en.pdf
- [55] "B. Bode and P. Heinacher, „Wirtschaftsspionage / Volkswagen ist kein Einzelfall. Sicherheit muss künftig zur Chefsache erklärt werden.“, Handelsblatt, p. 21, August 29, 1996. (German only)"
- [56] "A. Kreye, „Aktenkrieger“, Süddeutsche Zeitung, p. 19, March 29, 2001. (German only)"

- [57] "W. Drozdiak, „French Resent U.S. Coups in New Espionage", The Washington Post, Washington, D.C., pp. A1, A26, February 26, 1995."
- [58] "D. Ruschmann and T. Katzensteiner, „Spionage Antennen gedreht", Wirtschaftswoche, p.62, November 9, 2000. (German only)"
- [59] "S. Shane, „Documents Show N.S.A. Efforts to Spy on Both Enemies and Allies", The New York Times, November 3, 2013." <https://www.nytimes.com/interactive/2013/11/03/world/documents-show-nsa-efforts-to-spy-on-both-enemies-and-allies.html>
- [60] "J. Ball, „NSA monitored calls of 35 world leaders after US official handed over contacts", The Guardian, October 25, 2013." <https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>
- [61] "„NSA hörte Zentrale der Vereinte Nationen in New York ab", Der Spiegel, August 25, 2013. (German only)" <https://www.spiegel.de/politik/ausland/nsa-hoerte-zentrale-der-vereinte-nationen-in-new-york-ab-a-918421.html>
- [62] "L. Poitras, M. Rosenbach, and H. Stark, „Secret NSA Documents Show How the US Spies on Europe and the UN", Der Spiegel, August 26, 2013." <https://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html>
- [63] "„Belgacom: Geheimdienst GCHQ hackte belgische Telefongesellschaft", Der Spiegel, September 20, 2013. (German only)" <https://www.spiegel.de/netzwelt/web/belgacom-geheimdienst-gchq-hackte-belgische-telefongesellschaft-a-923224.html>
- [64] "Ministry of Foreign Affairs of the PRC, „Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference", Wuzhen, 2015." https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html
- [65] "The Internet Society, „Navigating Digital Sovereignty and its Impact on the Internet", 2022." <https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf>
- [66] "A. Chander and U. P. Lê, „Data nationalism", Emory Law Journal, 64(3), p. 677, 2015." <https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2/>
- [67] "S. Budnitsky and L. Jia, „Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance", European Journal of Cultural Studies, 21(5), pp. 594–613, 2018." <https://doi.org/10.1177/1367549417751151>
- [68] "G. Fung, „China Ramps Up Control of Domain Names, Adds New Layer to Great Firewall", Radio Free Asia, January 16, 2017." <https://www.rfa.org/english/news/china/internet-domain-01162017155356.html>
- [69] "T. Thiel, „Die Schönheit der Chance: Utopien und das Internet", Juridikum : Zeitschrift für Kritik, Recht, Gesellschaft, 15(4), pp. 459–471, 2014. (German only)"
- [70] "J. Seiffert, „Schengen Internet routing", Deutsche Welle, February 20, 2014." <https://www.dw.com/en/weighing-a-schengen-zone-for-europes-internet-data/a-17443482>
- [71] "N. Haase, „Merkel's European internet", Deutsche Welle, February 17, 2014." <https://www.dw.com/en/i-expect-merkels-actions-to-follow-her-words/a-17438783>
- [72] "J.-P. Kleinhans, „Schengen-Routing, DE-CIX und die Bedenken der Balkanisierung des Internets", netzpolitik.org, November 13, 2013. (German only)" <https://netzpolitik.org/2013/schengen-routing-de-cix-und-die-bedenken-der-balkanisierung-des-internets/>
- [73] "A. Braud, G. Fromentoux, B. Radier, and O. Le Grand, „The Road to European Digital Sovereignty with Gaia-X and IDSA", IEEE Network, 35(2), pp. 4–5, 2021." <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9387709>
- [74] "A. Barrinha and G. Christou, „Speaking sovereignty", European Security, 31(3), pp. 356–376, 2022." <https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2102895>
- [75] "M. Sander, R. Fulterer and G. da Silva, „Halbleiter und Chips - wie sie funktionieren und warum sie systemrelevant sind", Neue Zürcher Zeitung, August 3, 2022. (German only)" <https://www.nzz.ch/technologie/halbleiter-und-chips-wie-sie-funktionieren-und-warum-sie-systemrelevant-sind-ld.1602073>
- [76] "Moore's law: The number of transistors per microprocessor" <https://ourworldindata.org/grapher/transistors-per-microprocessor>
- [77] "T. Költzsch, „Apple: iPhone 15 Pro kommt mit 3-nm-SoC und ohne Schieberegister", golem.de, September 12, 2023. (German only)" <https://www.golem.de/news/apple-iphone-15-pro-kommt-mit-3-nm-soc-und-ohne-schieberegister-2309-177601.html>
- [78] "Nanoscale Informal Science Education Network (NISE), „Zoom into a Microchip video", NISE Network", 2013." https://www.nisenet.org/catalog/weizenbaum/zoom_microchip_video
- [79] "C. Miller, Chip war: the fight for the world's most critical technology. London New York Sydney Toronto New Delhi: Simon & Schuster, 2022."
- [80] "BMI (Federal Ministry of the Interior, Building and Community), „Cyber Security Strategy for Germany 2021", August 2021." https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf?__blob=publicationFile&v=5
- [81] "BSI (Federal Office for Information Security), „The State of IT Security in Germany in 2023", November 2, 2023." https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2023.pdf?__blob=publicationFile&v=9
- [82] "European Commission, Directorate-General for Communications Networks, Content and Technology, „Digital Services Act: Application of the risk management framework to Russian disinformation campaigns", Brussels, 2023." <https://op.europa.eu/en/publication-detail/-/publication/c1d645d0-42f5-11ee-a8b8-01aa75ed71a1/language-en>
- [83] "M. Kachelmann and W. Reiners, „The European Union's governance approach to tackling disinformation – protection of democracy, foreign influence, and the quest for digital sovereignty", L'Europe en Formation, 396(1), 2023, pp. 11-36." <https://dx.doi.org/10.3917/eufor.396.0011>
- [84] "H. Roberts, J. Cows, F. Casolari, J. Morley, M. Taddeo, and L. Floridi, „Safeguarding european values with digital sovereignty", Internet Policy Review, 10(3), 2021." <https://policyreview.info/articles/analysis/safeguarding-european-values-digital-sovereignty-analysis-statements-and-policies>
- [85] "E. Gräf, H. Lahmann, and P. Otto, „Die Stärkung der digitalen Souveränität - Wege der Annäherung an ein Ideal im Wandel", Diskussionspapier von iRights.Lab, Deutsches Institut für Sicherheit und Vertrauen im Internet - DIVISI, 2018. (German only)" <https://www.divisi.de/wp-content/uploads/2018/05/DIVISI-Themenpapier-Digitale-Souveraenitaet.pdf>
- [86] "European Commission, „Europe fit for the Digital Age: Artificial Intelligence", Brussels, 2021." https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682
- [87] "A. Bradford, The Brussels Effect: How the European Union Rules the World, Oxford University Press, 2020."

- [88] "European Commission, „Proposal for a DECISION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the 2030 Policy Programme "Path to the Digital Decade", 2021/0293 (COD), Brussels, 2021." <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0574>
- [89] "European Commission, „European Declaration on Digital Rights and Principles for the Digital Decade", Brussels, January 26, 2022." <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0028>
- [90] "M. J. Sá, A. I. Santos, S. Serpa, and C. M. Ferreira, „Digitainability—Digital competences post-COVID-19 for a sustainable society", *Sustainability*, 13(17), S. 9564, 2021." <https://doi.org/10.3390/su13179564>
- [91] "M. Mertz, M. Jannes, A. Schlomann, E. Manderscheid, C. Rietz, and C. Woopen, „Digitale Selbstbestimmung", Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres), Cologne, 2016. (German only)" https://kups.ub.uni-koeln.de/6891/1/ceres_Digitale_Selbstbestimmung.pdf
- [92] "BMBF (Federal Ministry of Education and Research), „Initiative Digitale Bildung", 2021. (German only)" https://www.bildung-forschung.digital/digitalezukunft/de/bildung/initiative-digitale-bildung/initiative-digitale-bildung_node.html
- [93] "BMI (Federal Ministry of the Interior and Community), „Digitalführerschein", 2023. (German only)" <https://difue.de/>
- [94] "N. D. Wright, „Artificial Intelligence and Democratic Norms: Meeting the Authoritarian Challenge", Sharp Power and Democratic Resilience Series, 2020." <https://www.ned.org/wp-content/uploads/2020/07/Artificial-Intelligence-Democratic-Norms-Meeting-Authoritarian-Challenge-Wright.pdf>
- [95] "J. Rone, „The return of the state? Power and legitimacy challenges to the EU's regulation of online disinformation", in *Power and authority in internet governance*, B. Haggart, N. Tushikov, J. A. Scholte (Eds.), London: Routledge, 2021, pp. 171–194."
- [96] "Superr Lab SL gGmbH, „Vier Forderungen für eine digital-souveräne Gesellschaft", 2021. (German only)" <https://digitalezivilgesellschaft.org/>
- [97] "European Commission, „Towards a more resilient, competitive and sustainable Europe", Brussels, 2023." <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0558&qid=1726478852722>
- [99] "G. Baldini, a.o., „Cybersecurity, our digital anchor", EUR 30276 EN, Publications Office of the European Union, Luxemburg, 2020." <https://publications.jrc.ec.europa.eu/repository/handle/JRC121051>
- [100] "European Commission, „New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient", Brussels, 2020." https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391
- [101] "K. Fritzsche, J. Pohle, S. Bauer, F. Haenel, and F. Eichbaum, „Digitalisierung nachhaltig und souverän gestalten", CODINA position paper, 2022. (German only)" https://codina-transformation.de/wp-content/uploads/CODINA_Positionspapier_Digitale-Souveränität.pdf
- [102] "D. Lambach and K. Oppermann, „Narratives of digital sovereignty in German political discourse", *Governance*, 36(3), 2023, pp. 293-709." <https://onlinelibrary.wiley.com/doi/full/10.1111/gove.12690>
- [103] "F. Steiner and V. Grzymek, „Digital Sovereignty in the EU", Bertelsmann Stiftung, 2020." https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Digital_Sovereignty_in_the_EU_Policy_Brief_BSt_EZ_European_Public_Goods_EN.pdf
- [104] "T. Madiaga, „Digital sovereignty for Europe", EPRS | European Parliamentary Research Service, PE 651.99, 2020." [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)
- [105] "European Commission, „A European strategy for data", Brussels, 2020." <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&qid=1726479175852>
- [106] "European Commission, „Shaping Europe's digital future", Brussels, 2019." https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en
- [107] "A. Blankertz, „Öffentliches Geld – Öffentliches Gut!: Wem sollen Daten nützen?", *netzpolitik.org*, 2020. (German only)" <https://netzpolitik.org/2022/oeffentliches-geld-oeffentliches-gut-wem-sollen-daten-nuetzen/>
- [108] "European Commission, „Data Governance Act explained | Shaping Europe's digital future", Brussels, 2024." <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained>
- [109] "C. Wölbelt, J. Bager, „Amerikanische Anbieter dürfen bei EU-Cloud Gaia-X mitmachen", *c't Magazin*, December 7, 2020. (German only)" <https://www.heise.de/news/Amerikanische-Anbieter-duerfen-bei-EU-Cloud-Gaia-X-mitmachen-4974504.html>
- [110] "C. Wölbelt, „Ich erwarte nicht, dass Gaia-X liefert, was wir brauchen": Yann Lechelle, CEO des Cloud-Anbieters Scaleway, im c't-Interview über Gaia-X", *c't*, 2022, No. 1, Heise, pp. 14–16, December 17, 2021. (German only)" <https://www.heise.de/news/Scaleway-Chef-Ich-erwarte-nicht-dass-Gaia-X-liefert-was-wir-brauchen-6292424.html>
- [111] "BMI (Federal Ministry of the Interior and Community), „Zentrum für Digitale Souveränität der öffentlichen Verwaltung", n.d. (German only)" <https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/zentrum-fuer-digitale-souveraenitaet/zentrum-fuer-digitale-souveraenitaet-node.html#facets-18094072>
- [112] "European Commission, „The Digital Services Act", Brussels, n.d." https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en
- [113] "European Commission, „The Digital Markets Act: ensuring fair and open digital markets", Brussels, n.d." https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en
- [114] "BMFSJ (Federal Ministry for Family Affairs, Senior Citizens, Women and Youth), „Achter Altersbericht - Ältere Menschen und Digitalisierung", 2020. (German only)" <https://www.bmfsfj.de/resource/blob/159916/9f488c2a406ccc42cb1a694944230c96/achter-altersbericht-bundestagsdrucksache-data.pdf>
- [115] "Federal Government, „Gigabitstrategie der Bundesregierung", 2023. (German only)" <https://www.bundesregierung.de/breg-de/themen/digitalisierung/gigabitstrategie-2017464>
- [116] "European Commission, „European Chips Act", Brussels, n.d." https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en

Digital Sovereignty

 Dr. Esther Görnemann

Weizenbaum Institute

<https://orcid.org/0000-0003-3958-2493>

Version  6/25/2024

Deutsch 

Contact

Dr. Esther Görnemann. esther.goernemann@weizenbaum-institut.de

Copyright note

The texts on this page are licensed under the Creative Commons License "Attribution-NonCommercial 4.0 International" (CC BY NC Open link). If you intend to make commercial use, please contact us.

CC BY NC

Conceptualization, design, development

Atelier Hurra - Conceptualization, design
[Webseite](#)

MADEFUL® GmbH - Projectmanagement, conceptualization, design
[Webseite](#)

Uninspired Studio - Development, conceptualization, design
[Webseite](#)

Image credits

Chapter 1.1 Technology layers, (own design, CC-BY-NC)

Chapter 1.1 Technology layers, (own design, CC-BY-NC)

Chapter 1.2 The General Assembly in Session (United Nations, PD-US-no notice-UN, via Wikimedia Commons)
[Wikimedia Commons](#)

In-depth text "What is sovereignty" - Bodin (François Stuerhelt, PD, via Wikimedia Commons)
[Wikimedia Commons](#)

In-depth text "What is sovereignty" - Leviathan (A.Bosse, PD-US, via Wikimedia Commons)
[Wikimedia Commons](#)

In-depth text "What is sovereignty" - Montesquieu (PD-US, via Wikimedia Commons)
[Wikimedia Commons](#)

In-depth text "What is sovereignty" - Rousseau (M.-Q. de La Tour, PD-US, via Wikimedia Commons)
[Wikimedia Commons](#)

Chapter 2.1 John Perry Barlow, Internet pioneer (own design, CC-BY-NC)

Chapter 2.2 Apple II, 1977 (own design, CC-BY-NC)

Chapter 2.2 iPhone, 2007 (own design, CC-BY-NC)

Chapter 2.3 illustration tech companies' revenues (own design, CC-BY-NC, Data source: Wirtschaftswoche 2022, via wiwo.de)
wiwo.de

Chapter 2.4 Chapter header "The NSA affair" (own design, CC-BY-NC)

In-depth text "The NSA affair" - X-Keyscore (US National Security Agency, PD-USGov, via Wikimedia Commons)
Wikimedia Commons

In-depth text "The NSA affair" – Worldwide network of submarine fiber-optic cables (©TeleGeography 2024, via submarinecablemap.com)
submarinecablemap.com

Chapter 2.5 Chapter header "The splinternet" (own design, CC-BY-NC)

Chapter 2.5 Prof. Dr. Thorsten Thiel (© 2024 Weizenbaum-Institut e.V.)

Chapter 2.7 Global cyber attacks in realtime (© 2024 AO Kaspersky Lab, via cybermap)
cybermap

Chapter 3.2 Technical proficiency (own design, CC-BY-NC)

Chapter 3.2 IT security (own design., CC-BY-NC)

Chapter 3.2 Impact assessment (own design., CC-BY-NC)

Chapter 3.2 EU Cyber Security Strategy (© 2013 European Union, via EC Audiovisual Service)
EC Audiovisual Service

Chapter 3.3 Chapter header data layer (own design., CC-BY-NC)

Chapter 3.4 Chapter header code layer (own design., CC-BY-NC)

Chapter 3.5 Chapter header physical layer (own design., CC-BY-NC)

Animated illustrations: own design, CC-BY-NC

Chapter 2.3 Prof. Dr. Jeanette Hofmann (© 2024 Weizenbaum-Institut e.V.)

In-depth text "The NSA affair" - PRISM (own design, CC-BY-NC)

In-depth text "The NSA affair" - Bullrun (own design, CC-BY-NC)

Chapter 2.4 Leaked NSA document (© National Security Agency 2007, via New York Times 2016)
New York Times

Chapter 2.5 Chapter header „The semi-conductor industry" (own design, CC-BY-NC)

In-depth text „What are microchips?" - Moore's Law (own design, CC-BY-NC, data source: Rupp, Microprocessor Trend Data (2022), via ourworldindata.org)
ourworldindata.org

Chapter 3.1 Simon Schrör (© 2024 Weizenbaum-Institut e.V.)

Chapter 3.2 Media proficiency (own design., CC-BY-NC)

Chapter 3.2 Legal certainty (own design., CC-BY-NC)

Chapter 3.2 Dr. Bianca Herlo (© 2024 Weizenbaum-Institut e.V.)

Chapter 3.2 Quantum Systems Research Program (© 2022 Federal ministry for education and research, Bundesministerium für Bildung und Forschung, department quantum technologies, via quantentechnologien.de)
quantentechnologien.de

Chapter 3.3 Margrethe Vestager Data Governance Act (© 2020 European Union, via EC Audiovisual Service)
EC Audiovisual Service

Chapter 3.4 Rita Gsenger (© 2024 Weizenbaum-Institut e.V.)

Chapter 3.5 Thierry Breton Chips-Act (© 2022 European Union, via EC Audiovisual Service)
EC Audiovisual Service