Föderation der Nationalen Elektrotechnischen Vereinigungen Europas AISBL
Convention of National Associations of Electrical Engineers of Europe AISBL
Fédération des Associations Nationales des Ingénieurs Electriciens de l'Europe AISBL

Technological Sovereignty:

Methodology and Recommendations

Summary

Technological sovereignty is the ability of a state or society to implement political and social priorities, without being hindered by inadequate or lacking control of technology. It must be distinguished from autarchy on the one hand and heteronomy on the other. Achieving objectives such as climate and environmental protection, digitalization in the framework of the social market economy and data protection depends on the availability of suitable technologies. On 19 February 2020, the President of the European Commission Ursula von der Leyen wrote on the occasion of the presentation of the European Commission's strategies for data and Artificial Intelligence that "technological sovereignty describes the capability that Europe must have to make its own choices, based on its own values, respecting its own rules. This is what will help make technological optimists of us all." President von der Leyen is right: Only in a joint European effort can we position the EU once again among the world leaders.

The aim of this position paper is to discuss the concept of technological sovereignty, to analyze which prerequisites are necessary to obtain or recover technological sovereignty, and to define specific recommendations particularly for the essential field of technology "Information and Communications Technology" (ICT).

Fields of technology should be distinguished from sectors and related applications, as they can be used in many different applications. This paper views fields of technology as an independent dimension that is relevant for appraising technological sovereignty. For identifying and evaluating fields of technology it proposes economic, social, and political criteria.

One key contribution made by the paper consists in evaluating technological sovereignty along a generalized value chain, as the requirements on technological sovereignty differ considerably according to the activities being performed within the value chain. The paper substantiates the meaning of technological sovereignty by describing corresponding requirements for the various positions along the value chain. It points out that specific manifestations of the sovereignty requirements depend on the field of technology; at the same time, a number of overreaching common features exist. Different degrees are proposed for classifying sovereignty.

Rue d'Arlon 25 – 1050 Brussels, BELGIUM
Tel. +32 2 234 61 26 – eurel@eurel.org – www.eurel.org

The methodology for recording technological sovereignty requirements along the value chain is exemplified in two specific topics: Artificial Intelligence as a field of technology and 5G as a key technology. ICT needs a pronounced capability for sovereign action based on our own detailed technical knowledge and our ability to pursue internationally relevant research; this also includes being able to design, set up and use our own infrastructures. Given that ICT components are purchased predominantly from international manufacturers, we must at least be able to validate their trustworthiness ourselves, and to proceed ourselves with operation and maintenance of the corresponding infrastructures. We need sovereignty, but not autarchy which is out of scope in today's world of ICT technologies.

From the EUREL's point of view, fostering training and boosting research are strong levers for warranting technological sovereignty in current and future fields of technology, with relevance for both the economy (development, production, use) and also for society.

With this position paper, EUREL aims to trigger a cross-sectoral process with defined criteria for identifying the relevant fields of technology and the corresponding key technologies. Interdisciplinary cooperation on a national scale is the only way to obtain a uniform picture of where special efforts are needed to obtain or recover technological sovereignty and which are the specific expectations on technological sovereignty.

To come back on the view expressed by the President of the European Commission Ursula von der Leyen, the requirements for technological sovereignty should always also be evaluated from the European perspective. Europe needs technological sovereignty, particularly in view of the current global political situation, with a need to ascertain the degree of sovereignty for the specific fields of technology. In situations where a desired degree of sovereignty cannot be achieved by an individual national economy, there is absolutely no reason why this should not be possible in the European context.

Issued by EUREL
Editor: Dr.Klaus Illgner from VDE ITG
Editorial team: Prof. Roland Gabriel, Prof. Wolfgang Halang, Prof. Albert Heuberger, Dr. Klaus Illgner, Prof. Dorothea Kolossa, Prof. Sebastian Möller, Prof. Hans Schotten, Sigurd Schuster

EUREL - The Convention of National Associations of Electrical Engineers of Europe
Rue d'Arlon 25, 1050 Brussels, Belgium
Tel. +32 2 234 61 26
Email: eurel@eurel.org
Website: www.eurel.org

1. Why is EUREL taking a stand?

We are currently in the throes of drastic, substantial transformation affecting all areas of life. Digitalization is putting ICT into all areas of life, proceeding to change functions, economic structures and, in the end, the substance of society itself. We can no longer rely on what we know because this won't last.

Triggered by cyber-attacks, internet espionage and the publication of confidential information, a debate is taking place, primarily in the context of digital sovereignty and technological sovereignty, as to how to sustain or establish trust in ICT infrastructures and how we can maintain or restore our capacity to act.

Discussions reveal that security is just one facet. Issues such as access to technology, access to components or the ability to make infrastructure components ourselves go much further and extend into parallel discussions about how far it should be possible for companies to be controlled or even taken over by foreign investors. Understood in this way, technological sovereignty addresses very basic questions of economic policy. This paper aims to make a contribution by placing various definitions of digital sovereignty and technological sovereignty in a kind of map that shows their corresponding range. It transpires that digital sovereignty and the corresponding security aspects are embedded in a greater context.

Furthermore, there are different degrees of technical sovereignty. How "sovereign" does who want to be? The range extends from relying on free market forces to issue (and enforce) regulations, through to being in a position to make and operate everything ourselves (national autarchy).

First and foremost, the position paper addresses specialized experts and the political sector. It aims to indicate the meaning of technological sovereignty for the national economy and for society. ICT is the key technology that runs like a red thread through all fields of technology. In the end, it comes down to warranting the future viability of our national economy and thus the whole basis of our society. A structured systematic analysis is suggested to illuminate and evaluate systemic aspects in particular. The political sector is challenged to bring all stakeholders together to elaborate a shared understanding of who deems which degree of sovereignty to be appropriate and which degree of sovereignty has to be achieved in which fields of technology with regard to the economic and political aspects involved. Politically defined points of guidance will be needed particularly in socially relevant areas such as mobility. Furthermore, there will be marked differences in how stakeholders see things along a general value chain, starting with education and knowledge management via research, production

Example 1: Manipulating critical infrastructures
Hackers have managed to log into and infiltrate power grids ***(Wet16), (NCA18)***. Hospitals have been brought to a standstill by ransomware. Personal data of people involved in public life (journalists, politicians) has been published on the internet. These are just a few examples to show how infrastructures are anything but secure and how essential infrastructures are vulnerable to attack.

Example 2: Investment cycles versus the speed of technical development
The public sector (including the military) and also various sectors of industry invest in infrastructure and operate it over very long periods of time (in some cases >20 years). Processing facilities in particular run for decades. What can be done to warrant that parts and know-how for operating and maintaining a certain infrastructure (hardware and software) will still be available decades later? At the moment, suppliers are mainly non-European companies, leaving little scope for influencing product life-cycles.

Example 3 – 5G in industry
5G is of key interest to industry as a communication technology e.g. for automation, with correspondingly high demands in terms of reliability and security. It must not be possible to manipulate facilities from the outside (e.g. a production facility for chemical substances), nor should data (even tax data) be revealed to third parties for competition reasons. Complete control of the infrastructure is therefore indispensable for industry. But how can the security, confidentiality and reliability of the infrastructure be warranted?

Example 4 – Banks (Keu18)
The capital markets play a key role in a functioning national economy. Up to now, the flow of money has been controlled by the banks. Digital platforms are now changing the flows of money and also the players involved in controlling/steering where the money goes. The dominant players are non-European private-sector technology companies. National companies (including the banks) depend on their goodwill (cf. access to Apple's NFC interface for the banks). How much influence do we still have on regulations? How much control do we need?

and operation through to usage and the impact on society. This can then be used to derive specific measures. One thing is important: technological sovereignty and/or digital sovereignty cannot be restricted to ICT security. Technological sovereignty affects ICT, energy technology, energy supply, biotechnology/bionics, industry and many other areas. In the end, a position should be elaborated for each field of technology.

2. What does technological sovereignty mean?

Sovereignty is generally understood to mean a state being independent from the influence of another state, but also the right to act freely at one's own discretion, as well as a person's self-assured, confident conduct. Originally coming from the French language, the word also describes the highest power in a state (the king as sovereign).

Key characteristics of sovereignty are therefore autonomous, independent action, including particularly the ability to act autonomously. Sovereignty covers not just acting at one's own discretion but also being the last (highest/final) decision-making body. Sovereignty differs from autarchy on the one hand and heteronomy on the other.

There is currently much discussion of digital/ICT sovereignty, against the backdrop of cyber-attacks particularly on critical infrastructure, intelligence services spying on citizens by tapping and evaluating huge quantities of data and also data collections by large international corporations. Many interest groups from industry, society and politics have already expressed their opinions and demanded corresponding measures ***(Bit15) (Mai15)***. The ZVEI ***(ZVEI15)*** defines digital sovereignty as the capability of consistently controlling the confidentiality, integrity and availability of data transfer, storage and processing.

However, in some cases different expression are used for synonymous or partly identical aspects. Wikipedia defines technological sovereignty as follows: "Technological sovereignty is a political outlook that information and communications infrastructure and technology is aligned to the laws, needs and interests of the country in which users located; data sovereignty or information sovereignty sometimes overlaps with technological sovereignty, since their distinctions are not so clear cut, and also refers to subjection of information to the laws of the country in which the data subject is a citizen, or the information is stored or flows through, whatever its form, including when it has been converted and stored in binary digital form." (***Wik20***).

The expression “technological sovereignty” appeared in Europe for the first time in 2011, when Thomas de Maizière (then German Federal Minister of the Interior) and René Obermann (CEO of Deutsche Telekom at that time) initiated the SICT working group "Security in critical ICT applications and ICT architectures" in order to develop a strategy for "sustainable safeguarding of ICT-critical application" (***Bau15***). Technological sovereignty was scrutinized in five different application areas: privacy protection and sovereign ICT, identity management, smart vehicle and smart grid as well as monitoring and controlling large-scale technical facilities (Bau15). Technological sovereignty is therefore primarily used with a focus on security aspects.

Current discussions in Europe and the USA about the possibility of banning Huawei as a 5G network supplier show how important it is to be able to trust those who manufacture the systems for critical infrastructure. It is not just about regulations but also about the production of components for the communications infrastructure and resulting insights into the very essentials of the corresponding network elements. The transition from digital sovereignty to the more comprehensive technological sovereignty is therefore a fluid one. The Huawei debate also includes economic aspects with regard to the competitiveness of trustworthy hardware and software and regaining digital sovereignty. The takeover of Kuka by Chinese investors is another example of how limiting technological sovereignty to just ICT and IT security is too short-sighted. Other fields of technology that are relevant or even existential for the future viability and acting capacity of a state/business location include biotechnology (food supply), bionics, energy (e.g. storage), geodata or pharmacy (medication). In fact, digital sovereignty can be seen as a special case of technological sovereignty that specifically addresses how data are handled, processed and communicated. In particular, digital sovereignty also addresses the individual (media sovereignty). (Fig.1)

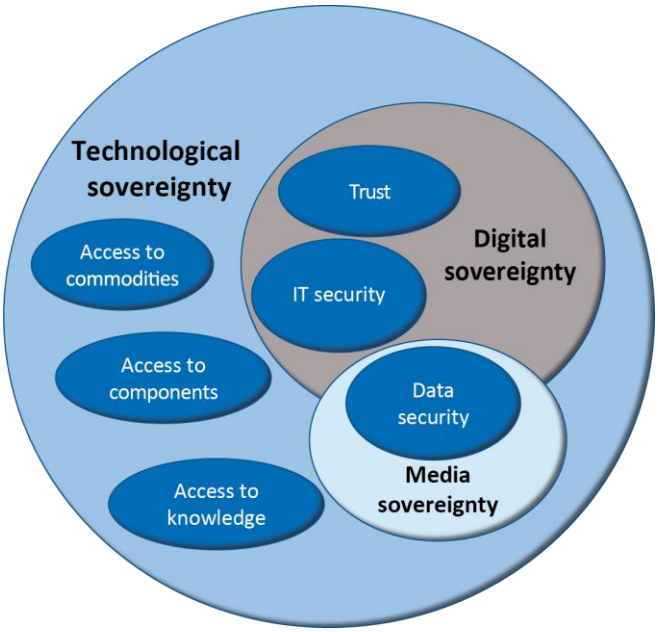


Fig. 1 Relationship between various forms of sovereignty

When ascribing sovereignty to technology, technological sovereignty means nothing more than acting and deciding autonomously with regard to a technology and, above all, having the final power of decision.

In the context of close international networks and dependencies, starting with science via commodities trading through to production, the question arises as to how far such technological sovereignty can be achieved at all, respectively which objectives technological sovereignty should actually achieve. The degree to which technological sovereignty is deemed desirable or even necessary, and in which sectors and fields of technology, depends on how comprehensively the value chain should be covered and which roles individual protagonists perform in the value chain. In the end, overarching strategic and political decisions will have to be taken.

This position paper focuses on ICT technologies which are meanwhile seen as existential. In the course of digitalization, ICT is influencing all sectors and, increasingly, all other aspects and areas of our lives. At the same time, the position paper also repeatedly refers to other fields of technology with a broader discussion of technological sovereignty.

3. Aspects of technological sovereignty

Getting closer to the possible meaning of technological sovereignty entails correlating several aspects as appropriate dimensions (Fig.2**Error! Reference source not found.**). The latest Bitkom statement on digital sovereignty also identified various dimensions for substantiation (***Bit19***).

One such dimension is technology itself, structured in fields of technology. Defining a field of technology is not as easy as the expression may initially suggest. The difficulty results from making a distinction between field of technology, sector and application area. While a field of technology necessarily focuses on the technology as such, a technology itself can be used for highly differing applications in various sectors. ICT technologies are an obvious example here. Sectors and applications are therefore viewed as the second dimension. The third dimension

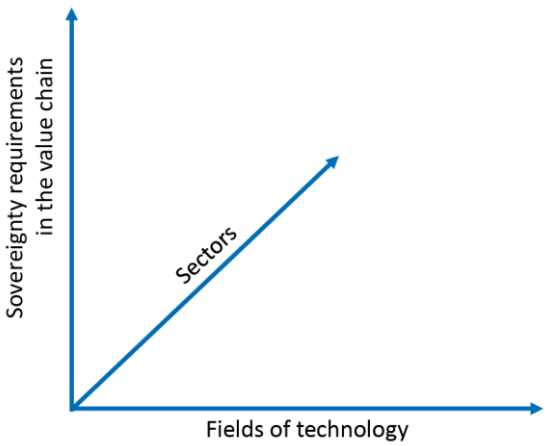


Fig. 2: Viewed dimensions of sovereignty

consists of the expectations regarding sovereignty. The things that can actually be achieved by sovereign action depend essentially on the actual task in hand. Is it a case of establishing knowledge, training, production or operation capability? Or "just" corresponding use by the consumer? The meaning of sovereignty is therefore put into specific terms along a generalized value chain.

The three dimensions are defined in greater detail below. A systematic approach is proposed for ascertaining the fields of technology. The three dimensions are then correlated accordingly, with proposed criteria for identifying and evaluating fields of technology that are relevant to sovereign action.

3.1 The "sectors" dimension

Companies are said to belong to a sector when they make essentially interchangeable products and services ***(Eng00***). Different classifications are used for allocating companies to a sector. The classification used by Statista for example differs clearly from that used by the German Federal Ministry for Economic Affairs and Energy (BMWi) , see Annex B. The following section uses the sectors defined by the BMWi as an evaluation dimension.

The expression "application area" describes areas where something, i.e. a certain technology, is applied or used. Sectors and application areas are therefore not necessarily congruent. Office communication for example is an application of IT that is used in many different sectors. IT is thus initially a technology, but it is also part of a field of technology, as will be explained below. But at the same time, IT is also part of ICT which is listed as a sector in its own right.

Given that applications are an attribute of sectors, separate structuring in application areas would not appear necessary (no additional insights). This applies all the more in view of the fact that in contrast to application areas, extensive economic data is available for sectors that depict key criteria for assessing the economic relevance.

3.2 The "fields of technology" dimension

Selected fields of technology will be used to analyze and depict the requirements and manifestation of technological sovereignty. There is no uniform, generally valid definition for “field of technology”, so that literature offers differing classifications with varying granularity (***Mai15) (GK16) (CP00***). The first point of reference is therefore the OECD classification which, after all, is an international normative reference (***OEC07***). Meanwhile twelve years old, the classification is very abstract with the fields of technology relevant in the further context of electrical engineering:

1.2 Computer and information sciences

2.2 Electrical engineering, electronics engineering, information engineering

2.5 Materials engineering

2.6 Medical engineering

2.10 Nano-technology

5.8 Media and communications

One possible indication for substantiation can be found in the way the classification of technology is refined into basic, future, pacemaker, key and high technology (***Zimmermann, 2007***). Working on this basis, the following fields of technology would appear relevant at present:

- Optronics
- Optical technologies
- Lasers
- Electronics
- Microelectronics

This selection alone already shows a very detailed classification. The aim is therefore to find a scheme that is specific enough for the classification of technologies without having an unmanageable number of fields of technology. Fields of technology should also reveal long-term temporal constancy.

With a view to technological sovereignty as the objective, an attempt will be made to distinguish fields of technology from sectors respectively application areas. Application areas can use many different fields of technology at the same time. By contrast, classification into fields of technology focuses primarily on essential technical functions and the technologies needed to achieve them, which can be used in many also very different applications and sectors. This is visualized in the diagram shown in Fig. 3. Depending on the degree of abstraction applied to the fields of technology, ICT can refer to both a sector and a field of technology.

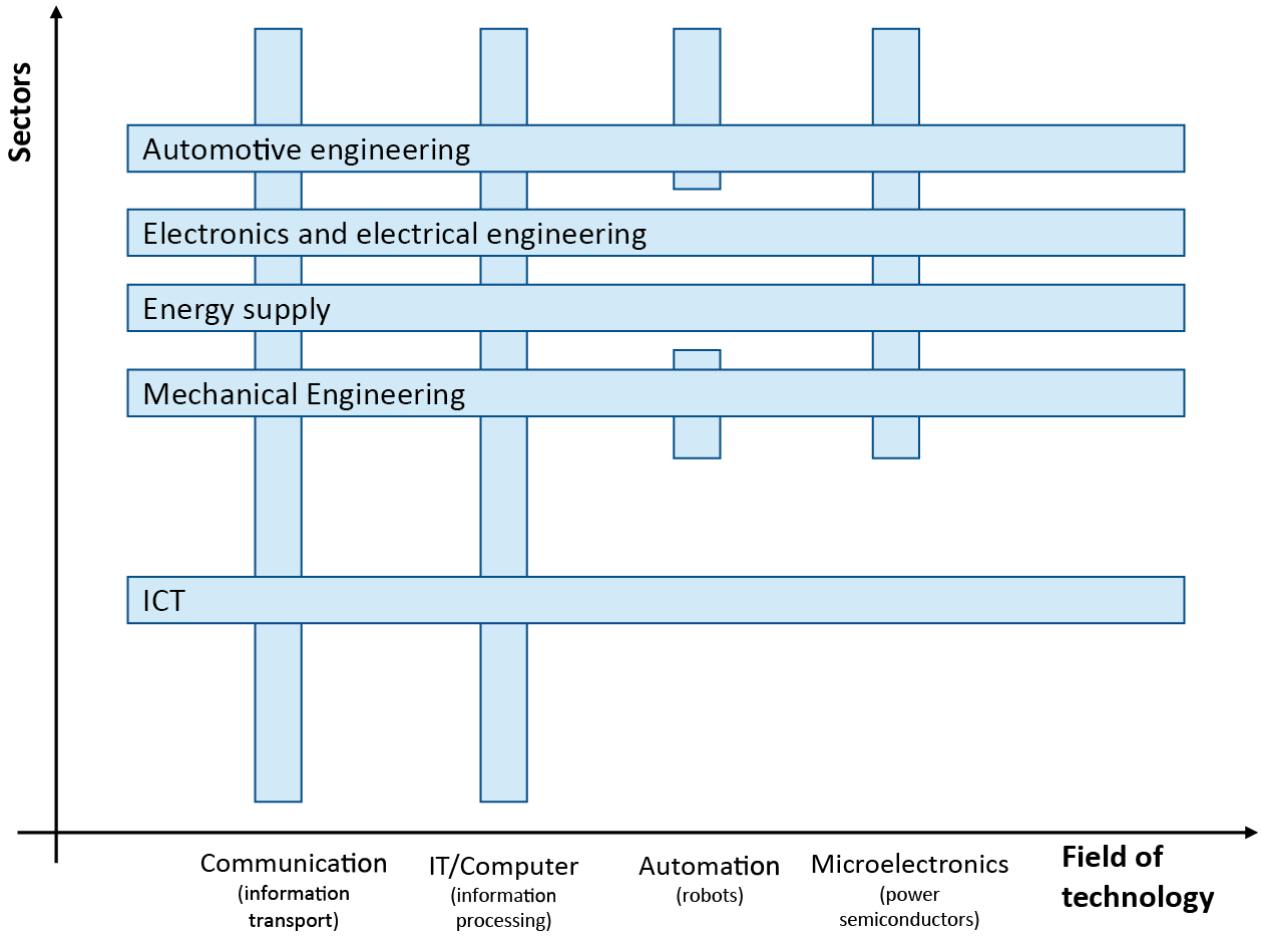


Fig. 3: Sectors / applications where fields of technology play a key role

But which criteria are suitable for defining and identifying a field of technology?

The technical sub-classifications used by the Technical Societies GI, VDE and VDI were taken as the starting point (see Annex to the study). The contents are geared more to technologies than sectors. Fields of technology can thus be derived on a relatively abstract level with similarities to sectors and applications but seen as being technological. However, this level is probably too abstract for technological evaluation.

In the end, technical systems emerge when certain functionalities are assembled into increasingly complex systems to fulfil certain tasks. In this paper, field of technology refers to technical systems that perform certain core functions. In ICT for example, it is essentially a case of transporting, preparing, saving and processing information. The expression is set on a relatively abstract level to make it relevant for a longer period of time.

Various (key) technologies are suitable for implementing these functionalities. While core functions do not change over time (e.g. data transport), the technologies used to implement them certainly do. In terms of technological sovereignty,

it is therefore a case of being able to use the current key technologies that are required to implement a function with the necessary performance data, costs etc. Key technologies here are understood to be technologies that make new economically relevant technical functionalities possible, or that make it possible to implement existing technical functions in a particularly economical way. Sovereign action is therefore not necessarily associated with a revolutionary method that "triggers an innovation boost going way beyond the borders of an individual economic sector" (***Wik19a***). Understanding key technology in this way means that it can depend on application and objective whether a technology is a key technology or not.

As an example, fig. 4 shows fields of technology that are relevant to EUREL together with the system areas / core functions. The listed key technologies should also be viewed as examples. Analysis reveals that individual key technologies can also be attributed to key functionalities of different fields of technology.

Technology Field	Systembereiche (Funktionen)	Key Technology
Information and Communications Technology (ICT)	Communications	5G
		swarm communications
		optical communications
	IT / Computer	quantu mcomputers
		ultra small computers (IoT)
		super computers
	Security	autom. Security analysis
		encryption
		Blockchain
Micro-elektronics	SoC	mixed signal integration
		nergy minimization
	power electronics	SiC / GaN
	neural networks	processro architectures
		TPU / GPU architectures
Software	Development	automated verification
		visualization
	Simulation	weakness identification
		digital twin
	MMI	voice / face / gesture recognition
		control by brain
Artifical Intelligence	machine learning	deep learning
		cgnitive systems
		training concepts
	recommendation / expert systems	
	data analysis	data acquisition and storage
		classification

Technology Field	Systembereiche (Funktionen)	Key Technology
Digitale Plattforms	trading platforms	busienss models
		identity management
	transaction systems	e-payment
		quthentication mechanims
	service platforms	Software as a Service
		Micro-Services
Energy	generation	small scale power station
		bio power generation
	distribution	smart networks
	storage	battery technology
		gas conversion
Automation	industrial automation	digital twin
	robotik / autonomous systems	human machine interaction
		cognitive identificaton
	measurement and control technology	sensors
Technology for Medical	Diagnostics	meassurement techniques
	Treatment	technology for surgery
		Bio-Sensorics / -Aktuatoren
		Micro-Robots (blood stream)
	Technoloky for Care taking	

Fig. 4: Identified fields of technology and relevant system areas within the respective field of technology. The listed key technologies should be viewed just as examples without any claim to offering full, comprehensive coverage of all key technologies.

3.3 Assessing the relevance of fields of technology

How is a field of technology to be assessed in terms of its relevance to technological sovereignty? Which key technologies must be mastered with which degree of vertical integration in order to implement a certain function or application in a certain sector? As an example, a new material could result in a highly sensitive tactile sensor for robots. If there are applications that can only be implemented with this sensor, then sovereign use of this technology would be desirable. On the other hand, if demand is limited just to applications that can be implemented with conventional grippers, then this special sensor technology is of minimum relevance for sovereign action.

It is not a case of mastering technologies for their own sake but of being able to make sovereign use of technologies with economic, social and political relevance.

Identifying relevant fields of technology needs corresponding classification criteria geared to technological sovereignty respectively the corresponding objective. By definition, this is often primarily a case of sustaining economic performance. However, at the same time discussions of digital sovereignty also show that security aspects should play a major role when identifying relevant fields of technology. Security here refers not just to IT security but also functional safety and, on a much broader scale, in the end also national security. Other aspects to be taken into account when analyzing fields of technology from the point of view of technological sovereignty should also include the reliability of supply (including food, health), sustainability (e.g. neutral carbon footprint, environmental protection) and relevant social aspects - in other words, overarching political objectives. The following criteria are proposed for assessing the relevance of fields of technology in terms of technological sovereignty:

- Economic benefit
    - Aggregated economic performance of the sectors for which the field of technology is relevant. A field of technology will not be responsible for the total economic performance, so that a percentage weighting is conceivable for depicting the so-called leverage of the field of technology for the sector.
    - The current growth rate of sales in a sector can be a point of reference, but it only covers fields of technology that are already being exploited economically. Allocation to a certain field of technology is only possible to a very limited extent.
    - Consideration should also be given to the life span attributed to the field of technology from today's perspective.
    - Potential for new business models: particularly in the age of digitalization, new business models using digital technologies challenge or replace established value chains. Fields of technology should therefore also be assessed in terms of the disruption potential for new (digital) business models. The way Apple has entered the field of payment services is just one example of how the financial sector is facing competition from market players outside the sector.
- Future viability
    - Innovation capability is the basis for future competitiveness. A suitable criterion in this context is the expected (estimated) economic potential that could evolve from using the field of technology in other economically interesting application areas.
    - The technological readiness level (Wik19b) helps to assess how long it will take until a technology can be put to successful economic use. It is usually easier to attain sovereignty in a very early stage of technological development than after the technology has been developed and is established on the market.
- Social acceptance
    - Under certain circumstances, a technology that finds no social acceptance at all may not be suitable from general economic aspects or may increase the overall costs (e.g. nuclear power).
- Necessity in terms of security
    - Relevance to domestic and/or foreign policy regardless of economy and sector

- It may be necessary to have sovereign acting capacity for a certain technology in terms of security (cyber-attacks, aspects relating to intelligence operations and/or the military). In the end, this is a political decision.
- Sovereign acting capacity in a certain field of technology can also be relevant to warranting supplies (electrical power, logistics, ...).

- Sustainability
  - Even if this aspect does not address economic issues directly, it should always be given due consideration today out of our responsibility for the environment. Furthermore, frugal and sustainable handling of resources (which includes recycling) also reduces our dependence on international and sometimes monopolistic suppliers.

Fig. 5 illustrates how the relevance of a field of technology can be derived from the assessment according to the above criteria. The increasing degree to which a Harvey ball is filled shows the growing significance of a criterion for a field of technology. For example, ICT is of great economic benefit at the moment, while on the other hand we currently have only very limited scope to influence the future development of ICT on an international scale. The diagram shows the ACTUAL status; the same approach can also be used to show a desired final state (PLANNED). Attention is drawn explicitly to the fact that the assessment shown here is just an example, as it is not based on any empirical analysis.

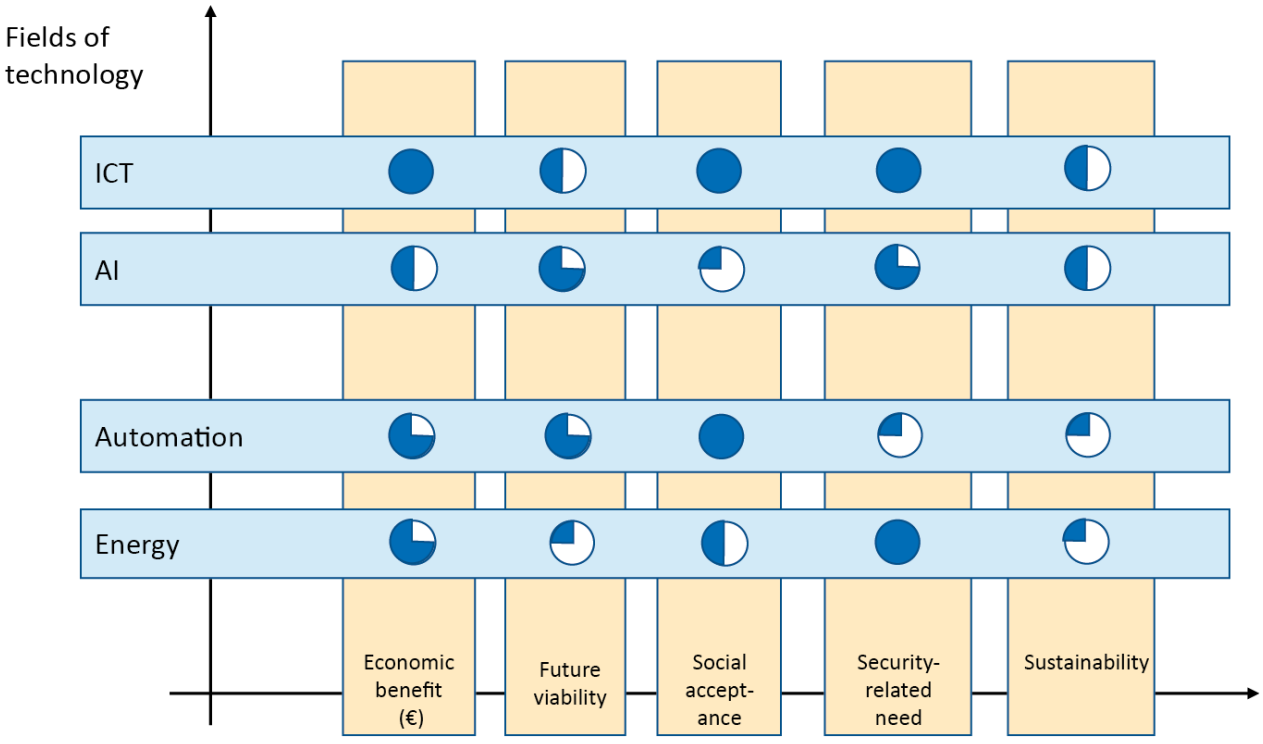


Fig. 5: Overall ACTUAL assessment of fields of technology.
The depicted assessment is just an example without any empirical basis

This summary fails to point out one essential aspect, and that's the significance and ability to think in complex systems, and to design, make and operate such systems.

ICT is another case in point. Making targeted use of ICT in other sectors needs detailed know-how about the specific requirements and context (domain knowledge). For example, in the energy industry, the transition from large central power stations to many small power stations (turbines, photovoltaic arrays, biomass, ...) is generating new requirements for the communication between a very large number of grid elements (generators, distribution, consumers). In the end, seminal solutions can only be developed by combining ICT with domain knowledge about the energy industry.

The development of industrial automation (Industry 4.0) also demands domain knowledge from highly differing fields of technology and specialist disciplines, including conventional manufacturing knowledge, ICT, AI and microelectronics.

But the success of increasingly significant interdisciplinary interaction across different fields of technology depends on having sufficient sovereignty in all affected fields of technology.

3.4 The "sovereignty requirements" dimension

What is the real meaning of "sovereign action" with regard to technology? A manufacturer makes completely different demands in terms of sovereign acting capacity than a grid operator or the consumer, or even the state with its institutions and its responsibility for social cohesion. It is therefore worth structuring the requirements for "sovereign action" along a generalized value chain (fig.6).

Fig. 6: Generalized value chain

3.4.1 Sovereignty along the value chain

Looking at the value chain, the stakeholders have highly differing requirements in terms of access to and the handling of technologies, depending on the specific stage of the value chain. Furthermore, market participants assess the requirements for technological sovereignty differently in individual sections of the value chain according to their role and task. In communications technology, a network operator has other ideas than a network supplier or the user. A simple model indicates the roles of market participants that are relevant for sovereignty:

- Customer / consumer
- Operator / provider / retailer
- Manufacturer
- Research / training
- Government / regulator

These roles fit in well with the levels of the generalized value chain, so that the market participant roles will not be viewed separately when looking at the requirements for technological sovereignty: instead, the individual levels of the value chain will be viewed primarily from the point of view of the assigned roles. Society and the political sector as legislator and regulator also take up certain overreaching roles. Their requirements are included in assessing the relevance of a field of technology.

The following section analyzes the requirements and possible expectations for sovereign acting capacity along the value chain.

- <u>Knowledge management, initial training, further training</u>

  Access to a technology requires knowledge about the technology itself. This refers to access to information, knowledge, databases and publications, as well as access to international expert groups for exchanging and sharing ideas. Teachers are needed for preparing and imparting the information. In the end, it is not just a case of elaborating new knowledge. In terms of using a technology, it is also a case of operating systems implemented with the technology, with corresponding initial and further training. Given that some technologies are in use for very long periods of time, there must also be long-term access to knowledge, possibly for even longer than a product is on the market.

  Regardless of who actually performs which tasks along the value chain, e.g. including foreign suppliers, it is crucial for sufficient expertise to be available "on the spot", i.e. in the country itself, in order to at least validate and define the quality of the "delivery".

Knowledge management is a basic prerequisite for being able to act in a field of technology. Regardless of the field of technology, any kind of sovereignty therefore also requires self-determined, autonomously organized knowledge building and knowledge transfer.

One special aspect of ICT is that there must also be a constant transfer of current knowledge to every citizen. To the same extent in which every citizen must be able to handle information and communication technology, e.g. when using the internet, which also increasingly applies in the context of public administration, here further training must also take place and people must be made more aware of issues such as IT security and data protection. Sovereignty in knowledge management is therefore a basic prerequisite for allowing the citizen to handle digitalization in a sovereign manner.

- Research

In addition to the above remarks about knowledge building, research depends on research projects that generate new theoretical and experimental findings. Access to international groups of experts is an indispensable element, as is close cooperation in international teams. The experimental side requires access to cutting-edge technology from many different areas, including measuring and production facilities, as well as materials / commodities. Access to software and algorithms is also needed, whereby the open source approach and the concept of freely available publications is firmly anchored particularly in the research community.

Sovereignty in the research setting therefore means first and foremost the political will for certain subject areas to be anchored at universities and colleges, and to fund research in these subjects.

International standardization plays a central role in ICT. Sound research that creates the basis for internationally acceptable technical proposals is necessary in order to assert our own requirements, such as depicting data management processes. Anyone not involved in standardization has to live with the technical procedures thus stipulated by others. Sovereign research and comprehensive active participation in international standardization are cornerstones for ensuring that certain properties are fulfilled by subsequent products - or not, as the case may be.

- Product development

Development focuses above all on devising a product and then producing a prototype which is tested and optimized. Production requirements such as necessary materials, producibility on available machinery and component availability are already integrated in the development phase. Developing a marketable product needs comprehensive, diverse technical expertise combined with practical experience not only in the particular core area (e.g. network technology) but also in many other specific fields. The more complex a product, e.g. a car, the more diverse the relevant fields of technology.

The degrees of possible sovereignty are larger here too. For example, it is possible to focus on system integration where most components are developed and supplied by third parties, as is currently the case in the automotive sector. Similarly, the strategy can pursue a high degree of vertical integration. In this case, a company produces the entire product itself, thus gaining sovereignty i.e. self-determined action. For example, in Dresden Bosch is building its own chip factory to "keep the key technology in its own hands ..." (***Dew17***). The requirements regarding product development are also growing at the same time. Successful development of a product needs a certain "sovereignty" in many fields of technology.

One current example is battery development, which is seen as the key technology for electromobility. The development of competitive electric cars, together with other applications that could benefit from efficient batteries, will be severely restricted without sufficient expertise and access to this technology.

Besides hardware developments, scarcely any systems exist without software. But today's software stacks are very extensive and consist of many libraries from a wide range of different origins. It has become almost impossible, or at least scarcely feasible in market terms, for companies to develop all software levels themselves. Software development also needs extensive software tools. Sovereign acting capacity in this case means access to the corresponding development tools and software libraries, as well as having experts familiar with software development tools and methods. Given the essential role played by software as a component in

modern systems, great attention must be paid to the safety requirements associated with the software. A high degree of sovereignty in software development reinforces the ability to warrant safety requirements.

- Production

  Manufacturing a product needs access to production machinery, materials and components. In some cases, extensive testing equipment, machinery and additional materials are necessary for quality assurance. Furthermore, successful production today also depends on sophisticated logistics. And in the end, suitably qualified staff must also be available. Particularly where complex products are concerned, the requirements in terms of infrastructure, material and knowledge are not limited to just one field of technology.

  The technical challenges for example in chip production or when making precision optics are so high that there are only very few companies worldwide capable of supplying the corresponding production and testing machines.

  It would therefore appear very difficult, if at all possible, to achieve comprehensive technological sovereignty (national autarchy) when it comes to manufacturing more complex products. With regard to ICT, it is repeatedly said that we should be able to produce key components of the communication infrastructure ourselves. This has far reaching consequences. It's not just a case of assembling the router or base station; these are modules that consist of a large number of components, particularly chips. Sovereignty in producing the router would also mean sovereignty in chip production, including the production machinery and testing equipment. Besides these technological issues, the highly complex nature of many products with the necessary development workload and the resulting economic pressure to use effects of scale tend to make national autarchy less expedient.

  What degree of sovereignty, of self-determined acting and deciding, is appropriate and possible when manufacturing products and devices? Given the inevitable need for cooperation and supplies from foreign companies, the question arises in terms of how to verify not just reliability (quality assurance is an established step in the process) but also, particularly when ICT is involved, how to immediately verify trustworthiness. The discussion of Huawei's trustworthiness as a supplier for 5G network equipment shows just how delicate this issue is. The fact that China is replacing the IT hardware in state organizations with national products through to 2022 (Han19) shows that sovereignty over a country's own infrastructure is also highly significant for other national economies. To a certain extent, availability is already being safeguarded today with the dual supplier strategy.

- Operation

  Operating a technical infrastructure/technical equipment demands comprehensive knowledge about the operating behavior of a device/infrastructure. Here the aim is for sovereign action to establish and sustain the required operating status for an infrastructure/network and to restore operation in the event of disruptions.

  Maintenance demands a deeper understanding of the components. As a rule, only the manufacturer knows all the details and is able to remedy deep-seated problems. But this also means that the manufacturer gains access to highly sensitive operational data.

  Sovereign operation also includes the aspect of resilience. How can infrastructure be set up to prevent the entire infrastructure from being paralyzed when problems arise? In the case of communication networks, this means not only sending content via two completely different routes but also using different transmission technologies for the alternative communication route.

  Another aspect of system operation is providing feedback to the development process. If operating experience is integrated in the production or conception of following generations, then products can be made which are by far superior.

  As far as state action goes, special requirements often apply to the operation of technical systems used for sovereign tasks or warranting internal and external security.

- Usage

Firstly, all citizens need a certain degree of sovereignty in handling digital infrastructures and data. This requires corresponding know-how. Citizens also have a great interest in what happens with personal data.

When it comes to professional usage, sovereign acting capacity may be necessary. But there are clear differences here, depending on the user. The corresponding economic range is great and varies according to the specific business activity. The public sector and the security authorities in particular have a vital interest in high-security data communication. Absolutely secure operation of IT devices must also be possible. In the defense sector, extensive autarchy is necessary for example with regard to communication.

- Renewal

  In some application areas, the investment cycles do not correspond to the technical development cycles. Systems are kept operating for far longer than the period of time in which the manufacturer provides technical support. Examples include public infrastructures, processing facilities or also military technology. In this context, sovereignty means being able to take decisions over and beyond investment cycles, regardless of technical development cycles.

4. Manifestations of technological sovereignty

The detailed look at the value chain has already indicated that sovereignty has various different manifestations (MRB18). These describe what sovereignty is supposed to achieve. Based on the requirements arising from the value chain, it is proposed to distinguish between the following forms of sovereignty.

- Knowledge sovereignty
  - Warrants access to knowledge and the ability to impart knowledge
  - Sovereignty in preparing information and knowledge
  - Availability of experts / teachers who have the knowledge
  - Ability to assess technologies
- Research sovereignty
  - Self-determined decisions about research topics (taking them up, monitoring and funding them, ...)
  - Self-determined access to international groups of researchers where information is shared and exchanged freely
  - Access to current technologies, components and commodities to perform experiments, measurements and related activities
- Infrastructure sovereignty
  - Capacity to record, assess and influence the functioning of complex systems
  - Capacity to set up technical infrastructures in a trustworthy manner or at least to validate the trustworthiness of the corresponding infrastructure
  - Capacity to operate technical infrastructures in such a way that the offered services are trustworthy
- Data sovereignty
  - Freedom of decision and self-determination with regard to the usage of "own" data, where "own" means either data belonging to a company or personal data
  - Absolutely confidential use of personal data must be warranted.
  - Everyone must have full control of who has which data.
  - Applications only register the data that is verifiably indispensable for a service to function Voluntary registration of further data does not rule out the use of a service
  - Warranting privacy (privacy by design)
- Transparency sovereignty:
  - Possibility of tracing the origins and justifications for decisions and recommendations given by autonomous systems/AI and assistants, and to influence these with human intervention when the need arises
- Development sovereignty

Developing a product not only needs comprehensive knowledge about subsequent production during the development phase but also certain production skills, e.g. for prototypes and also for testing production steps. Most aspects of production sovereignty are therefore also relevant for development sovereignty. Additional aspects include

- Self-determined decisions about the concept, manifestation and, finally, the implementation of a product
- Access to the means of production → production sovereignty

Detailed knowledge of the markets plays a key role in product development. This refers to the future operator and user who have an essential impact on technical aspects in terms of "how something should work". Today, no development (hardware and software) is possible without comprehensive access to (trustworthy) software tools. The more software becomes part of the value creation process, the greater is the need to be able to adjust software to one's own specific requirements.

- Production sovereignty

  Particularly where complex products are concerned (e.g. car), many different prerequisites are necessary in the sense of sovereignty in order to be able to make a product For example, many components have to be produced before a car is finished. The components also have to be viewed from the perspective of production sovereignty.

  - Access to commodities
  - Ability to process commodities (→ production)
  - Access to components
  - Access to production machinery and equipment goods
  - Operation of production infrastructures (→ operation, infrastructure, data, transparency)
- Platform sovereignty
  - Capacity to set up and operate market-relevant platforms, including the necessary financial transaction systems. This may mean that the non-linear scaling effects of digital platforms are channeled by regulatory standards in such a way as to allow fair competition.
- Operational sovereignty
  - Availability of specific equipment necessary for operation (hardware and software), particularly when produced by just one or only a few manufacturers (export control is an effective means of "steering" the acting capacity of a state/industry)
  - Know-how in terms of complete set-up, control and troubleshooting
- Media sovereignty
  - Digital literacy as a social task

4.1 Degrees of sovereign action

Regardless of which specific requirements are made of sovereignty, overarching degrees of sovereignty can be defined independent of roles and technologies (and visualized as Harvey balls):

1. Knowing, developing, making and/or operating everything by the company/country itself (extensive autarchy). (ball full)
2. Making only selective use of the knowledge, skills and components of others, keeping full control over the entire system and all its parts. (ball 3/4 full)
3. Third-party knowledge, skills and components are used to a significant extent and the company/country depends on them working reliably. This also includes partial operation and maintenance of components. (ball half full)
4. Setting up and integrating the system is entrusted to third parties, together with selecting and making the components. Operation is still in the company/country's own hands but is not (comprehensively) possible

without support from the system integrator. Basically, only the knowledge required for operation is available. (ball ¼ full)

5. The company/country has no expertise of its own; manufacturing and operation is entrusted completely to others. (ball empty)

Usage has already been covered as part of the value chain with its specific sovereignty requirements. In areas where totally sovereign usage of products was taken for granted in the past, this can change in the course of digitalization. For example, the manufacturer of a smartphone today is definitely in a position to intervene in the functioning and functionality of a device, thus restricting the user's sovereignty in using his smartphone to a certain degree. It would therefore seem necessary to attribute different degrees of sovereignty to usage. Sovereignty can thus be assessed for the identified fields of technology along the value chain, as illustrated in Fig. 7. The assessment symbols shown here must be seen as examples. Substantiated statements need comprehensive, systematic verification. This would also make it possible to register both the actual and the planned status, which in turn reveals where there is particularly great need for action.

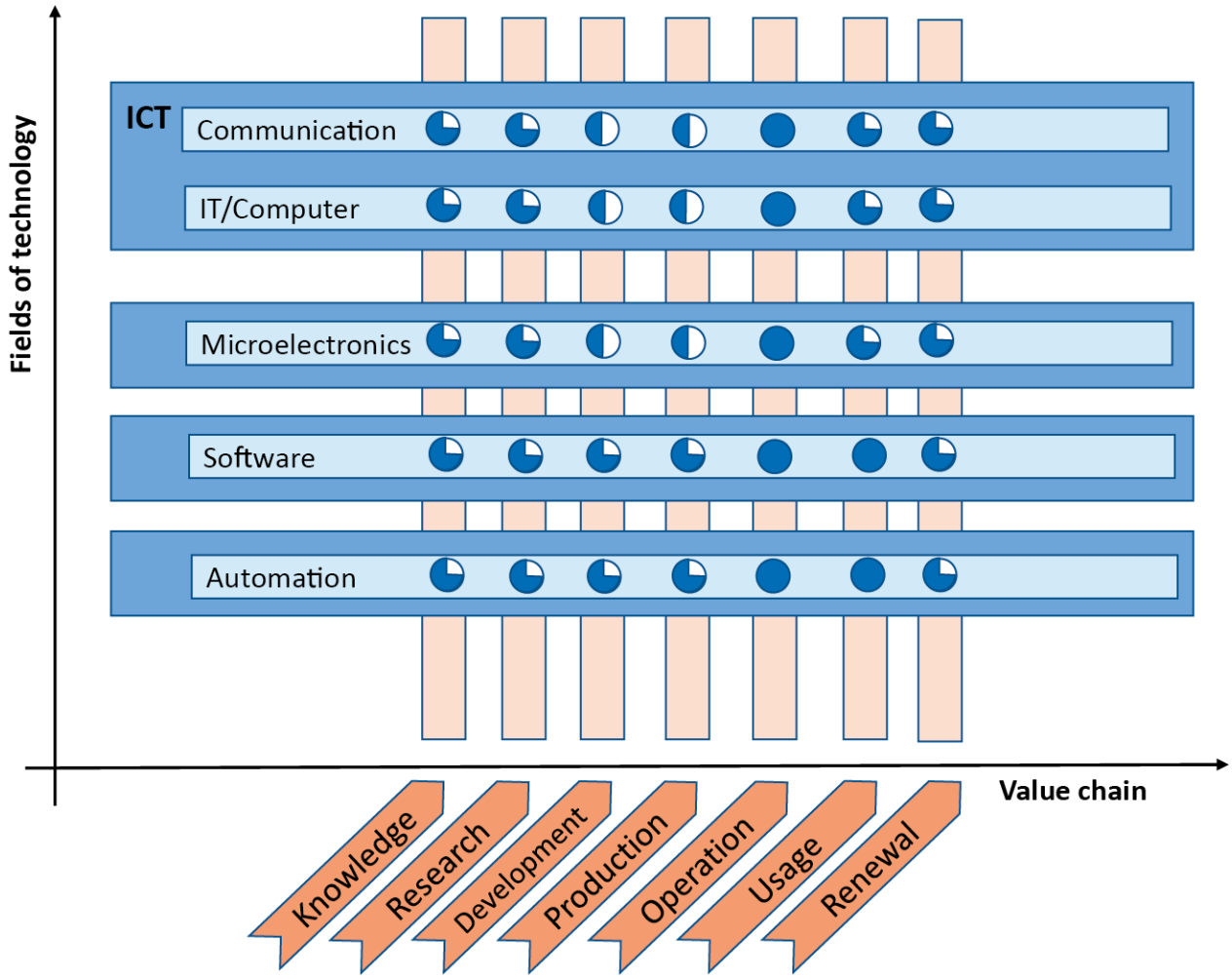


Fig. 7: Examples of the degrees of technological sovereignty for fields of technology along the value chain

Closer analysis reveals that it is nearly impossible to formulate overarching uniform sovereignty requirements along the value chain for a complete field of technology. For example, assessing the ICT field of technology from the point of view of 5G will differ completely from taking the point of view of quantum computers, for example. This is illustrated with two examples in the following section, At the same time, the diagram shows that the proposed systematic approach can be used for assessing fields of technology on different levels of abstraction through to the level of key technologies.

4.2 Examples for using the systematic approach

The suitability of the proposed systematic approach for deriving positions and requirements in terms of technological sovereignty is presented with two examples from the context of the ITG. Already when analyzing the sovereignty types along the value chain, it transpired that it is only possible to assess a field of technology from the point of view of a specific application / application area. Specific domain knowledge, i.e. knowledge about the application, is necessary before a statement can be made about the actual requirements for technological sovereignty. In the end, the systematic approach can be applied to both a specific (key) technology and to a field of technology.

At this point it should be stated explicitly once more that the assessments are indicative by nature: they were drawn up by experts but are not based on a systematic, statistically substantiated study.

4.2.1 Example 5G (key technology)

5G is the "5th generation of cellular communication systems" and is currently being rolled out on a global scale. Here is a short outline for better understanding:

1G = analogue technology, for voice communication

2G = digital technology, for voice communication, SMS and slow data services (GSM, GPRS, Edge)

3G = digital technology, for voice communication, SMS and internet access (UMTS)

4G = digital technology, for internet access, voice communication, SMS and video (LTE)

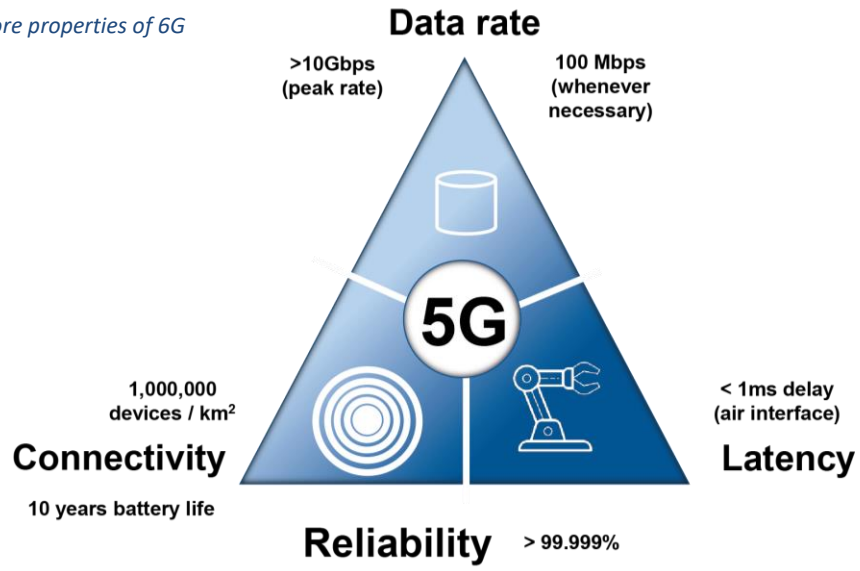
5G = digital technology, cloud native, for video, internet access, voice communication, SMS and for the highly differing requirements of the "Internet of Things" in the context of digitalization across all sectors and all areas of life.

5G has three core properties that can be combined depending on the specific application:

- Extremely large capacity and speed for data transmission (up to 10 Gbit/s per radio cell)
- Real-time capability (down to 1 ms latency in data transmission) and highly reliable data transmission ("five nines" 99.999% for 1 ms latency and "six nines" 99.9999% for larger latencies)
- Connectivity for connecting very large quantities of IoT devices (up to 1 million devices per km²).

Besides these functional properties, 5G with its modern cloud-based system architecture permits so-called network slicing, i.e. virtual private networks with application-specific properties on shared physical infrastructures. The 5G architecture is also designed for combining 5G with edge computing. IT functions for data processing and storage can thus be made available in physically close proximity to the user. This opens up further potential, depending on the application, with low latency, security and greater efficiency through local processing/pre-processing and data storage.

Fig. 8: Core properties of 6G



With these characteristics, 5G opens up a whole range of new applications for various user groups. Examples:

- Companies can use 5G for real-time process control and monitoring, for object localization or highly reliable wireless machine communication, thus boosting productivity through more flexible, connected production processes.
- Autonomous vehicles and drones permit visual inspections of building structures and facilities with high-resolution images and videos, and AR/VR applications assist service technicians in their work.
- Sensors can be used for collecting massive quantities of environment and status data which are then made available for further evaluation.
- Highly promising applications in transport and logistics include providing support for autonomous driving (e.g. platooning or automated driving for truck fleets) together with the automation of freight depots and sea ports.

In Germany, the build-out and operation of 5G networks is not reserved exclusively for (public) mobile network operators: companies can also be allocated frequencies for local use specifically for their sites, thus making maximum use of 5G's character as an innovative means of production.

5G is currently attracting considerable public attention, not just due to the diverse possibilities and expectations associated with it, but also in terms of which international network suppliers can really be trusted for setting up a critical infrastructure.

Besides the system as a whole with its possibilities and the 5G network, the 5G devices themselves deserve a specific look. The named 5G applications can only be used beneficially if the "things" in the Internet of Things are connected by tailor-made, efficient, reliable and economical devices (e.g. modems or chips integrated in the "things") via the 5G network with the corresponding application platforms in the background.

The following table shows the sovereignty requirements along the value chain for the key technology 5G in general. Where necessary, a distinction is made between the 5G network and the 5G communication component on the user side ("5G device/modem/...").

Value chain			**Degree of necessary sovereignty**	
Training / further training			**5.0**	In the emerging digitalized world, knowledge about ICT in general and thus also about 5G is vitally necessary in Europe as an industrialized area. The special focus and depth of knowledge depends naturally on the individual's role in society, in the company, etc.
	Knowledge sovereignty		5	5G is a key technology for completely new application areas in industry and society. We can only tap into these new areas if we know how the technology works in detail and which potential is thus revealed.

Research			**5.0**	In the course of digitalization over the next few years, 5G will penetrate business and society and become a central "nervous system". The 5G technology available today will go through substantial further development over the next few years. Understanding 5G's application possibilities and specific applications has only just begun, To discover the innovation potential of 5G in business and society, and to use and implement this potential in competitive advantages for our companies, we must be among the front runners both with technological research and also with an interdisciplinary approach to applied research. The timeline of previous network generations would tend to indicate that the next generation 6G can be expected from approx. 2030. We will only be able to make a significant active contribution here from the basis of sound 5G research.
	Knowledge sovereignty (see above)		5	Specialist knowledge about 5G, its technological development and application is necessary for the corresponding experts involved in teaching, R&D and application/operation.
	Research sovereignty		5	Broad, in-depth and in particular also interdisciplinary research with corresponding resources is necessary to be and stay at the forefront when it comes to using 5G and ploughing 5G experience from industry and business into the further development and global standardization of 5G. Furthermore, previous network generations have illustrated the important role played by joint research projects between industry and universities in the success of early phases in technological development.
Product development			**3.0**	Given the future potential for many application areas, it must be possible to develop our own products for the 5G infrastructure. Developing all the necessary products, starting with the chips, is not realistic. Purchasing components is simply unavoidable. At the same time, there is a need for comprehensive technical knowledge about the overall system in order to develop application-specific systems (Industry 4,.0, autonomous driving)
	Knowledge sovereignty (see above)		4	Specialist knowledge about 5G, its technological development and application/operation is necessary for the corresponding experts.
	Development sovereignty		3	5G infrastructure can only be provided by international players, due to the complexity involved and the immense R&D work needed in advance. We must therefore have the expertise to cover important aspects of product development, but we don't have to be able to develop entire 5G systems in Germany. Accordingly, the same also applies to 5G components in devices/IoT devices connected via 5G. However, optimum use of 5G may make it necessary to completely master the development of applications/sector-specific products and solutions equipped with 5G.

	Production sovereignty		2	5G components do not have to be produced in Europe, as long as adequate access to the network elements is guaranteed for setting up the networks and the 5G communication components in devices/user systems (see below). R&D aspects such as production launch etc. are therefore not of prime importance.
	Operational sovereignty		3	It must be possible to incorporate experience and innovation from operating the systems and from 5G applications in 5G products.
Production			**2.4**	5G components do not have to be produced in Europe, as long as adequate access to the network elements is guaranteed for setting up the networks and the 5G communication components in devices/user systems.
	Raw materials			
		Access	1	No significance
		Processing --> Production sov.	1	No significance
	Components			
		Access	5	Access to parts must be warranted to set up own production. Network components must be reliably available from trustworthy production: functionality and performance capability, economic efficiency, quality, security (particularly in terms of cyber security) and delivery volumes. The same applies to 5G devices/modems for integration in user systems. Depending on the application, it may be beneficial to integrate 5G components and application components in special chips (example: IoT sensors).
		Own production --> Production sov.	3	May be necessary for devices, depending on the application. Otherwise, having access to finished network elements and devices/modems is what counts, and not the production itself.
	Production facilities / equipment			
		Access	2	Only relevant for network elements if it should be necessary to set up own production capacities (see below). In terms of highly integrated application devices (see above), the availability of suitable means of production can be prerequisite for ensuring that the products connected with 5G are competitive. To be assessed in the application context.
		--> Knowledge sovereignty	3	Knowledge is necessary in order to assess the situation and, if necessary, to plan and implement the measures involved in setting up own production capacity (geopolitical aspects).
	Operating production infrastructures			
		--> Operational sovereignty	2	Relevant only where own production is necessary (see above)

Operation (network operators, B2B)			**4.8**	
	Operational sovereignty		5	In order to use 5G systems, operation must be assured at all times by competent companies with trained, trustworthy personnel. This applies to the operators of public 5G networks and also to in-house networks in companies and public authorities, possibly with aaS components. Integrating operational experience in the further development of 5G and related research is a crucial element for upholding research sovereignty.
	Infrastructure sovereignty		5	There is a need for autonomous, sovereign mastery of setting up, expanding, operating and optimizing 5G network infrastructures, both on the part of the operators of public networks and on the part of organizations/companies involved in local firm/campus networks.
	Transparency sovereignty		5	Indispensable for acceptance. Confidence in the 5G systems, particularly in the network itself, plays a crucial role for society and for institutions/companies using the systems. Can 5G be trusted? Is data transfer via 5G tap-proof, non-corruptible? Is it protected from being shut down or falsified by external criminals, states, foreign companies etc.? Transparency along the 5G value chain is therefore essential for all stakeholders and players.
	Data sovereignty		5	Indispensable for the sovereignty of companies/organizations and for the country. A crucial factor, given the anticipated penetration of 5G. Encompasses all aspects of cyber security, particularly the security of data transferred with 5G and the safeguarded availability of the 5G systems (network and devices/modems) from possible sabotage.
	Platform sovereignty		4	5G networks will develop into platforms for a wide variety of digital B2B and B2C transactions. Sovereign development and operation of corresponding eco-systems is therefore important.
Usage (consumer / society)			**3.7**	
	Data sovereignty		4	Important for the sovereignty of companies/organizations and for the European Union. Even more relevant than today, given the anticipated penetration of 5G.
	Transparency sovereignty		4	Necessary for broad acceptance of 5G. Confidence in the 5G systems plays a major role for society and for individuals (see above): Can 5G be trusted? Is it tap-proof, non-corruptible? Is it protected from being shut down or falsified by external criminals, states, foreign companies etc.? Transparency is also essential in terms of radiation exposure from 5G, so that the expansion and operation of 5G systems is not hindered by unfounded protests.
	Media sovereignty		3	The public at large must have knowledge about competent use (see above).
Replacement			**3.0**	Specialist know-how, access to corresponding data/information and suitable degrees of freedom with regard to legal/contract issues will be necessary when migrating application systems that used previous

			communication technologies to the 5G systems The same will also apply in the distant future when 5G is migrated to 6G.

4.2.2 Example AI / data science (field of technology)

The following section takes a closer look at the field of technology “artificial intelligence” (AI) as another example. At the moment, AI is so hugely dynamic that it appears to have the character of a key technology as defined elsewhere. However, AI itself is already several decades old, while the technologies used in AI have changed dramatically over time. This field of technology is currently attracting great public and political attention. For example, autonomous systems are currently astounding the general public with their capabilities. Furthermore, demands are being made of the political sector to invest more in these technologies than in the past. Other countries are investing great amounts in corresponding research, and critical voices fear we may already have "missed the boat".

To take a closer look at AI, firstly it is necessary to define what it means. Under the overall heading of AI, machine learning (ML) is currently seen as having particular practical relevance. Machine learning means that machines are capable of autonomously detecting patterns in data, and learning how to assess and clarify new information building on the patterns, as well as how to develop new solutions. Deep learning (DL) refers to a special case within machine learning. This probably has the greatest practical relevance at present because these methods are already being used in a large number of applications. The application portfolio is constantly growing, and the methods involved in deep learning are getting more and more refined all the time. This paper therefore also treats deep learning as a key technology. In technical terms, deep learning is based on neural networks which can have very many layers in some cases (deep networks). However, there are a great many different network structures, rules for linking the neurons (nodes) and functional properties of the neurons. Convolutional neural networks (CNN) are currently being used as highly diverse, efficient network structures for classification tasks. For a neural network to analyze and classify input data, the network must be trained with corresponding pattern data. The data must adequately characterize the task being solved, and contain the events being classified with sufficient statistical relevance. It can be challenging when large volumes of classified data (labeled data) are needed for training.

In the context of machine learning, frequent use is also made of data analytics / data science. But the methods used in this field of science are only partly related to machine learning as such, as data analytics frequently uses classic mathematical, statistical procedures. The context is illustrated in Fig. 9. However, data analytics is highly significant in the context of deep learning so that this paper also attributes data science to the AI field of technology.

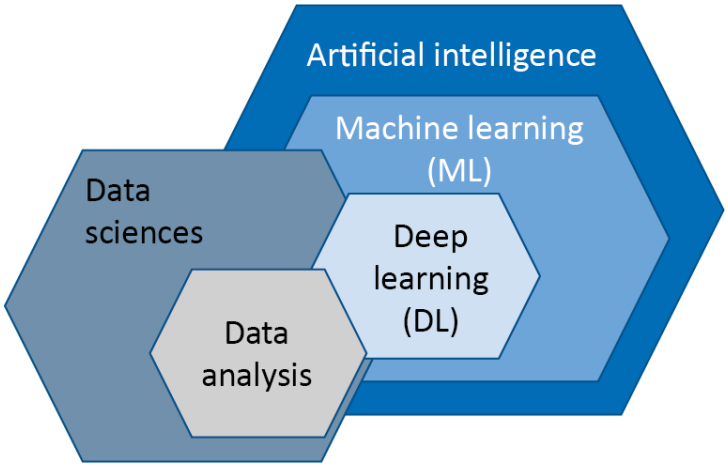


Fig. 9: Relationship between artificial intelligence and machine learning.

Data analytics is both prerequisite and an application for deep learning. Larger volumes of data have to be prepared for networks to be trained. On the other hand, neural networks can also be used to analyze large quantities of unstructured data (big data / smart data analytics). The technical concepts involved in deep learning find broader application today among others for analyzing usage data in order to predict future usage. Data analytics is also increasingly used to optimize processes (logistics, manufacturing, ...) on condition that operating data can be made available in sufficient quantity and quality.

Initially, machine learning (ML) or also deep learning (DL) just stands for an abstract algorithm that could also be called a tool box. The actual potential of these methods only emerges when applied to specific tasks. But not every neuronal network is equally suitable. The objective, requirements and framework conditions must be known and defined to make expedient use of this tool box. A suitable neural network can be developed and appropriate training devised once the specific framework conditions have been identified and defined. Specific domain knowledge is therefore indispensable for selecting and configuring a deep learning method /neural network. Which statements are expected as the result? Which input data and which training data are available? When developing a suitable network, it is necessary to understand exactly what the algorithms can and cannot do. CNNs for example can only reliably classify those events that are present in the training dataset with sufficient statistical relevance. The availability of comprehensive relevant training data is therefore crucial for the development and application of machine learning methods. Furthermore, the classification is only correct with a certain statistical probability. Under certain circumstances, false positive decisions made by machine learning can have serious consequences. The same also applies to the failure to recognize incidents or events, for example in the context of autonomous driving.

As an example of using the proposed methodology, AI is viewed as a field of technology for applications in the field of Industry 4.0 / automation. Examples of machine learning in the context of Industry 4.0 include:

- Process optimization
  - Analysis of process data with resulting optimization of production processes, for example
  - Adaptive control of complex machines, production lines
- Predictive maintenance
  - Analysis of operating data to ascertain when a part has to be maintained or replaced. A part is then only maintained or replaced if really necessary.
- Smart sensors, e.g.
  - Classification of parts directly in the camera
- Autonomous vehicles in logistics
- Image classification (near-human image processing)
  - For example during interaction between man and robot during joint installation.
- Smart tendering
  - For example, configuring complex machines with a high degree of flexibility (batch size 1)

The fact that this method can also make fundamental changes to the business principles is of considerable significance. Predictive maintenance is a striking example in this context, where sales of regular inspection and maintenance services no longer works when these methods are used. Platforms also change value chains. Increasingly, far more business relevance will be given to tendering services instead of machines. In the end, the technology involved in AI systems will also have to be optimized by quite conventional means under economical aspects.

The following section looks at the sovereignty requirements along the value chain for AI / deep learning from the point of view of industrial automation.

Value chain	Degree of necessary sovereignty	
Training / further training	**5.0**	Self-learning systems and machine learning / deep learning methods will soon be ubiquitous. Everyone will be confronted with them, directly or indirectly. To make professional use of such methods, comprehensive knowledge will be necessary about how they function and work and about the possible applications. The use of ML/DL methods is usually not obvious, so there will be a need to foster general acceptance for usage conventions and transparency in society at large. Training is particularly important in the engineering sector that has no natural intersection with AI.
Knowledge sovereignty	5	The technology can be neither used nor further developed without own knowledge. Nor is any appraisal possible without own knowledge.
Research	**5.0**	Both data science and AI methods are currently going through highly dynamic development. This is a topic with political significance as it is used as a competition attribute (China, USA). Europe has a wealth of domain knowledge in the engineering sector, while automation is also an important sector of the economy. This applies particularly also in interdisciplinary research projects that involve engineering, electrical engineering and IT for developing new concepts and solutions to safeguard competitiveness in the long term.
Knowledge sovereignty (see above)	5	No research is possible without comprehensive own knowledge.
Research sovereignty	5	Research in the general field of AI can only succeed with international sharing and exchange. The European research institutes therefore have to be large enough with sufficient research funding to keep pace with the major international facilities. It must be possible to take autonomous decisions about research contents (--> knowledge sovereignty). Access to sufficient training data is seen as being important, together with the possibility of influencing data type and quality.
Product development	**3.5**	AI facilitates the development of new products and services in the field of industrial automation. Only autonomous product development allows us to make use of (domain-)specific challenges when applying AI. Finding own solution paths boosts competitive capability. Using available AI methods to solve partial tasks makes economic sense.
Knowledge sovereignty (see above)	4	see above under Research
Development sovereignty	4	Basic application concepts (e.g. digital twin, predictive maintenance, man/machine interaction) are developed on the international level. It must be possible for us to proceed with autonomous (sovereign) adaptation to our own specific needs. Furthermore, there must be access to the latest development tools.
Production sovereignty	3	Functioning capability depends particularly on knowing about how hardware and software interact, e.g. in autonomous systems. A high degree of sovereignty is therefore necessary. This means for example having access to (AI) tools and (AI) components together with the ability to use these on a

			completely autonomous basis for on-going development towards the specific requirements.
	Operational sovereignty	3	The AI systems and SW tools necessary for development must be available, trustworthy and suitable for autonomous operation.
Production		**3.1**	This looks at the specifics in the context of using AI. Central significance is attributed both to having access to the development tools and data, and to the ability to make these work for a product/service. If AI systems are used as part of more complex systems (e.g. robots), the supplementary requirements for hardware production are also accompanied by the requirements resulting from the interaction between hardware and software.
	Raw materials		
	Access	4	Permanent, uncompromised, secure access to data is a specific aspect in the AI context.
	Processing --> Production sov.	1	The knowledge and ability to optimize and operate AI systems for applications (including controls, operating safety, ….)
	Components		Specific components include e.g. smart sensors with integrated AI-based preprocessing.
	Access	3	Access to such components is necessary: own production does not always necessarily make economic sense. However, autonomous use and operation must be possible.
	Own production --> Production sov.	2	see above
	Production facilities / equipment		
	Access	4	It is essential to have access to software development tools and to be able to use them autonomously.
	--> Knowledge sovereignty	4	
	Operating production infrastructures		Software operation is initially not a sovereignty problem. What matters is completely autonomous use of the software (no talk-back with the manufacturer).
	--> Operational sovereignty	4	
Operation (providers, B2B)		**4.0**	
	Operational sovereignty	3	The sovereignty requirements for operating AI systems depend greatly on the specific application. For example, they will be very high in the production of industrial goods, but less so in consumer products.
	Infrastructure sovereignty	3	see above

	Transparency sovereignty	5	The transparency of decisions plays a crucial role in the B2B setting. The basic information must therefore be accessible without having to go via third parties.
	Data sovereignty	5	Data plays a central role in AI, whether for training purposes or in analysis. At the same time, the datasets contain a great deal of specific knowledge (domain knowledge). Autonomous data generation and evaluation is therefore necessary.
	Platform sovereignty	4	AI systems can also be an (essential) part of platforms in the industrial setting, for conveying services, for example.
Usage (consumer / society)		**3.0**	
	Data sovereignty	4	Data sovereignty is very important for companies, and even vital for survival in some cases.
	Transparency sovereignty	4	Transparency is very important when it comes to generating acceptance for AI in the general public.
	Media sovereignty	1	Not really relevant in this context. However, when AI is used, media sovereignty is important for automatic verification of news sources.

5. EUREL's position

From an EUREL perspective it is important to establish sufficiently precise definitions for "technological sovereignty" and "field of technology" so that they are distinguished from other terms such as digital sovereignty. For EUREL, technological sovereignty expands much beyond digital sovereignty as it covers all fields of technology, including biotechnology, for example. There is not ONE technological sovereignty. Instead, the requirements with respect to technological sovereignty differ essentially depending on the position on the value chain. At the same time, it appears that there is no principle difference between the various fields of technology regarding the basic requirements within a stage of the value chain, but there definitely is a difference in the specific manifestation.

5.1 Requirements to achieve technological sovereignty

The following aspects emerge as the key elements for sovereignty regarding ICT and the related fields of technology:

- We need a high degree of "*knowledge sovereignty*" in all economically significant fields of technology, particularly in those fields of technology with high relevance in many application areas/sectors. This applies especially to ICT, AI, and microelectronics. Knowledge is the basic prerequisite for all subsequent action. Without knowledge sovereignty, no form of sovereign action is possible. Above all, this means early training in schools, universities, and also in apprenticeship vocations. Such training must also reach every single person. It is not just a case of social acceptance for the application based on the technology: it is also a case of generating interest in proper training for these technologies. Such training is prerequisite for being able to actually use the technology independently.
- A high degree of overarching sovereignty is also needed in research. On the one hand, we must be able to define our research topics autonomously, which demands corresponding knowledge. At the same time, the research must be adequately funded for us to proceed with research work in internationally relevant contexts and benchmarks. The complexity of present-day technologies demands close international research collaboration. But here too it is only possible to protect our own interests on the basis of our comprehensive own knowledge, e.g. with early patent applications.

- From EUREL's point of view, software plays a central role today in the development of products, including both development tools and software architectures. The tools define the scope of use and generate a dependency that extends into the application (take Android for example: the core functionalities of an Android smartphone are stipulated by Google). Developments in the field of AI-assisted autonomous systems demonstrate the key role played by software architectures. Development and production sovereignty thus demand a high degree of autonomy in software development. This is also the only way to protect security interests.
- No systems work anymore without microelectronics, a trend that will get even more pronounced when nearly all devices are connected in the IoT era. Capability for technological sovereignty regardless of the field of technology therefore demands the ability for sovereign action in the field of microelectronics. Besides the ability to develop corresponding systems, we also need to be able to build these systems in notable quantities. This in turn is associated with access to raw materials, development tools and machines together with the ability for sovereign use of these systems.

5.2 Measures for developing technological sovereignty

Based on the relevance of a field of technology and the identified degrees of sovereignty along the value chain, it is now possible to derive quite specific steps of action that have to be taken in individual fields in order to achieve the (desired/expected) sovereignty.

- Research funding faces the challenge of identifying relevant cross-sectoral fields of technology and potential key technologies at an early stage such that they can comprehensively funded and supported.
    - Cross-sectoral identification of relevant fields of technology and their key technologies should be supplemented with the proposed methodology.
    - In this context, mirroring today's process against the actual sovereignty requirements along the value chain helps to set the right points of emphasis.
    - At the same time, an effective way to assist with research funding could consist in setting up programs aimed at developing solution concepts for specific problems, regardless of a certain technology. This would promote the interdisciplinary approach.
    - Today we are seeing the emergence of increasingly complex systems where many fields of technology and domain knowledge from various sectors have a relevant role to play. Research programs should do more to encourage interdisciplinary cooperation in the development of systems.
    - One essential driver behind digitalization is the partly radical change in business models. This aspect has to be taken into account already in research projects.
- Standardization is closely related to research and development. Communication in particular does not work without standards. Active, coordinated involvement in defining international standards and specifications warrants on the one hand that certain desired functionalities are included, while on the other hand ensuring that many will then be able to produce and offer devices, infrastructures etc. to eliminate any isolated dependency. We need strategically aligned and politically supported standardization activities, particularly when it comes to ICT, software and AI. The USA and China are the driving forces here and dominate the capabilities of the systems.
- The ability to develop software is a necessary prerequisite for technological sovereignty. But targeted, efficient software development is not possible without specific application knowledge, domain knowledge. Research programs should therefore be designed to include the imparting and use of domain knowledge from other applications / sectors as an important aspect, particularly in ICT and software development. The ability to think in complex systems, to design and operate them is quite central, while at the same time including requirements and experience from use.
- Software training programs for engineers could be one expedient approach, as well as integrating computer science in specific technical development projects. This aspect should also be included accordingly in funding programs by the European Union. Start-ups often experience this symbiosis: due to their limited resources, the developers need both software expertise and domain knowledge.

- In the context of software development, sovereign acting capacity is also supported by open source communities. This counteracts problematic developments where companies put technologies on the market as so called “open standards”, whether e.g. Android or AI software. Withdrawing access can substantially limit the ability to act (cf. Google Apps with Huawei). Publishing the source code in these communities also helps to prevent or better identify security loopholes.
- There is a principle contradiction between data protection and the need to evaluate data with the greatest possible diversity. New concepts should therefore be developed that do not focus on the central acquisition and processing of as many data as possible. Local processing of data is also possible, given the performance of modern computers (e.g. smart phones) and communication infrastructures (e.g. edge computing). All that is needed is to provide uniform regulations respectively evaluation logics. Broader social acceptance with fewer reservations about application in industry (competition) would expand data availability while making systems more robust at the same time.
- Giving a third-party insight into digital data automatically entails transferring the data to the third party, giving them actually more than just an insight. The data ought to be able to self-destruct after being revealed to the third party, e.g. by means of a one-time key.
- Social acceptance of technical systems must be enhanced. Society at large tends to be ambivalent about technology: while taking the use of smartphones for example for granted, on the other hand people are less willing to take a more in-depth look at the technical elements.
    - On the user side, trustworthiness must be enhanced by transparency. People must be able to understand what a technical system does.
    - With the growing number of AI based systems it becomes absolutely essential that the reasons for decisions are made transparent and interpretable.
    - In terms of training, it is important to convey that we can only retain our room to maneuver for economy and society if we play an active role in crafting technical systems.
- Processes are needed for testing and monitoring the trustworthiness of infrastructures (devices, hardware, software, services). Corresponding research programs should be created e.g. for developing methods and (software) solutions for validating system trustworthiness.
- Technical systems must function reliably and be easy and transparent to operate.
    - Among others, this needs a greater awareness that everyone must be able to use technology,
    - an enhanced role for standardization in warranting interoperability and
    - intuitively usable interfaces to technical systems.
- Particularly where long-lasting infrastructures are concerned, we need access to knowledge and spare parts for long-term maintenance. Software is particularly the case here, where the source code of critical units has to be stored in a kind of "escrow memory".
- When investing in school education, the focus should be not just on applications (digital classroom) but also on the basic principles of ICT including software development / programming. There are some very good, isolated examples of schools that use the learning-by-playing approach to trigger an interest in technology and also in physics. The technical prerequisites can be fulfilled already today at low cost (e.g. Raspberry PI). What is missing are suitably trained teachers and the possibility of bringing interested outside experts (e.g. committed engineers) into schools for this kind of training. Mentoring schemes with universities or companies can also have a conducive effect.

5.3 Technological sovereignty in the broader (political) context

Technological sovereignty is embedded in a broader context that includes resilience and sustainability. In some areas, technologies have become essentially significant for Europe as a business location and for social cohesion. ICT is one such technology.

- Particularly the cross-sectoral significance of ICT indicates that today it is more urgent than ever for us to think in systems that encompass different fields of technology and sectors. This understanding should develop from within the sectors. But experience shows that it is very difficult for a certain sector to develop an understanding

for the specific aspects of another sector. Politics can play a facilitating role here and bring the different sectors together. Discussions of specific issues, help to develop cross-sectoral understanding.

- This paper focuses on the presentation of a methodology, supplemented by exemplary indicative assessments for the purpose of explanation. In a first step, selected cross-sectoral initiatives should produce empirical analyses of the most important fields of technology and key technologies. The methodology presented here could be used to compare the required and the actual status obtained in an assessment of technological sovereignty, using the Delphi method, for example. The most urgent aspects could then be precisely identified, and corresponding measures proposed.
- Technological sovereignty includes the ability to build and operate robust infrastructures, with individual components continuing to operate reliably even when faults occur. Safeguarding resilience is an overarching requirement which must be warranted on the political level in view of the resulting sovereignty requirements for different sectors, fields of technology and value creation stages.
- In this context it is crucial to also keep an eye on software development. No infrastructure can be operated and used, no logistics work and no production functions properly without the ability to develop and operate own software with modern development tools and software architectures.
- Access to resources is another basic prerequisite for sovereign action. Current trade disputes already show that raising customs duties impedes access not to just to raw materials but also to essential components of devices. ICT is particularly susceptible in this respect due to the many components that can only be purchased from international companies. At the same time, ICT is relevant for a nearly all branches and constitutes a critical infrastructure for public life in general. Here we're talking not just about raw materials or specific components and products, such as routers, memory devices, computers, and chips but also about access to software tools, algorithms and data. It is therefore suggested that the requirements for sovereign action should be aggregated on the political level with a political warranty for access to the necessary resources (making them available on the national /EU level or delivery possibilities from different parts of the world).
- Warranting the energy supply is another aspect. Internationally connected energy systems are vulnerable with grid disruptions having a cross-border impact. Reliable ICT is needed to manage the local energy systems that are meanwhile typical features of regenerative energy sources. On the other hand, a robust, reliable, and adequate energy supply is prerequisite for fully functional ICT. A specific aspect in this context is access to raw materials for making batteries.

6. Conclusions

European Union and its member states must recognize and accept that the geopolitical setting in which our societies and economies are embedded is increasingly being shaped by a return to national and European Union interests, respectively. Technological dependencies are turned into political instruments; in some cases, technological dominance is even declared to be a political and national objective. If technological sovereignty is defined as the ability of a state to implement its political and social objectives without being hindered by the non-availability of or lacking access to special technologies, then this results directly in the demand to take a systematic look at the whole issue of technological sovereignty.

This position paper takes a detailed look at the concept and basic dependencies of technological sovereignty. Among others, it seeks to trigger more intensive discussion about how we in Germany want to proceed in terms of sovereign development and use of technology.

To this end, it proposes a systematic approach for identifying fields of technology, together with criteria for assessing the fields of technology. Sovereignty itself is defined and a systematic approach is suggested for putting the meaning of sovereignty into more specific terms for individual players along the value chain. This is illustrated with two examples: 5G and AI in automation.

The paper wants to trigger a process that uses defined criteria to identify both relevant fields of technology and the actual associated key technologies. Possible criteria were identified in the paper. As far as possible, the process should include various players from different sectors of the market. The aim is to identify where special efforts are needed on

the national and European level to obtain or restore technological sovereignty, with the specific requirements for technological sovereignty and the degree to which it should be achieved being defined in the course of the process. The need for a cross-sectoral, politically managed process is revealed by the fact that many different technologies are used in ICT with corresponding sovereignty requirements, and that ICT has become an indispensable, integral part of the technical systems in other sectors.

Although the systematic approach was developed from the point of view of electrical engineering/ICT, the paper aims to contribute to a more standard, cross-sectoral systematic approach so that those responsible for taking decisions in politics and the economy can identify fields of technology, derive the sovereignty needed for these fields and implement it accordingly in both political and economic measures.

List of references

Bau15 Baums, A. Technologische Souveränität: Strategie oder PR-Hype. Oktober 2015. von www.digitale-standortpolitik.de abgerufen.

Bit15 Digitale Souveränität: Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. Berlin. BITKOM e.V. 2015

Bit19 Digitale Souveränität: Anforderungen an Technologien- und Kompetenzfelder mit Schlüsselfunktionen. Berlin. BITKOM e.V. Dezember 2019

CP00 Technologische Vielfalt im Überblick. Vom Clusterportal Baden-Württemberg: https://www.clusterportal-bw.de/clusterdaten/technologiefelder abgerufen.

Dew17 von Dewitz, W. (Juni 2017). Warum Bosch so viel wie nie in eine Fabrik investiert. manager magazin. Juni 2017. Von https://www.manager-magazin.de/digitales/it/bosch-baut-chipfabrik-milliarden-investition-in-dresden-a-1152881-3.html abgerufen.

Eng00 Engelhard, J. Branche. Von Gabler Wirtschaftslexikon: https://wirtschaftslexikon.gabler.de/definition/branche-27701 abgerufen.

GER1 "Together for Europe's recovery" Programme for Germany's Presidency of the Council of the European Union1 July to 31 December 2020; https://www.eu2020.de/blob/2360248/e0312c50f910931819ab67f630d15b2f/06-30-pdf-programm-en-data.pdf

GK16 Gausemeier, J., & Klocke, F. Industrie 4.0 – Internationaler Benchmark, Zukunftsoptionen und Handlungsempfehlungen für die Produktionsforschung. Heinz Nixdorf Institut, Universität Paderborn, Werkzeugmaschinenlabor der Rheinisch-Westfälischen Technischen Hochschule Aachen. 2016.

Han19 Hua, S. China will ausländische Computer und Software aus seinen Behörden verbannen. Handelsblatt. 9.12.2019.

Keu18 Keupen, R. Die Bank als Plattform braucht ein Mindestmaß an technologischer Souveränität und Unterstützung. IT-Finanzmagazin. Oktober 2018.

MR15 Machnig, M., & Rohleder, B. Leitplanken Digitaler Souveränität. Nationaler IT-Gipfel. (BMWi, Hrsg.) Berlin. 2015.

Mai15 Mair, S. Sicherheit durch technologische Souveränität. (BDI, Hrsg.). 2015.

MRB18 Müller-Quade, J., Reussner, R., & Beyerer, J. Karlsruher Thesen zur Digitalen Souveränität Europas. Datenschutz und Datensicherheit, 42(5), 277−280. Springer Fachmedien. Mai 2018.

NCA18 Nationales Cyber-Abwehrzentrum. Gefährungslage der Stromversorgung in Deutschland durch Cyberangriffe. 2018.

OEC07 OECD (Hrsg.). Revised Science and Technology Classification in the Frascati Manual. Februar 207. Von http://www.oecd.org/science/inno/38235147.pdf abgerufen.

Wet16 Wetzel, D. So fatal wäre ein Cyberangriff auf die globale Stromversorgung. Die Welt. 29. 09 2016. Von Wirtschaft: https://www.welt.de/wirtschaft/article158440599/So-fatal-waere-ein-Cyberangriff-auf-die-globale-Stromversorgung.html abgerufen.

Wik19a Schlüsseltechnologie. November 2019. Von Wikipedia: https://de.wikipedia.org/wiki/Schlüsseltechnologie abgerufen.

Wik19b Technological Readiness Level. Mai 2019. Von Wikipedia: https://en.wikipedia.org/wiki/Technology_readiness_level.

Wik20 Technological Souveränität. April 2021. Von Wikipdia: https://en.wikipedia.org/wiki/Technological_sovereignty#cite_note-techinfosov-1 .

Zim07 Zimmermann, K. (2007). Technologieklassifikationen und –indikatoren. Techn. Univ. Chemnitz. 2007. Von https://nbn-resolving.org/urn:nbn:de:swb:ch1-200701448 abgerufen.

ZVEI15 Diskussionspapier − Digitale Souveränität. ZVEI (Hrsg.). Juni 2015.

ANNEX

A. Technical Societies

a. VDE
- Information Technology Society (ITG)
- Power Engineering Society (ETG)
- German Society for Biomedical Engineering (DGBMT)
- GMM → VDI/VDE Society of Microelectronics, Microsystems and Precision Engineering
- GMA → VDI/VDE Society for Measurement and Automatic Control

b. GI
- Operating Systems, Communication Systems and distributed systems (SYS)
- Databases and Information Systems (DBIS)
- Graphic Data Processing (GDV)
- Informatics Basics (GInf)
- Informatics in Law and Public Administration (RVI)
- Informatics in the Life Sciences (ILW)
- Informatics and Training / Didactics of Informatics (IAD)
- informatics and Society (IUG)
- Artificial Intelligence (KI)
- Human/computer interaction (MCI)
- Security − Protection and Reliability (SICHERHEIT)
- Software technology (SWT)
- Technical Informatics (TI)
- Business Informatics (WI)

c. VDI
- Construction and Building Services
- Energy and Environment
- Vehicle and Traffic Engineering
- Materials Engineering
- Measurement and Automation Technology
- Microelectronics, Microsystems and Precision Engineering
- Product and Process Design
- Production and Logistics
- Technologies of Life Science (e.g. Bionics)
- Process Technology and Chemical Engineering

B. Sector Classifications

a. BMWI
- Automotive Engineering
- Rail Industry
- Construction Industry
- Mining and Raw Materials
- Education Industry
- Biotech Industry
- Chemistry and Pharmacy
- Electrical Engineering and Electronics Industry
- Energy Supply
- Fine Ceramics Industry
- Precision Mechanics and Optics
- Freelance Professions

- Healthcare Industry
- Rubber
- Trade
- Wood and Furniture Industry
- Information Technology and Telecommunication
- Financial Services and Insurance
- Culture and Creative Industry
- Food Industry
- Leather Industry
- Leather Goods Industry
- Aviation and Aerospace
- Maritime Industry
- Engineering
- Paper and Printing
- Care Industry
- Postal Services
- Show Industry
- Security and Defense Industry
- Sport Industry
- Steel and Metal
- Textile and Clothing
- Water Industry
- Cycle Industry

b. Statista

- Agriculture
- Construction
- Chemistry & Raw materials
- Services and Skilled Crafts
- E-Commerce & Mail Order Business
- Energy & Environment
- Financial Services, Insurance, Real Estate
- Leisure
- Society
- Trade
- Internet [Apps, Usage]
- Consumer Goods & FMCG

- Countries
- Life
- Media & Marketing
- Metal & Electronics
  - Electrical Industry
  - Precision Mechanics & Optics
  - Vehicle Engineering
  - Aviation & Aerospace
  - Engineering
  - Metal Industry
  - Rail Vehicle Construction
  - Shipbuilding
- Pharmacy & Health
- Technology & Telecommunication
  - Television Reception
  - Landline & Cell Phone
  - Hardware
  - Household Appliances
  - IT Services
  - Software
  - Consumer Electronics
- Tourism & Hospitality
- Transport & Logistics
- Management & Defense
- Economics & Politics