COMMISSIONED BY

Federal Ministry
of Education
and Research

THE FUTURE OF TRUST IN DIGITAL WORLDS

Study (abridged version)

Authors:
Anna Hornik
Dr Christian Grünwald
Daniel Bonin
Jan Reichert
Marie-Kristin Komendzinski
Julian Sachs
Holger Glockner
Michael Astor

October 2022

This publication is a translated version of the study: Prognos AG; Z_punkt GmbH The Foresight Company (2022). Die Zukunft des Vertrauens in digitalen Welten. It was translated by Agentur Tranzzlate GmbH.

The authors are responsible for the content. The Federal Ministry of Education and Research (BMBF) does not guarantee the correctness, accuracy or completeness of the information. Views and opinions expressed in this publication do not necessarily reflect those of the BMBF. Furthermore, the scenarios outlined in the study should neither be considered as forecasts, nor do they necessarily represent desirable visions of the future for the federal government or the Future Office of the BMBF.

This publication was produced as part of the service contract "Future Office of the Foresight Process (Foresight III)" of Prognos AG and Z_punkt GmbH on behalf of the BMBF, Department – Strategic Foresight; Participation; Social Innovation.

Table of Contents

List of figures

Executive Summary

Objective and structure of the study

The study "The future of trust in digital worlds" sheds light on the potential importance of trust for social interactions in an increasingly digital world, and also reflects on possible consequential changes of trust-based actions in the digital environment. It first examines the phenomenon of "trust" and investigates the extent to which known mechanisms for building trust are transferable to the digital environment. Various development paths in a digital domain of tomorrow are described in parallel. Six future spotlights illustrate the different forms in possible everyday situations.

This essay is an abridged version of the study and provides insight into the future of trust in digital worlds with two of six future spotlights. The full version of the study with the remaining future spotlights, further details regarding the results and the methodology that was used is available for download at vorausschau.de (German version only).

Why do we need trust in the digital environment?

Trust is essential for interactions in complex social contexts. Trust allows us to make decisions about interactions with others, notwithstanding a lack of control or predictability of a situation, and therefore makes us able to act.

Three factors in particular contribute to the need to think of trust in the digital environment differently to direct interactions:

- Rapid technological change and the use of new technological advancements make it more difficult for individuals to accumulate reliable empirical values about new forms of interaction. This also makes it harder to form heuristics to serve as the basis for assessing the trustworthiness of a counterpart. Sets of criteria for evaluating whether to trust in a situation need to be constantly reviewed or adapted to changed surrounding conditions.
- Interactions in digital environments always occur with technology as an intermediary. This makes situations more complex: not only does the trustworthiness of the interaction partner have to be evaluated; the extent to which the operators of the technology infrastructure that is being used are trustworthy is also relevant for evaluating the situation as a whole.
- A stable system of laws and sanctions establishes certainty in a number of situations that would otherwise be based solely on trust. Due to continuous change in the digital space and its transnational nature, legal regulation would have to take place at a global level. To date, corresponding authorities for decision-making, coordination and law enforcement are lacking.

What is trust?

Trust is generally defined as a positive expectation regarding the future actions of a counterpart. On the one hand, trust depends on personal experiences, the overall assessment of the situation and the individual tendency to trust. On the other hand, the perception of the counterpart is decisive: important factors are how competent, upright and benevolent the counterpart is perceived to be.

Trust in technology

According to today's scientific understanding, trust-based decisions always depend on the assumed intention of the counterpart. Since technology has no will of its own, one can neither trust nor distrust it – but one can trust or distrust those who built a technological device or developed software.

Two future developments could soften the existing differentiation between trust and related concepts (such as relying on something or someone):

- Increasingly anthropomorphic technology – in terms of language, appearance and feel – could make it impossible for individuals to discern whether they are interacting with a person or with software. Whether one "trusts" when ascribing will to a counterpart that does not have it remains debatable from today's perspective.
- Meanwhile, assistance systems support human decisions in many situations. Some AI algorithms that are used in this context "learn" to make decisions themselves and are not comprehensible – or only to a limited extent – even for the programmers. Here too, the question is whether one "trusts" AI in these situations.

In what kind of digital worlds will we place our trust tomorrow?

The study assumes that the interactions of technologies such as AI, intelligent sensors, AR, VR and the like will largely blur the boundaries between the physical and online worlds. A spatial web – also called Web 3.0[1] or metaverse – is emerging.[2] New forms of interaction appear in a spatial web – for example, when avatars communicate with each other – and, where applicable, lead to new patterns and forms of building trust.

Trust, risk assessment and security in the digital worlds of tomorrow

Whether and to what extent we trust is determined among other things by the assessment of the individual risk that the trust that is given will be abused. This assessment is often distorted in digital space. Threats are over- or underestimated depending on the state of knowledge. In future digital worlds, risks could however be perceived as more real, also because they have a greater impact in the offline world due to their spatial display formats. Moreover, the decision to use a service and the trustworthiness of the operator have in part become disconnected. Online services are used even though the operators are not trusted.

Network effects can lead to reservations being suppressed: once the number of users exceeds a critical mass, the benefits appear to outweigh the risks.

Digital infrastructures are increasingly replacing their precursors, making it more and more difficult to withdraw from them, regardless of the risks associated with them.

Digitisation raises the question of trust in communication and interaction anew. New abilities, cultural technologies or authorities for the verification of content but also authenticity and therefore trust in our counterpart are needed.

1 Here the term Web 3.0 must be differentiated from Web3, which has been discussed increasingly since 2021. See Section 1, page 6 for a more exact definition.

2 The concrete form of a spatial web as promoted by Mark Zuckerberg with the metaverse is only one possible form that could be assumed by the future digital/analogue world.

1 WHY DO WE NEED TRUST IN THE DIGITAL ENVIRONMENT?

Without any trust, people would not be able to get out of bed in the morning. It is with this thought that the sociologist Niklas Luhmann introduces his well-known essay on trust.[3] The idea behind this statement is that social interactions in a society are too complex to be understood in their entirety, let alone controlled. Nobody can constantly check whether their social environment is deceiving them, whether houses are built so they will not collapse on top of them, whether fellow human beings are abiding by general rules and laws so they do not have to fear being robbed in the street. Trust is able to reduce the complexity of the environment and social interactions to an acceptable level, making us capable of acting and living despite considerable uncertainty.

Trust opens up courses of action without having to invest resources in control. In the economy, trust is therefore commonly viewed as a "lubricant," for example, allowing us to make buying decisions when the quality of a product cannot be checked in detail.[4] There are a number of phenomena at the overall societal level suggesting that trust is good for society as a whole. Countries with higher levels of trust also have higher economic growth, more innovations and healthier, more educated people.[5]

Beyond the findings in economics, trust on a small scale enables social networks and trust on a larger scale ensures social cohesion – and therefore shapes social togetherness. In the course of "the legacy study" Jutta Allmendinger reaches the conclusion that societal cohesion is crumbling. With her colleague Jan Wetzel, she ascribes dwindling social cohesion to a lack of trust: "In many areas, our ability to deal with major changes and to shape them depends on whether we trust others."[6] One of these

3 Luhmann, N. (2014).

4 Speck, U. (2020).

5 Zak, P. J.; Knack, S. (2001), Beugelsdijk, S.; Smulders, S. (2009), Cardenas, J. C.; Carpenter, J. (2008), Dincer, O. C.; Uslaner, E. M. (2010).

6 Allmendinger, J.; Wetzel, J. (2020), p. 111.

major changes has been ongoing for quite some time – it has already defined our interactions and will keep doing so in the future: the digital transformation, the interconnectedness of data, people and things. The convergence of what we know as the "analogue world" and what we differentiate from it today as digital or virtual. How can we deal with this major change? Is trust merely a prerequisite for dealing with change – or will trust as such become the object of change?

The omnipresence of the internet and the fusion of technical systems with the "real" world are lastingly changing social interaction. At the latest due to the worldwide spread of smartphones and social media, the importance of the digital world and the number of users increased to such an extent that withdrawing from digital infrastructures became next to impossible. The digital domain became a permanent part of daily life. Temporary "dial-on-demand" became "always on". Not being part of that means being excluded from many things. The economy, society and politics are increasingly aligning themselves with digital infrastructures. This raises the question of whether and how trust is changing in these new digital interactions. Do the familiar heuristics used in analogue interactions continue to apply in order to decide whether to trust one's counterpart, or do we need to develop new strategies? Technological transformations are always associated with social latencies. With reference to Clay Shirky it could be said that communication tools only become interesting socially by the time they become technologically boring.[7] We always feel the social effects of technological innovations with a time delay, once the technology is in widespread use. New technologies often serve and intensify social change processes that are already in progress[8] – for example, the transformation from the industrial to the knowledge society was accelerated and intensified by digitisation.

While the internet is long since past being a new technology, many social effects of this far-reaching innovation are only now being seen. Cyberspace exhibits two fundamental differences compared to analogue/physical space, which in turn significantly define trust building processes in the digital domain.

The first difference is that the internet and many of the technologies emerging from it were at first largely unregulated and in part remain so. Regulation was initially difficult because the applicability of existing tools to the internet was limited. Much in cyberspace was simply new legal territory. In addition, the challenge of nation states – whose regulatory authority largely ends at their borders – regulating global, cross-border networking technology remains.

The second difference in the early phase of the digital domain resulted from a few "internet experts" versus a large majority of "internet beginners" who did not understand how the technology works – and still do not today.

This knowledge imbalance also results in an unequal distribution of trust. Neither individual nor collective empirical values exist when new, unknown spaces open up. A reciprocity of trust – the better people know the objects and subjects of trust, the better they are able to assess behaviour – is not given in such spaces. Empirical values are formed in new environments by trial and naturally also by error. In this context, trust as defined by Niklas Luhmann has a disproportionately greater impact as a means to reduce social complexity, because movement in an intangible (incomprehensible) domain only becomes possible in the first place through an enormous advance of trust.[9]

In this collective learning process interaction patterns solidify – including trust building patterns. Meanwhile the consensus seems to be that the cyber-utopian dreams of the internet pioneers have not come true, even though they are attempting to continue dreaming the dream in real political dimensions.[10] Put another way: the belief in the self-regulating power of the online world was considerably shaken, notwithstanding many positive effects of the digital world. Trust in technology companies is low. More than one quarter of consumers around the world have little or no trust in the digital giants.[11] New phenomena such as the platform economy, bots, cybercrime, fake news and shitstorms have altered the public perception of the digital domain. Calls for comprehensive regulation, especially of social media, are getting louder year

7 Shirky, C. (2008), p. 105.
8 Stalder, F. (2016), p. 21f.
9 Luhmann, N. (2014).
10 Contract for the Web (2019).
11 Fleishmanhillard (2020).

after year.[12] Some are of the opinion that a public network can only be maintained over the long term with stricter regulation.[13]

Dynamic developments of technologies such as augmented, mixed or virtual reality, blockchain or holograms, the increasing use of virtual assistance systems, progress with machine learning and game changers visible on the distant horizon, such as quantum computing,[14] support the assumption that digital domains will be defined by highly dynamic development over the coming ten to fifteen years.

So what might trust in digital domains look like in the future? This question can only be answered in two stages. The first step is to work out how and on what levels trust is built. In the second step, this needs to be compared to the knowledge of how digital domains may develop. Specifically: What might a Web 3.0 look like? What technologies and convergences could define it? What could possible interactions between people, and between people and technology, look like in this further developed digital or hybrid domain?

In the interest of defining terms, note that "Web 3.0" in this study stands for a further development of the internet into a ubiquitous, semantic web defined by spatial 3D components with high-performance data-linking by AI systems. "Spatial web" is an alternative, equivalent term, but rarely turns up in the debates. "Web 3.0" must be differentiated from "Web3," which defines the further development of the internet in much narrower terms, striving for a decentralised web based on distributed ledger technologies, non-fungible tokens (NFTs) and cryptocurrencies. However, these similar-sounding terms are often mixed up in the media.[15]

To make interactions visible, the alternative digital futures will be embedded in social scenarios. Therefore, this study builds possible futures of the digital world based on the surrounding conditions of the scenarios from the study "The future of values held by people in our country".[16] To make these abstract futures tangible, the scenarios were made perceptible as "everyday stories" of a future persona (Lana, 38, German blogger) and enriched with "future artefacts".[17]

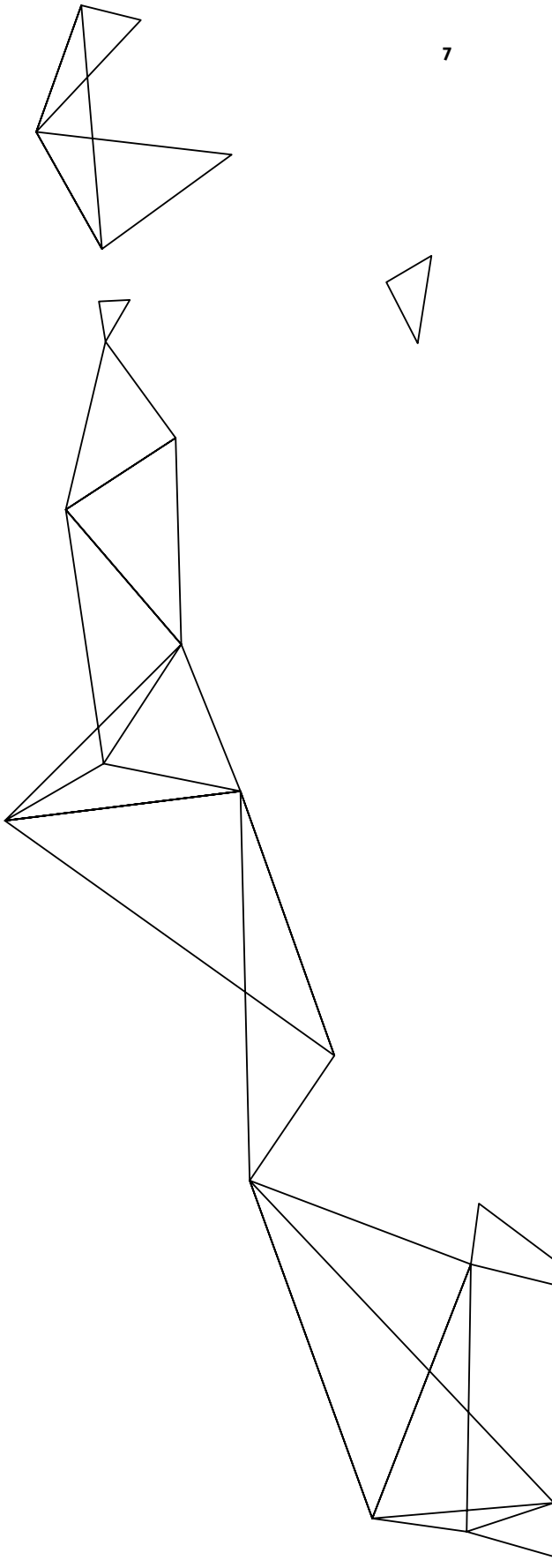
The study "The future of trust in digital worlds" looks ahead up to 15 years into the 2030s. This essay summarises the key concepts, insights and findings of the overall study.[18] It is based on the theory that the digital domain 15 years from now will be as different to today's digital domain as today's digital domain is to the digital domain of 15 years ago. This means that trust building processes will also be redefined. Cyberspace and possible convergences of the relevant, underlying technologies are thus explored in forward-looking, alternative visions of the future in order to derive the future of building trust.

It is also important to disassociate from the current debates of 2021 (for example, regarding fake news or the debate culture in social media) and to embed the evolution of existing germ cells, trends and weak signals in possible futures. Some visions of the future for 2035 may seem like science fiction in 2021, especially against the background of the recent debate regarding the internet's further development to become a metaverse.[19] However, a retrospective analysis of development leaps in the digital domain since 2006 shows that much of what constitutes today's normality was difficult to imagine then. For a retrospective placement of past dynamics, Facebook was founded in 2004, the market launch of the first iPhone was in 2007, WhatsApp only came to market two years after that.

Therefore, "Any useful idea about the future should appear to be ridiculous."[20] This is because new technologies enable new behaviours and call old convictions into question. Much of what will be characteristic for the future is new and challenging at first in the current discourse. At first it typically appears obscene, impossible, illogical and sometimes even grotesque. Yet it ultimately becomes familiar and finally "normal" – and thus to a certain extent also mundane in the public perception. What is often viewed as the "most likely future" today is one of the least likely futures on closer examination.[21] No mat-

12 Pörksen, B. (2021); Süddeutsche Zeitung (2021).
13 Rudelle, J. (2019).
14 BMBF (2020).
15 CNN (2022).
16 Prognos AG; Z_punkt GmbH The Foresight Company (2020b).
17 Schaich, A.; Neef, A. (undated), Peter, S. et al. (2020).
18 The study can be downloaded free of charge from www.vorausschau.de.
19 Merten, M. (2021).
20 Jim Dator's "second law of the future," familiar in future research. Dator, J. (undated).
21 Dator, J. (undated).

ter what the future of the digital domain will look like, trust building as an implicit social mechanism will adapt to the changed environmental conditions. Determining the future of trust in a digital world therefore first requires a closer definition of the term "trust," especially considering its downright inflationary use in the public discourse.



Note on the full version of this study

A comprehensive account of factors influencing the trust of tomorrow is found in the full version of the study, Sections 2.4 and 2.5. The full version of the study can be downloaded on the website vorausschau.de (German version only).

Everyday story from the future
Future spotlight "The European Way"

Thursday, 17 May 2035.

6:15 am. "I'm walking on sunshine…" Like every morning, the EU-certified assistance system PAT – short for Personal Assistant Technology – plays Lana's favourite wake-up playlist. With 4.8 out of 5 points, PAT is the virtual assistance system with the highest anti-bias rating of the EADA (European Algorithmic Debiasing Agency) that is currently available. For some time, companies have only been allowed to use assistance systems in their human resources departments with a minimum score of 4.65.

Lana, still quite tired, mumbles, "PAT, any messages?" The music stops and PAT answers, "Lana, you have two new voice/image messages". The ultra-thin, seemingly transparent smart card on Lana's bedside table vertically projects a three-dimensional, speaking hologram. It is the image of her husband João, currently visiting her in-laws in Portugal with their four-year-old son Luis. "Bom dia, Querida…" Lana loves being greeted by the hologram in the morning when João is not at home. Apparently he was just screening the news feed, since he talks excitedly about a promising research project in the European Cluster of Excellence at the university in his home town of Coimbra, where stroke patients will be treated using non-invasive brain-to-brain interfaces between healthy family members and affected individuals. João loves exciting research projects. "My little nerd…," Lana thinks. When João's message ends, his hologram disappears into the smart card. Most people in the EU use the smart cards as a multi-communication tool, but also as a means of payment, digital vaccination certificate and digital identity card. A classic all-in-one device, in other words. At this point just about all her friends are using the smart card exclusively. "It's hard to believe how cumbersome the old smartphones were," Lana thinks. Market approval for a smart card requires all data to be stored exclusively on servers located and certified in the EU.

Another hologram appears with a new message. It's from Jan, her Belgian fellow blogger from Antwerp. He and Lana are part of an investigative European blogger network that provides mutual research support. The group also meets on social media, for instance in the Web 3.0 network EUTOPIA, where they have set up their own virtual editorial room in Brussels for their avatars. After the Chinese and US networks massively lost ground in Europe as a consequence of data protection scandals, the French platform EUTOPIA is considered the new virtual place to be, at least in the European Union. The plattform uses an efficient ai-bases identification system of hate speech and cyber or avatar mobbing, allowing victims to make a report quickly. This made a big contribution to EUTOPIA's reputation as a "nice network". A friend and virtual interior designer did the interior decorating for the group. Lana and Jan are currently working together on a story about deep fake real image avatars. These deep fakes appear so real that even experienced cyber forensic experts can only identify them in social media after numerous, AI-assisted validation processes.

Since Jan's message is in Flemish, Lana gives the voice command for real-time translation: "PAT, please translate to German." The message is played back in German. This is done using the deep-learning-based, real-time translation system EUROtranslate developed by a group of European universities. This tool has also supported the emergence of a European public. When EUROtranslate was launched in 2027, the translations for some official languages were still quite rough. But thanks to extensive use – and a corresponding high volume of training data – even the Maltese version is now at a high level. Jan talks about his research on the latest identify fraud cases with hacked real image avatars. The avatars of the unsuspecting owners shopped online for luxury goods in the high five figures at the virtual twins of Munich's upscale stores on the Maximilianstraße. Since even the mandatory three-factor authentication required by the EU was successfully circumvented, the culprits must have had access to all of the victims' data. Lana thinks that the smart cards of the affected real image avatars were probably hacked. Or they had access to the voice samples. In any case, Jan reports that Europol is

warning against prematurely blaming cyber mercenaries from Central Asia. As Jan talks, Lana briefly wonders if that is in fact the "real" Jan whose hologram is currently speaking to her. She smiles and quickly dismisses the thought. Calls for decentralised, multi-stage identify verification in the digital space will likely get louder again, thinks Lana. The EU Parliament's Cyber Security Committee has been requesting this for years, but was unable to implement it so far. Sceptics are defending central data capture and fear a "new bureaucratic monster".

"PAT, turn on the coffee machine," Lana calls from the bathroom and her Italian portafilter machine immediately starts to heat up. Still a bit tired, Lana goes into the kitchen. She puts on her smart glasses and an iris scan enables her individual virtual assistance system. She reaches for her smart card. The assistance system PAT knows that Lana peruses the leading European media every morning over coffee. The European Center for Political Education provides bundled, relevant EU media content in all common languages each morning. Today PAT recommends articles in the Danish "Politiken," the Spanish "El Pais" and a short report by a Slovakian video blogger living in Toulouse on allegations of corruption during the construction of new water harvesting plants in southern France, among other things.

Just then, Lana remembers that she urgently needs to contact a potentially sensitive source for her report. The clock on her smart card reads 7:52 am. "Screen and keyboard," she commands, and the smart glasses turn her field of vision into a transparent screen while the smart card horizontally projects a keyboard onto the tabletop. She starts typing, but stops again directly. Lana recalls that the source – unlike herself – views digital communication as fundamentally insecure. Normally she offers to use the multi-stage NGO verification tool TRUST in such cases, which specifically omits the use of government interfaces for verification. But in this case, the distrust appears so great that it probably wouldn't be a good idea to write a message right now, even if it is double encrypted. So she goes to the cabinet, gets paper and an envelope, and starts writing a letter with her recycled ballpoint pen...

New patterns of interaction and elements of trust and distrust building in the future spotlight "The European Way"

New patterns of interaction	› Virtual assistance systems are extremely widespread; using them is even more normal than already today › Communication with holograms serving as communicative transmitters between people is commonplace › Spatial social media forums that can be experienced in three dimensions › Day-to-day interactions with real image avatars › Smart card as the new personal data storage tool
Trust building elements	› Anti-bias assessment of the EADA (European Algorithmic Debi-asing Agency) › Three-factor authentication › AI-based hate speech identification in social medium EUTOPIA › voice samples and other biometric security methods
Distrust building elements	› Deep fake real image avatars › Avatar mobbing and hate speech

Source: © own illustration by Prognos AG and Z_punkt 2021.

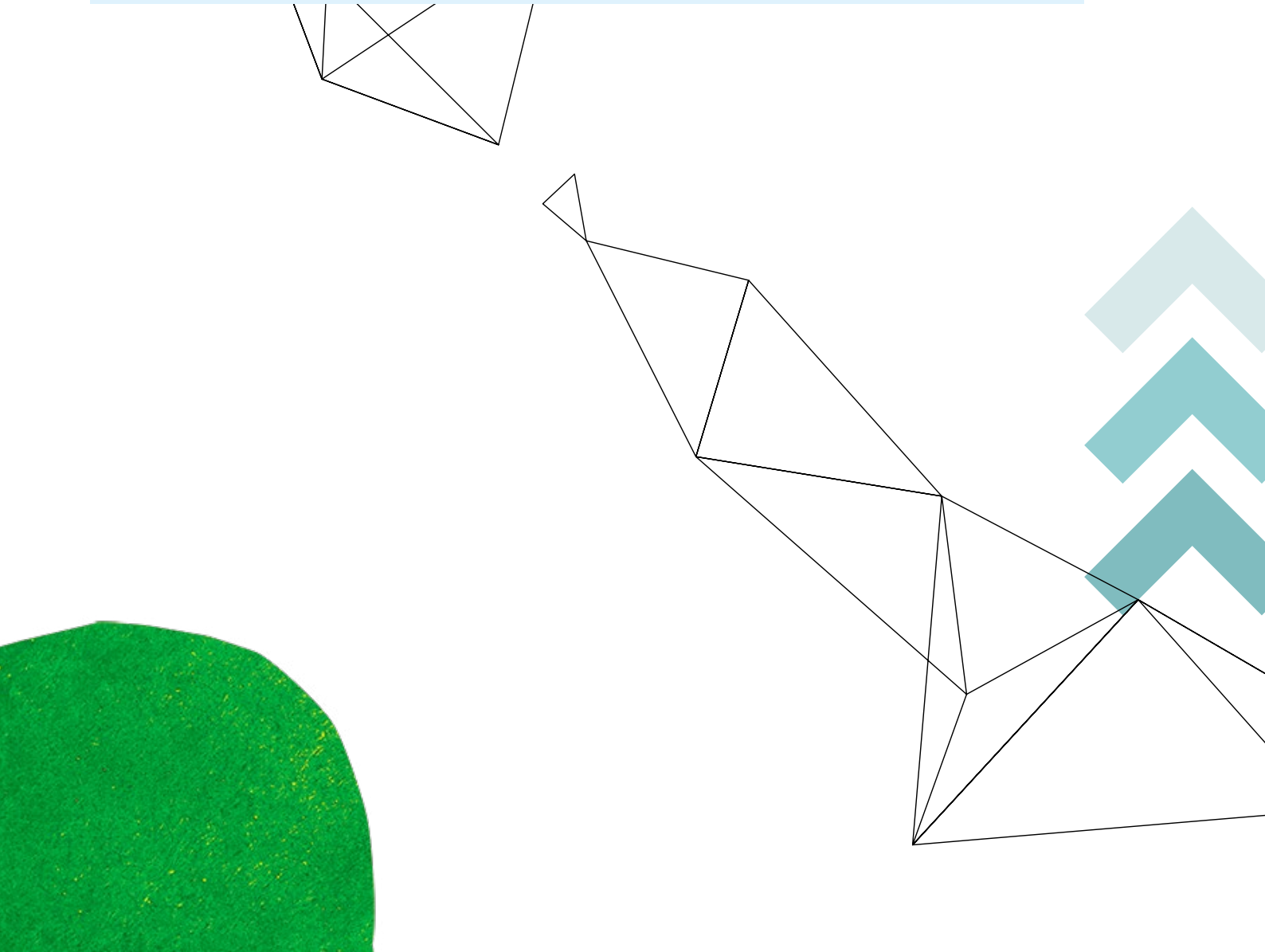
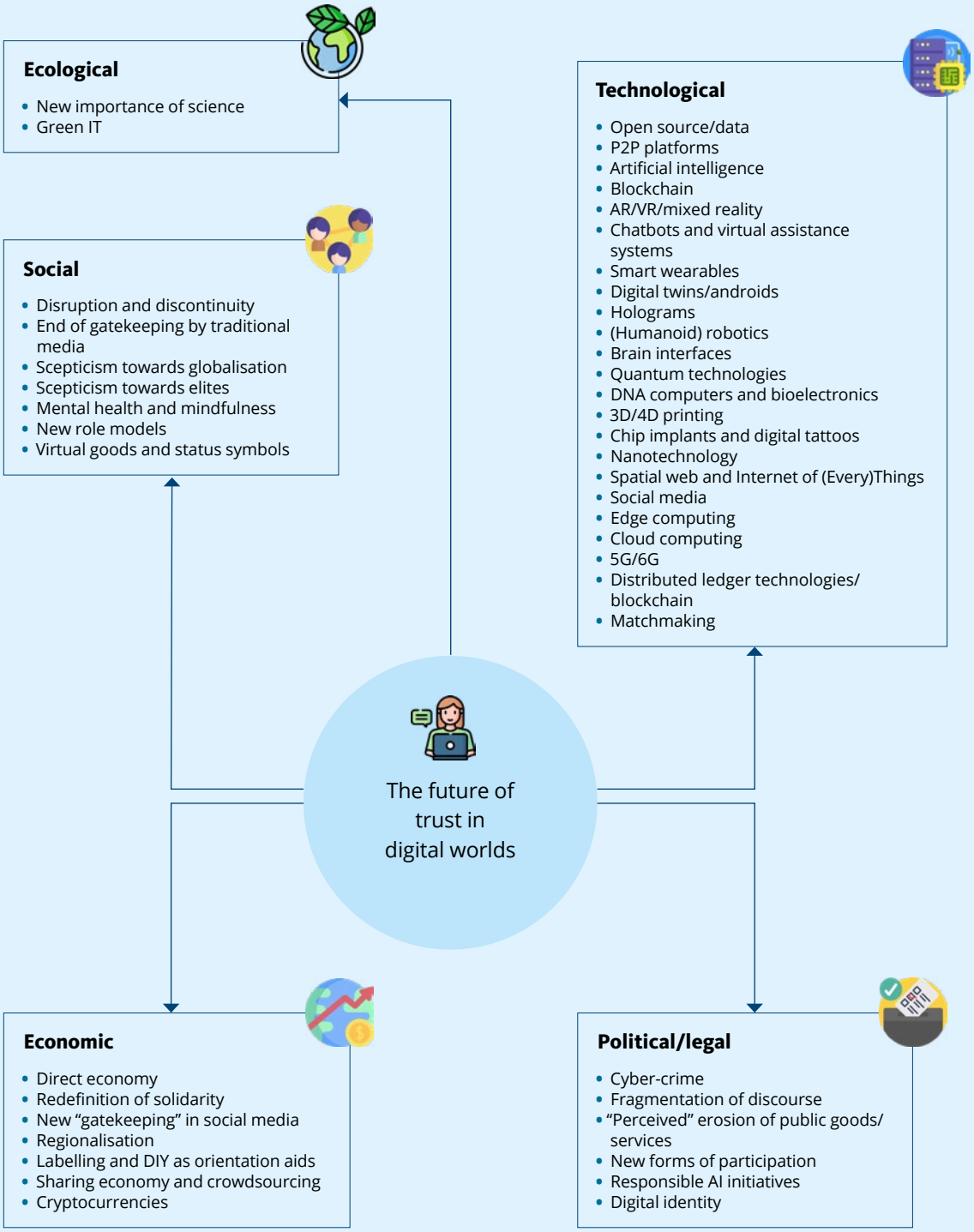


Figure 1: Driver map ordered by STEEP sectors



Source: © illustration by Prognos AG and Z_punkt 2021.

1.1 What is trust?

Luhmann's approach to the importance of trust in our society mentioned at the outset not only shows that trust makes action in complex societies possible in the first place; it also illustrates that trust pervades all areas of life. Hundreds of guide books examine trust and jealousy in relationships. Politicians solicit the trust of citizens, banks the trust of their customers, even vaccines demand trust. The demand for trust appears to be omnipresent. The diversity of contexts in which trust appears to play a role provides the first indication that trust not only reduces complexity, but is in itself a complex phenomenon. Two problems are encountered in the examination of trust as a concept. One, the understanding of trust in everyday speech is different from the scientific understanding, and two, each scientific discipline defines trust with its subject-specific focus, so that one definition of trust simply does not exist.[22] Thus we attempt here to examine the term and to develop a working definition of trust. The goal is to better understand on this basis what special roles are played by trust in its various forms for social interactions, how trust is built and what can contribute to an increase or decrease in trust.

What Luhmann describes above is often lacking from the use of the term trust in everyday speech: trust enables freedom of action. Therefore, trust should be more concretely defined as a positive expectation of a counterpart's future actions. The expectations can by all means vary and depend on the respective context. In trusting doctors, pilots or banks, the positive expectations are generally limited to their (professional) role. Thus not all trust is equal – it also depends on various contextual factors.[23]

Trust is always associated with uncertainty. It allows us to act notwithstanding a lack of (absolute) control and/or certainty. Thus we act in the knowledge that our own trust may be breached. This can also mean that the counterpart exploits the trust placed in them for their own benefit. Trust therefore always carries an element of risk. Some authors therefore characterise trust as a cost/benefit assessment,[24] while others focus more on the level of damage when trust is breached and therefore understand the element of risk as "accepted vulnerability".

Whether and how one trusts depends on two fundamental aspects. One is that people are different, also in their propensity to trust. Individual disposition and character traits influence the readiness to trust others.[25] Perception of the situation and one's counterpart is also important.[26] This perception in turn is shaped by one's own experiences, knowledge and values. At the same time, it is not static: that knowledge of and experience with the (potentially) trusted counterpart can change over time. Our own expectations can develop as well, changing according to the (temporal) context and life phases of the individuals/institutions involved. With these changes, the quality and depth of trust can be altered as well.[27]

Two factors are of particular interest for our examination (see Figure 2). One, how risks are perceived or how vulnerable one feels. Two, on what factors we base our belief that a person (or institution) is trustworthy. First we focus on characteristics that determine whether one is inclined to trust a counterpart. These can be summarised in three categories:

- Skill/competence
- Integrity/honesty/authenticity
- Friendliness/positive intent

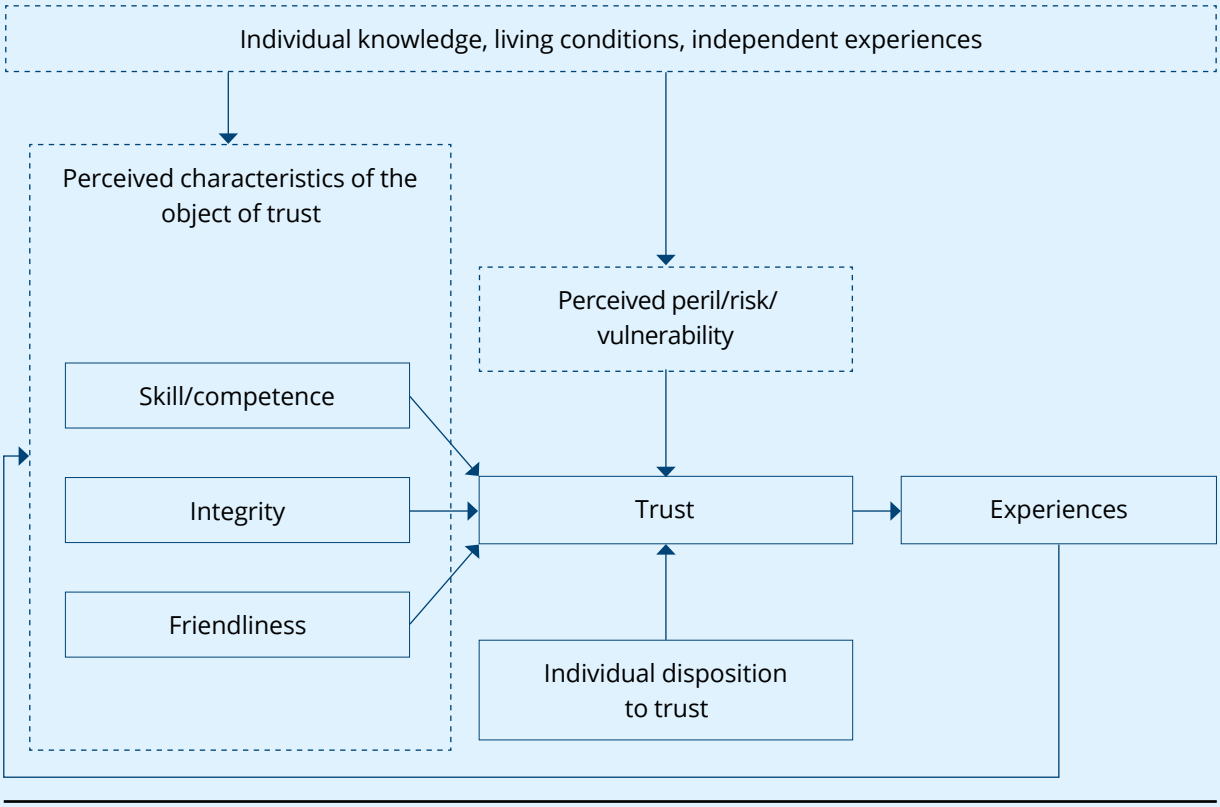
These three characteristics are not equally important in all trust relationships. With friends and acquaintances in particular, competence and skill tend to play a subordinate role. This factor is more important with persons and institutions we expect to play a concrete (professional) role. Most people

22 Hatak, I. (2011).
23 The willingness to accept information provided by a counterpart as trustworthy, generalisable and relevant is called epistemic trust.
24 Classic authors who follow this argumentation include, for example, James Colemann and Diego Gambetta.
25 Enste, D.; Suling, L. (2020).
26 Mayer et al. (1995).
27 Lewicki, R. J.; Bunker, B. B. (1995).

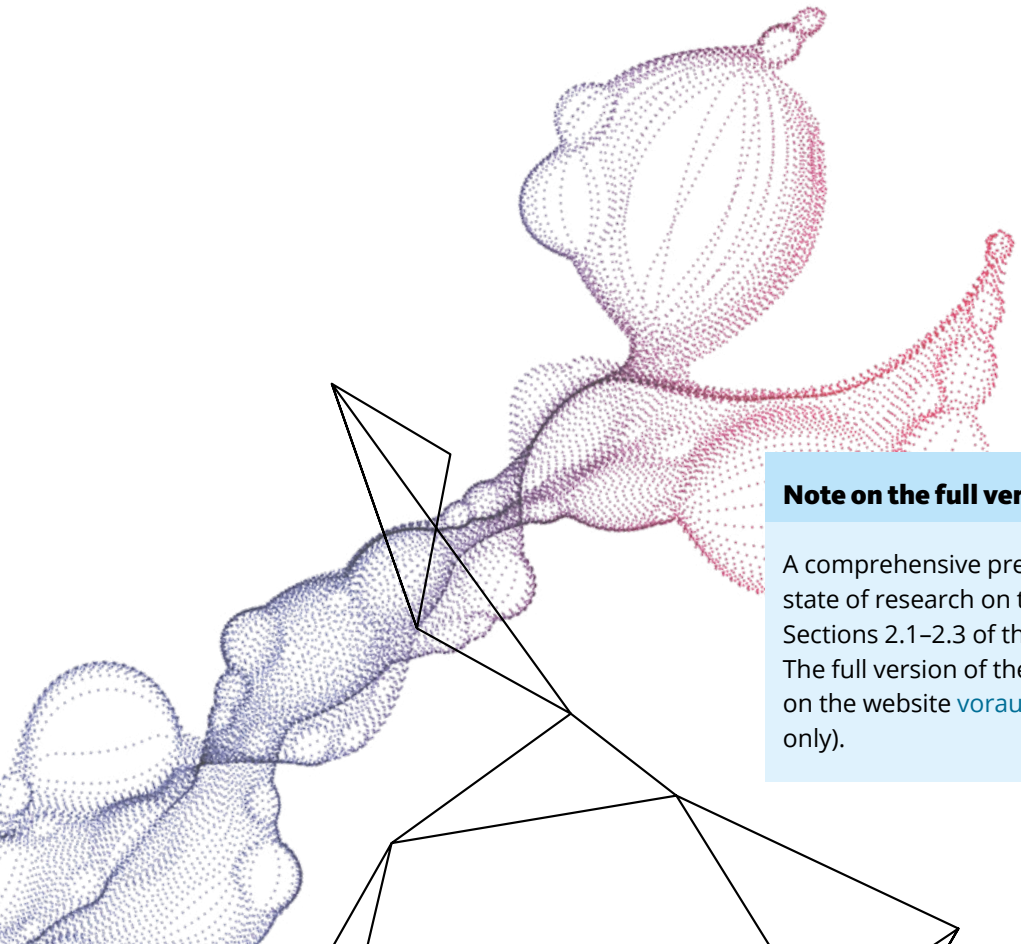
would likely find it difficult to trust a police force that is unable to maintain public order, even when acting with the best intentions. For the skill factor in particular, one should note that all of the characteristics listed here are perceived characteristics. Ultimately, how competent the police actually are is not decisive, but primarily how competent the police are perceived to be.

The trust building characteristics "integrity/honesty/authenticity" are explained by the definition of trust as "positive expectations". They all impart the feeling of being able to better assess the future actions of the counterpart. The last point is probably the most specific factor for trust: the perceived "positive intentions of the counterpart". This aspect is rather intuitive in personal relationships. The impression that a counterpart is well-disposed towards you appears to be an almost indispensable condition for establishing a friendship with them. However, the friendliness factor also helps differentiate trust from other social phenomena in more abstract relationships. Politics serves as an example here: no matter how competent and upright we consider a politician, we are hardly going to trust them to represent our own interests as long as they pursue different political goals. Shared values or perceived respect and recognition are therefore frequently cited in the literature and by the experts interviewed in the course of the study as further trust building factors.

Figure 2: Trust building factors



Source: © representation, Prognos AG and Z_punkt, based on Mayer et al. (1995).



Note on the full version of this study

A comprehensive presentation of the current state of research on trust can be found in Sections 2.1–2.3 of the full version of the study. The full version of the study can be downloaded on the website vorausschau.de (German version only).

1.2 Trust in technology

Does trust in technology even exist? As of 2021, the highly predominant opinion of the experts we consulted in the course of the study underlying this essay is: no.[28] One might object that many people trust they will not get an electric shock when they pick up a hair dryer every morning. Their situation meets all the criteria in view of the definition provided above. They act with the positive expectation that the hair dryer will do exactly what they expect of it – dry their hair. One can presume that most people lack both the technical expertise and the time to take their hair dryer apart every morning to verify whether it is still intact. So they act with uncertainty. They do in fact run a certain risk of injuring themselves should there be an unexpected technical defect. Yet the experts claim that one cannot trust technology. The wording gives us an initial indication of why that is so. Few people would say "I trust my hair dryer". They are more likely to say "I trust that my hair dryer will work". The wording "trust that" shows that this is about something one could describe as "trust in the system". One does not so much trust the hair dryer as such, but rather the system of certifications, inspections and personal experiences related to the hair dryer. This becomes even clearer when someone does actually get an electric shock. In this case, the person in question will probably stop using the hair dryer, perhaps even with the justification that they no longer trust the hair dryer. But would people also say that the hair dryer broke, breached or even abused their trust? Probably not. Doing so would presume that the hair dryer has a motive and ultimately also a will of its own. Thus we get to the heart of this little philosophical excursus: by trusting, we recognise the motives of the counterpart – in the expectation that they will not rank their motives above our own, exploiting the trust placed in them for their benefit. Since technology has no will of its own and no agenda, it cannot exploit trust. If it does, this is not because it "wants to" but because it was designed to do so. When we speak of trusting technology, we generally mean trusting the developers, engineers or authorities who control the technology, and trusting standards.[29]

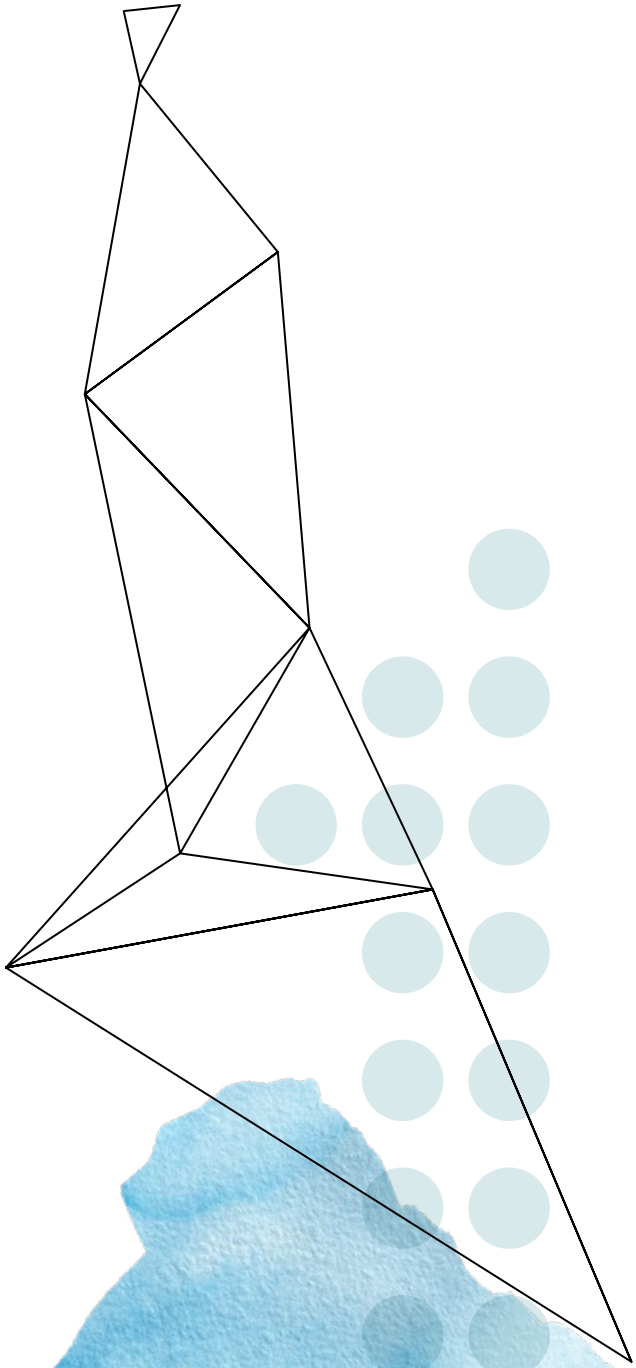
So why do we explicitly state that, according to some experts as of 2021, there is no trust in technology? Algorithms as digital assistants at home, vehicle navigation systems or customer service chatbots help us make decisions or organise our daily lives. Many of the algorithms used to date are based on classic decision trees. Here the response of the technology to our own actions is clearly comprehensible. However, various AI algorithms no longer function according to this principle. They have "learned" to make autonomous decisions. The principles on which the decision is based in part remain hidden even for the programmers. Complicated linear systems are becoming complex non-linear systems, in which a linear predetermination of the output from the input is no longer possible.[30] Thus only the algorithm's performance can be evaluated – the quality of the results it produces. We as laypersons know nothing about why a decision was made. Put a different way, we do not know the motives behind the decision. However, the trust building models described above presume that the decision to trust is always associated with personal perception of the counterpart's intentions. But when the counterpart has no intentions, no will of its own – which can still be assumed given the state of the art – the concepts of "trust" used today are blurred here. Even if no assumptions can be made about the intentions of AI, we do expose ourselves to decisions we cannot comprehend and cannot control, thereby putting ourselves in a situation that would be typically defined by trust.

A second, independent development is on the horizon: technology has become more human. Among other things, algorithms are learning to express themselves in natural language and robots are looking increasingly human. This leads to a question: what happens when we are no longer able to tell the difference between technology and humans? Even if the technology still does not have a will of its

28 Discussions with experts in the course of this study. A list of people involved in these discussions is found in the technical report.

29 Hartmann, M. (2020).
30 Ramge, T. (2020).

own, would we not ascribe motives to it regardless, not knowing that it isn't human? Can we then trust the technology as well? This is where new forms of trust come in – or simply a redefinition of what we mean by trust. However, this new trust could be far more fragile than trust in our fellow human beings. While we forgive people for their mistakes – on the assumption that the mistake was not intended and that they will learn from it – so that trust can be restored, all that remains for the machine is a new attempt, a reprogramming and the hope that it will work this time.[31]



31 Dietvorst et al. (2015).

1.3 In what kind of digital worlds will we place our trust tomorrow?

The long-term outlook should focus on what might come after the Web 2.0. While people live in three dimensions, today's web is largely two-dimensional. The Web 2.0 was devised for the shared use of information delivered to the flat screen of the user's device. Current efforts aim to literally bring the digital domain into a new dimension. Numerous concepts exist for these visions: the spatial web, Web 3.0 or the metaverse.[32] Even though it comes from a rather dystopian science fiction context,[33] the term "metaverse" appears to be gradually establishing itself in the public debate as a synonym for the spatial further development of the internet. This is surely related to the great global attention attracted by the renaming of Facebook to Meta and by the plans of its founder, Mark Zuckerberg, for a metaverse.

However, the concrete form of the metaverse imagined by Mark Zuckerberg is just one of many possible scenarios for a further development of the digital domain.[34] Something all terms from spatial web to Web 3.0 to metaverse have in common is the idea of a spatial web – a computer atmosphere that exists in an extensive three-dimensional space. Here the borders between analogue and virtual reality become blurred.[35] It may no longer be so easy to categorise what is part of cyberspace in the future and what is not. This spatial and semantic web is to be made possible through the convergence of numerous technologies, infrastructures, applications and social technology phenomena (see Figure 3). The interactions of technologies such as AI, intelligent sensors, distributed ledger systems, digital twins, 5G (and 6G), AR, VR and networked objects largely eliminate the borders between the physical and online worlds.

In this new digital domain, a large proportion of interactions with digital information may no longer take place on today's omnipresent screens, tablets and smartphones. New interfaces are emerging. In parallel to the new structures, new devices could also become reality. AR and VR applications, IoT wearables and smart glasses and contact lenses that seamlessly connect with the physical environment are conceivable in this context. Over the long term, every physical element in the real world could be fully digitised in the spatial web. Every human being could also have a virtual avatar that meets other avatars at virtual workplaces or meeting points. This availability of a techno-physical presence could expand human interaction patterns with new elements. While URLs are assigned according to a domain name system in Web 2.0, room addresses are assigned in Web 3.0/the spatial web. Thus users can identify and visit locatable places, physical objects, persons or digital content in cyberspace.

32 Rene, G. (2019), Deloitte (2020), The Economist (2020). For a long time, the concepts have been used synonymously in the public discourse, without one term ultimately predominating. The term "spatial web" also appears suitable for this study, since it appropriately describes the spatial dimension and the fundamental development tendency of the internet's further development.

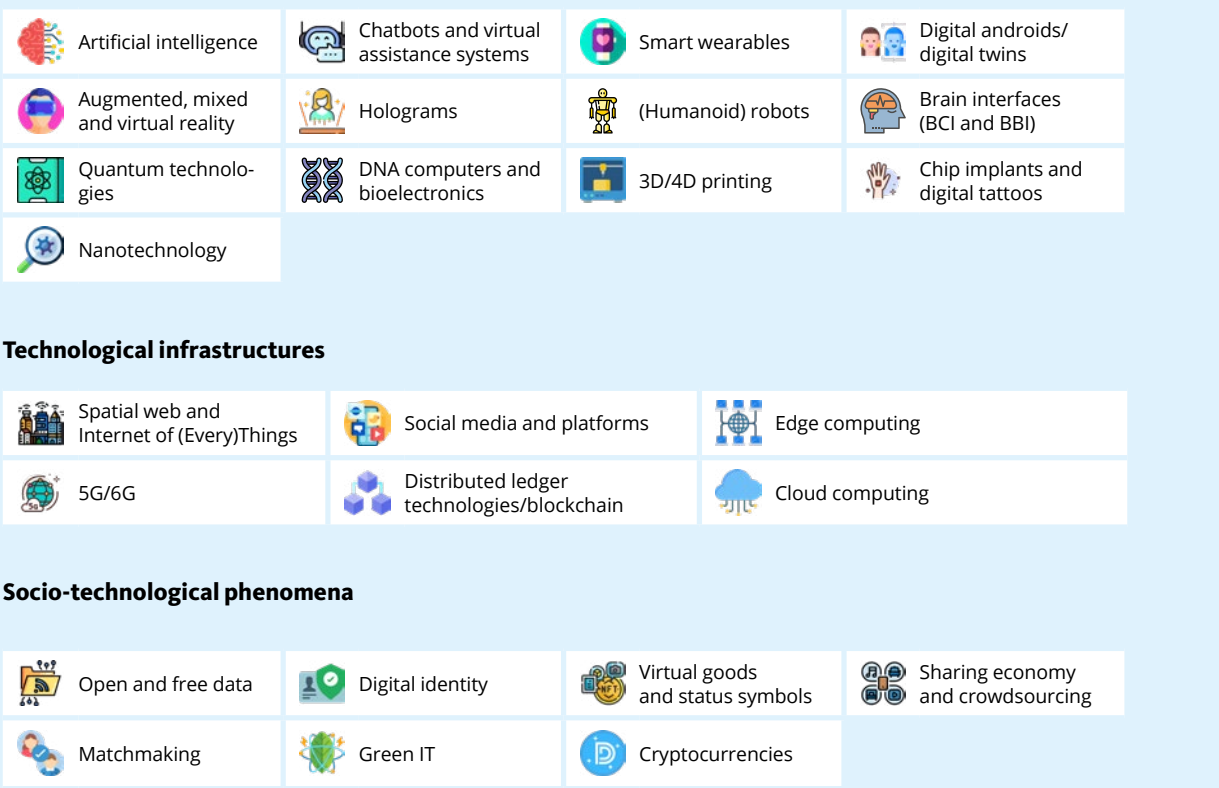
33 The term was coined in 1992 by science fiction author Neal Stephenson in his cyberpunk novel "Snow Crash".

34 Tagesschau.de (2021), Merten, M. (2021), Ball, M. (2021); The Economist (2021).

35 Deloitte (2020).

Figure 3: Fundamental technology drivers of Web 3.0 (spatial web)

Technologies, technology infrastructures and socio-technological phenomena



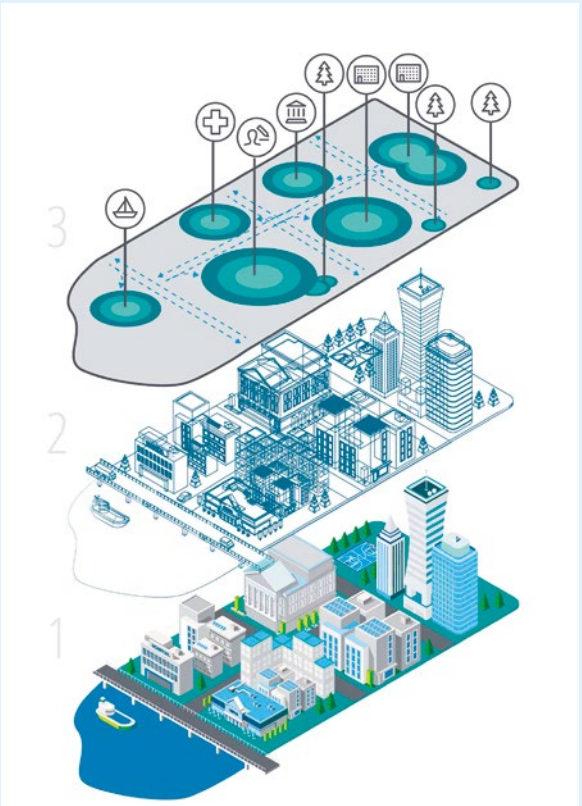
Source: © illustration by Prognos AG and Z_punkt 2021.

Lasting changes in human interactions with real and virtual versions of other people are possible. This also means that new patterns of trust building would be necessary, since this extended digital dimension cannot be captured by the existing cultural technologies. A Web 3.0/spatial web/metaverse could alter our view of the world in many ways (see Figure 4). However, a spatial digital domain could also lead to a fundamental increase of trust in the digital domain, since a much more extensive sensual experience of the virtual domain is possible here than in the "flat" 2D world of Web 2.0. New forms of interpersonal and institutional trust building should emerge in these new realities, such as trust building processes between avatars, between people and avatars, or people's trust in the new technologies.

A spatial web/Web 3.0/metaverse could therefore expand existing trust patterns with new elements. A spatial digital domain could help increase trust by replacing websites with rooms that can be experienced by "real" avatars, with the appearance of their real-world models. In combination with AI-based real-time translation, cultural barriers to understanding could be overcome more easily as well. At the same time, the distrust of people with negative experiences could increase so that fears in the digital domain would become more concrete as well. This open question shows that the future of trust in the digital domain will not only emerge in the course of technological progress, but also in the context of larger social developments. The digital domain's further development is based to a significant extent on the complex interplay of relevant

Figure 4: The spatial web's three levels

Technologies, technology infrastructures and socio-technological phenomena



Spatial interaction level

Next-generation interfaces such as smart glasses or voice will enable us to interact with context-specific, real-time information, accessible through intuitive and sensory triggers such as geolocation, computer vision and voice, gesture or biometric commands. The end effect is that the digital and physical planes merge for the user.

Digital information level

Ubiquitous sensors and digital mapping of the physical world could in theory lead to a digital twin of every object at every location. Today this type of digital information is primarily accessed using screens and dashboards. In the future, it may be accessed primarily via the spatial interaction level.

Physical level

The physical "real" world perceived by people with their five senses.

Source: © Deloitte (2020), descriptions adapted by Prognos AG and Z_punkt 2021.

technologies, technology infrastructures and socio-technological phenomena – that could also have different effects, given various social, economic and political surrounding conditions.

Note on the full version of this study

Section 3 of the study's full version presents the results for the digital domain of tomorrow. The full version of the study can be downloaded on the website vorausschau.de (German version only).

1.4 Trust, risk assessment and security in the digital worlds of tomorrow

Digital infrastructures have proven themselves indispensable, and not just since the coronavirus crisis. Everyday life and economic activity without them would be unthinkable. Increased convenience, networking and ease of communication also force us indirectly to use the digital infrastructures. Many services are only available online today. Consciously choosing not to use digital infrastructures also means a massive loss of social participation – and ultimately, exclusion from civil services.

As described above, the emergence of cyberspace would not have been possible without trust. A distorted perception of potential risks in the digital domain contributed to this as well: since virtual risks are not tangible, they are not viewed as genuinely threatening. Instead, people fear threats the most when they are unknown, spread rapidly, can assume catastrophic magnitudes and are potentially fatal for everyone.[36] Virtual risks on the other hand do not (yet) represent a direct threat to life and limb. This is compounded by a habituation effect: the more familiar we become with a risk, the more our initial anxiety decreases.[37] Network effects intensify this: when a critical mass of users is reached for an app or software, reservations are suppressed and the benefits of use move into the foreground.[38]

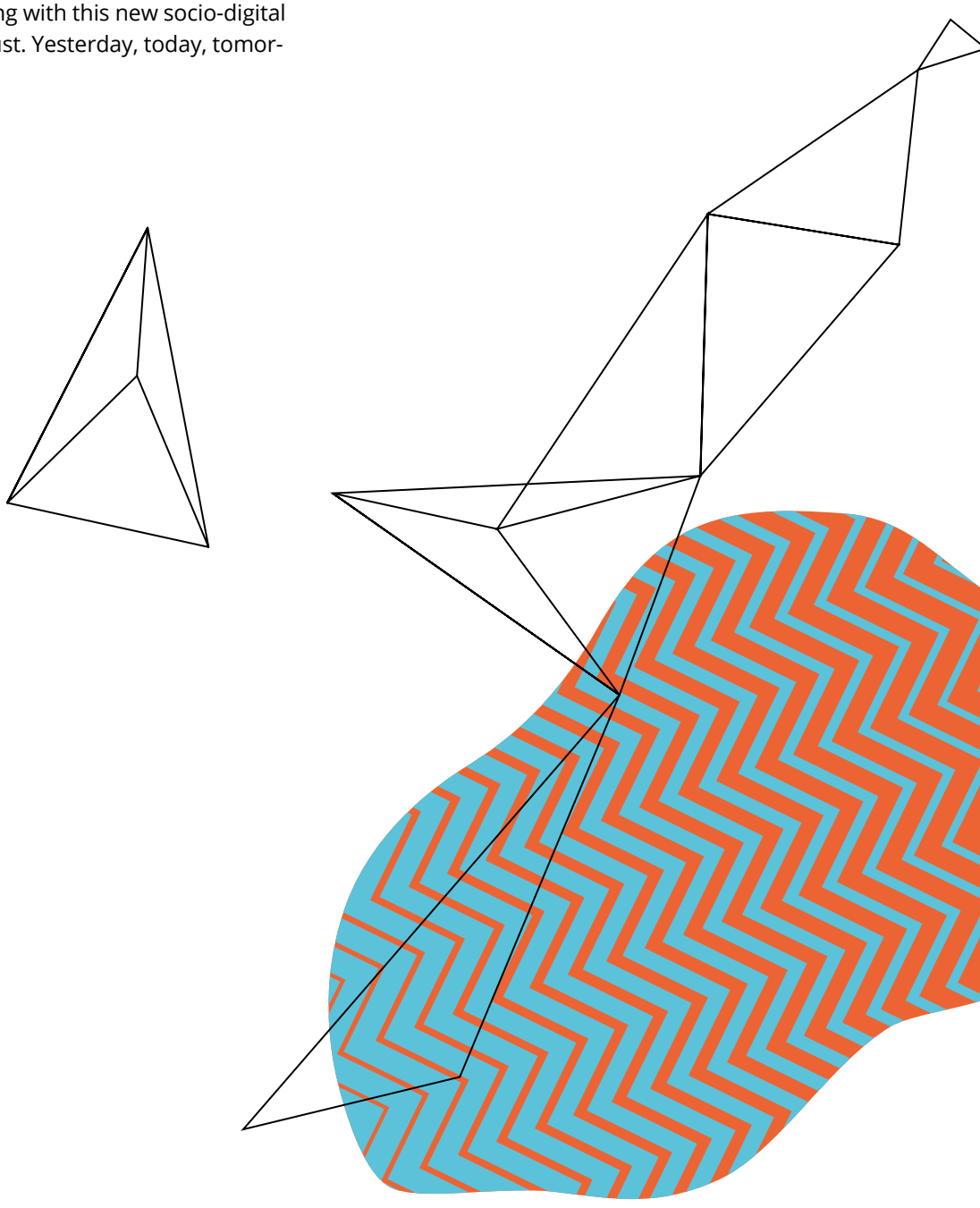
As described above, the spatial web/metaverse/ Web 3.0 could alter our perception of virtual risks with its spatial, haptic appearance. Risks may be perceived as more "real". It can be assumed that cybercrime and harassment will play a major role in the spatial web as well.[39] The three-dimensional experience could make discrimination and criminality much more tangible, making existing, comparatively abstract fears in the digital domain appear as more realistic threats. Initial indications of this are already emerging in reports of sexual assault in VR-based computer games or VR worlds.[40] The extent to which existing prejudices and patterns of discrimination from the real world are continued in the spatial web, or whether new patterns of discrimination emerge in this context, is likely an important aspect here. Forms of avatar harassment likely to weaken interpersonal trust in the spatial web are fundamentally conceivable here. Like the existing phenomenon of cyber-harassment, effects in the analogue world in the form of mental problems are also conceivable with new variations of physical violence. Both new cyber-phenomena and the fundamental level of trust are likely dependant on regulatory surrounding conditions. Further developments, both technological and socio-political, are highly uncertain. Discussions of questions regarding a possible future obligation to disclose digital identities and to use real names are far from over.[41]

At the same time, it can be assumed that the importance of digital infrastructures will continue to increase. This is illustrated among other things by major investments in this area over the coming years,[42] also based on collective expectations with regard to future significance.[43] This could further intensify the existing "indispensability" of the digital domain. A dynamic development of the digital domain is simultaneously expected due to technological progress. Digital sceptics would become increasingly less able to opt out. A differentiation of the basis of trust with regard to the use of digital services and infrastructures is therefore possible. On one side are those who engage in a dynamically developing digital domain of the future with a sort of "basic trust". On the other side, there are those who (have to) engage in digital worlds, contrary to their convictions, or be denied social participation or access to relevant services.

For the latter, gaining trust could become easier to the extent that cybersecurity is improved. For the former group on the other hand, what is true since

36 Slovic, P. (1987).
37 Die Zeit (2021).
38 TH Köln (2015).
39 Security Affairs (2021).
40 Süddeutsche Zeitung (2022).
41 Marx, I. (2020).
42 Federal Ministry of Finance (2020).
43 Beckert, J. (2018).

the start of the internet applies: the web of the future also requires trust for its development. Thus people who are ready to keep exploring new spaces, no matter what technological means are used to do so, will still be needed in the future. So far the journey has been a one-way street from analogue to digital. Web 3.0 with the generation of hybrid realities could now turn the flow in the other direction as well. Dealing with this new socio-digital complexity requires trust. Yesterday, today, tomorrow and the day after.



Everyday stories from the future
Future spotlight "Ecological Regionalisation"

Thursday, 17 May 2035.

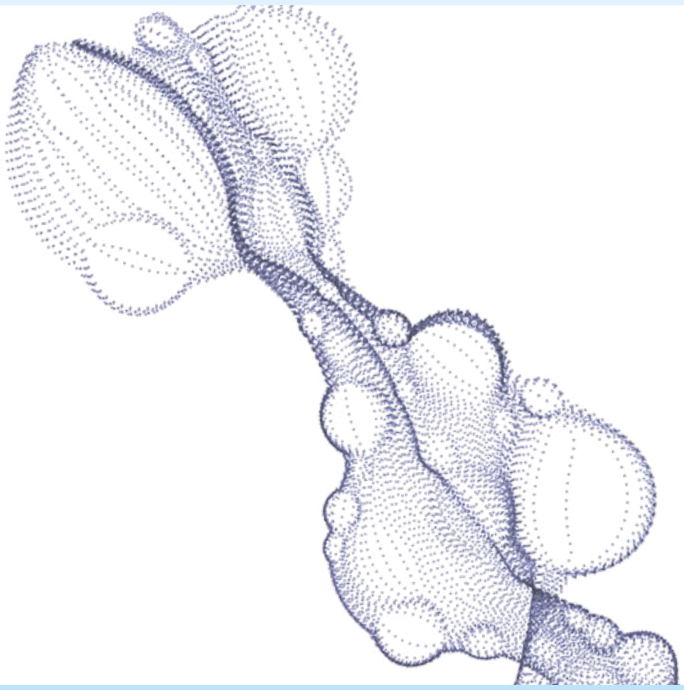
11 am. Lana returns from her morning's work on a joint project. She just dropped her son off at day-care. Twice a week, she helps Pasquale with the establishment of an urban garden. Pasquale is a pensioner striving to set up a vertical farm for the community in an old warehouse, providing other volunteers with intuitive access to digital gardening. Lana is helping him with the programming of a humanoid robot designed to teach children about caring for the various species of plants, and about how the farm works. Both know that convincing parents of the project will be a challenge. While many see the economic benefit of digital applications, they don't want to bring their young children into contact with the immersive and virtual world just yet. Lana's son, for one, is excited about the project and she is convinced that he learns a great deal more this way than by watching videos.

When she gets home, Lana goes to the kitchen for a glass of water. Her smartwatch vibrates. Lana turns off the tap and looks at her watch: "Today is Friday. You have achieved half your usual weekly water consumption. Congratulations!" Lana is part of a digital twin pilot project for households. Her home is equipped with smart sensors to analyse electricity, water and waste volume data. In addition, Lana regularly gets personalised tips for optimising her consumption or information about initial signs of illness. Like many other citizens, she views digital data as an important contribution to society, especially for climate protection. Green IT has become a matter of course. Users can explicitly choose what information is shared, and for what purpose. The collected data are anonymised and supplied to the regional open data platform, and used mainly to improve public administration.

At noon she has her monthly meeting with the colleagues of ShareHub, a platform for the transfer of knowledge between European regions. Lana is in charge of media relations and the official blog. With the rise of the spatial web, many municipalities and organisations in this network have committed to a strict separation of the virtual and physical worlds. Lana is currently working on a post for the Share-Hub blog describing the feasibility of and obstacles to this separation. In schools, nursing and medical care, for example, real human contact is often preferred over virtual encounters. A colleague from the Czech Republic reports that using virtual reality applications in his region is limited to business meetings and the control of automated production systems. However, this is leading to the significant challenge that fewer and fewer people are willing and able to use these intuitive yet complex applications. Another colleague from Germany describes heARt, a new campaign focusing mainly on AR applications instead of immersive, virtual reality for social media. Lana has already heard of that. In the afternoon, she meets with Maria, one of the founders and part of the initiative.

Maria is already waiting for Lana in a small neighbourhood café. With her start-up, she is developing an application for the context-based integration of information in everyday life, intended to strengthen the local economy and community. The new 6G network frequencies have only recently been opened for such services. Networked glasses or ear buds provide information, for example, to people out for a walk about cafés or shops they are passing by, friends and acquaintances nearby, possible places of interest or current developments in the city. Anyone can contribute and comment on content. The idea is a social network that is based on the real human environment, thereby ensuring the authenticity and transparency of information and behaviour. Maria gives Lana a pair of glasses. Lana looks around the café and the menu with today's recommendations appears immediately. She sees a construction site across the street. A message appears in her field of vision: "Home of the new aquatic centre. Construction 80% complete. Opening October 2035. Do you want to live there? Register here." Lana blinks twice and the glasses record her registration. Really cool, Lana is looking forward to testing the application with her own glasses!

When she gets home, Lana flops down on the sofa. It's been a busy day and her son will be home soon... a bit of time for herself would not be amiss. One of her friends keeps talking about her new "Find Yourself Bubble": A personal, virtual space that helps you get away from the workday and make a clear transition to private life. It offers a choice of mindfulness and meditation offers or immersive nature experiences. A short walk through the jungle would be just the thing right now...



New patterns of interaction and elements of trust and distrust building in the future spotlight "Ecological Regionalisation"

New patterns of interaction	› Humanoid robots as learning aids and "teachers" › Digital twins of homes to improve energy efficiency and waste management › Ability to communicate with the surroundings using smart glasses and smart ear buds › Widespread use of AR applications and smart glasses
Trust building elements	› Individual limitation of data sharing is possible › Recorded data are anonymised and collected in an open data platform › Human interactions are preferred over virtual ones where possible
Distrust building elements	› Widespread fundamental scepticism regarding digital applications

2

CORE FINDINGS AND FOLLOW-UP QUESTIONS

2.1 Core findings

Trust is a key mechanism for dealing with complexity and uncertainty, and for maintaining the capability of action in new situations and spaces. It was therefore a prerequisite for conquering digital space, and will continue to be of central importance due to the constant further development of the digital domain.

There would be no cyberspace, internet or social media without trust. The rapid advance of digital networking due to the internet and development leaps in technologies such as smartphones, AI, VR and big data applications are symbolic of the digital domain's constant further development. A development slowdown is not foreseeable in the near future. Instead, the analogue and physical worlds are becoming increasingly intertwined with digital technologies, virtualisation and networking. Hybrid realities are already on the horizon. This (seemingly) makes everyday life easier and more convenient for the individual. Access to information is easier and faster, digital assistants help with routine tasks and organise the daily routine. However, individuals are unable to understand or retrace, let alone control the underlying technologies and algorithms. Citizens have to trust in order to continue functioning in this complex world. This trust does not necessarily have to be placed in the stakeholders behind the technologies and software. Just like trust in public authorities gives everyone the feeling of being able to move about in public space without danger to life and limb today, new or established regulative authorities could promote trust in the system in the future, enabling interaction and movement in a digitally networked world.

Knowledge asymmetries between users and providers of digital network technologies distort the perception of risk in the digitally interconnected world. The relationship between the added value and the risk of digital technologies is misjudged. This knowledge asymmetry could become even greater in the future.

The digital domain is defined by a fundamental knowledge asymmetry. A few companies and experts have insight into the functionality, decision processes and business models of the digital world, which remains largely opaque for the majority of users. Overcoming this knowledge asymmetry is also driving the debate about responsible AI.[44] Regulatory frameworks are often outpaced by technological innovations. At the same time, the risks and potential for abuse associated with the use of technologies and their applications are difficult to evaluate: risks such as the misuse or manipulation of data are still comparatively new. As a rule, the consequences and possible personal harm cannot be assessed based on empirical values yet. Collective empirical values are only available in anecdotal form. In addition, the risks are more abstract and less immediate than risks to life and limb in physical space. This leads to misjudgements regarding the added value and risk of use. Against the background of looming technological change due to new technologies and technology convergence, this knowledge asymmetry is not expected to decrease in the digital domain of the future. Quite the contrary: complex technology applications such as deep learning could actually increase it since, for various AI algorithms, the ability of even the programmers to comprehend the functionality is limited. The importance of initiatives aimed at responsible AI or ethical coding is expected to continue to increase.

The digital domain is dominated by a sort of convenience paradigm. To a large extent, the willingness to use new technologies depends on their added value. A high perceived added value and network effects drive distribution. Usage paradoxes emerge: technologies are used in spite of distrust of the operators and their intentions.

Many technology applications in the digital domain promise an easier, more comfortable life. This phenomenon is reinforced by network effects. Technologies and applications that add value by connecting people or data in turn benefit from monopoly or oligopoly structures. The higher the number of people or things that are connected, the greater the (perceived) benefit for individuals to use the same solution or platform. At the same time, alternatives are always associated with greater effort and costs. The following are usage paradoxes: even though the positive intentions of operators are called into question, and there are data protection concerns, meaning the operators are actively distrusted, the perceived benefit (or the critical mass of users) outweighs the perceived risks. The increasing pervasiveness of algorithms that replace or support human decision-making (e.g. digital assistants) could drive this process.

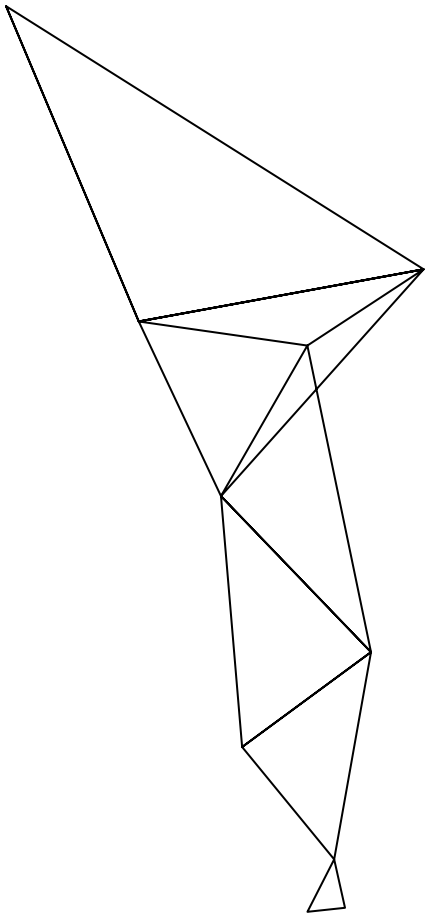
Even though it seems paradoxical at first glance, security does not mean more trust. The greater the security in a situation, the less trust is needed to deal with the remaining uncertainty. But the more secure the surrounding conditions, the more inclined one is to "bridge" the remaining uncertainty with trust.

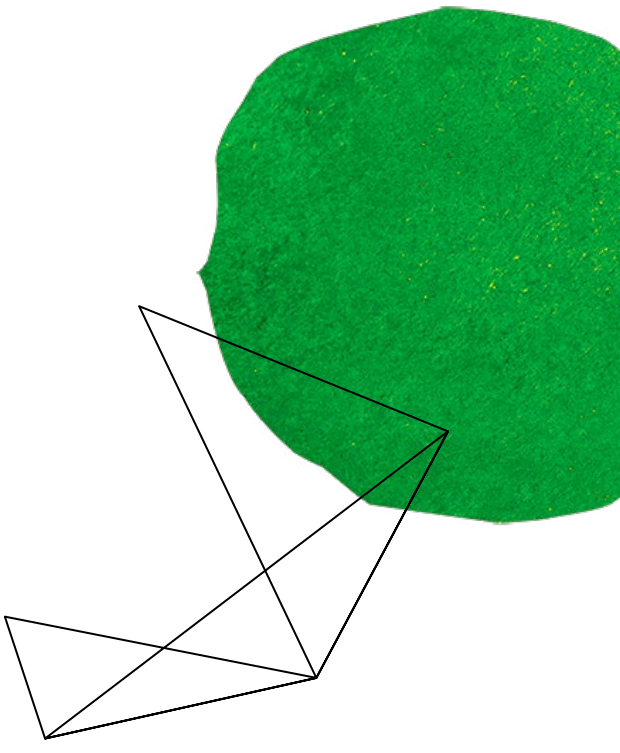
Security and trust are often used in the same breath, with the claim that security builds trust. In fact, the interactions between security and trust are highly complex. With complete security, trust would no longer be needed. When we consider ourselves completely secure, for example, by concluding contracts, through control mechanisms or possible sanctions, we no longer need to trust. Nevertheless, a feeling of fundamental security in the face of greater risks can contribute to bridging remaining uncertainties with an advance of trust. As security building elements, technical security measures (cybersecurity), intermediaries and regulations can reduce risks in the digital domain. More security means less trust is needed as a "lubricant". But the more secure the overall situation is, the more "fundamental trust" exists.

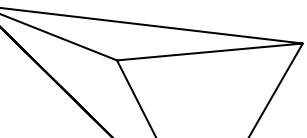
44 See Section 2.4.4 in the full version of the study. Available for download at vorausschau.de (German version only).

Trust primarily depends on the perception of the counterpart. The fusion of the analogue and virtual changes this perception, and therefore also trust. New forms and new qualities of trust may emerge.

Increasing digitisation and virtualisation also reduces the immediacy of encounters and limits perceptions compared to physical encounters. But how the counterpart is perceived is crucial for determining whether they are considered trustworthy. Technologies are increasingly becoming communication and interaction mediators. Thus the existing strategies on which we base our decision regarding the trustworthiness of a counterpart are becoming less and less reliable. This is because there is less information on which to base our judgement compared to a direct encounter, since visual, haptic and sensory stimuli are reduced. Also, the authenticity of the perceived stimuli can no longer be verified. Thus trust becomes more complex, since we also need to trust all technologies and mediator instances that make the interaction possible. This applies, for example, to the virtual assistance systems making far-reaching decisions in the everyday scenarios described in the future spotlights, where they have long since established themselves in daily life. Or to interactions with humanoid robots. It applies most of all to complex interactions with avatars, including real image avatars, animated graphics and holograms, producing entirely new forms of encounters in the spatial web/Web 3.0/ metaverse. Will there be a parallel “avatar check” for trustworthiness by virtual assistance systems? Are there scoring systems for avatars? Are we going to trust real image avatars more than animated graphics? How will we assess avatars and holograms as trustworthy? These new patterns of interaction could lead to new trust building cultural technologies in the future; paradoxically, these may in turn use technology in the form of AI verification systems.







2.2 Follow-up questions

Numerous follow-up questions for the future realm of possibility arise from the study. Many of these questions were implicitly examined in the future spotlights as alternative visions of the future. However, listing them here again explicitly is worthwhile.

Increased interconnectedness allows us to find spaces with like-minded persons, which in turn subjectively increases trust in other people. At the same time, there is the threat of increasing separation from other groups. How can new digital meeting places be created that bring society together?

If technology becomes more individualised (digital assistance systems etc.) and humanoid, will people attribute subjectivity to technology? What is the influence of algorithmic decision making (ADM) or AI-based systems on how we view the world, and how could these technologies control our actions? To what extent could humanity lose its autonomy of action?

Are technologies that appear increasingly human promoting a new version of trust? Do algorithmic decisions that are no longer comprehensible require new forms of trust?

Hartmann speaks of "warm trust" and adolescents in the focus groups see "human closeness" as a prerequisite for deep interpersonal relationships. Can avatars and holographic images become an equivalent for human closeness or convey the closeness of other people?

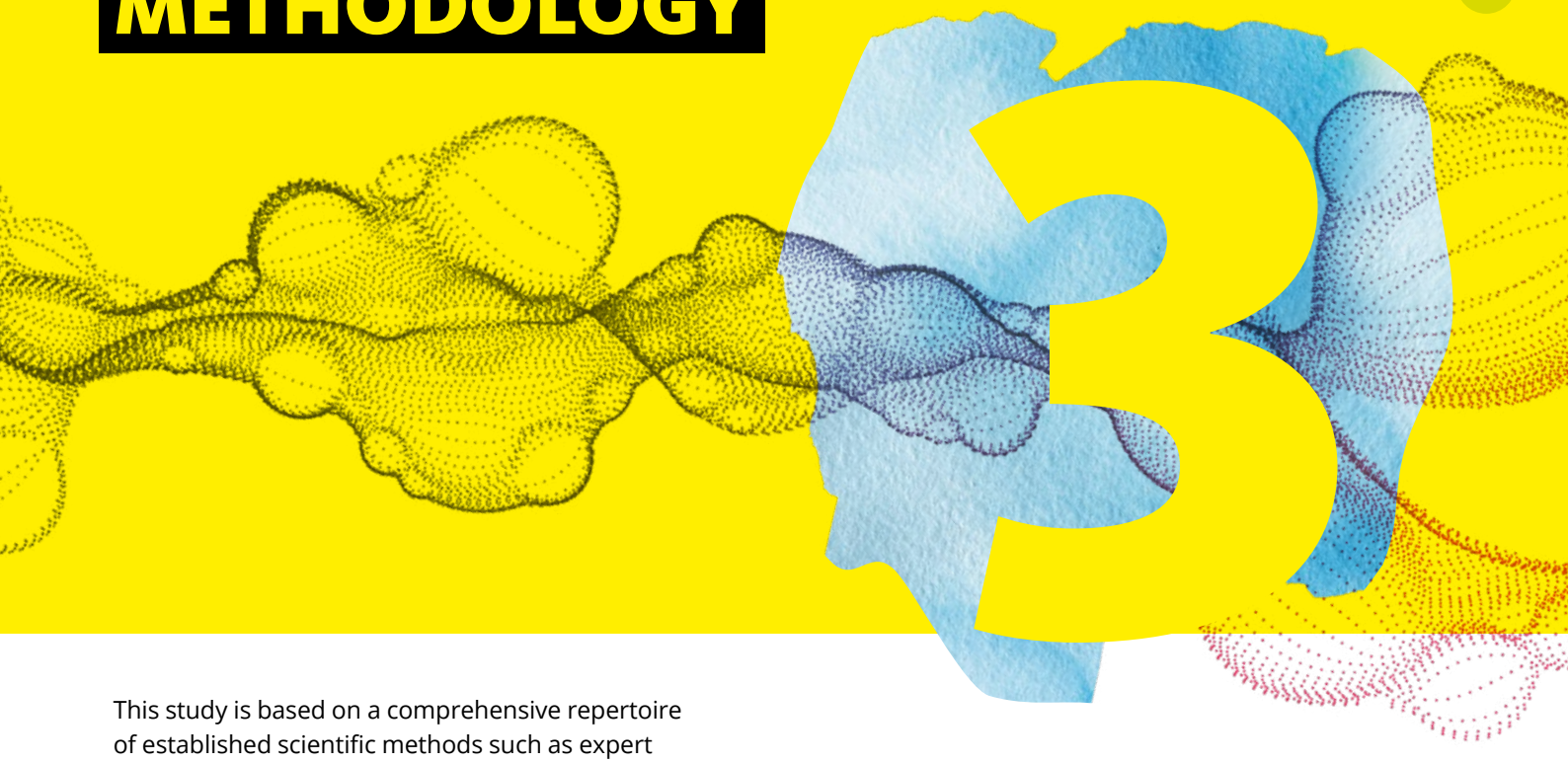
Ubiquitous digital twins could make "digital simulation rooms" the basis of decisions. Will this cause a shift in the weighting of empiricism and "digital simulations"?

Technological developments, such as new encryption methods and blockchains, attest to an increased striving for security in the digital world. Does this need for increased security run contrary to an organic network culture?

To what extent does security (including data security, for example) require stricter regulation because citizens are increasingly dependent on digital infrastructures? Do legislators need to anticipate future developments to a greater extent – increasingly regulating what may be, not only what already exists? Can this even succeed at the national level without creating a Splinternet?

How could new forms of hate speech or physical violence (e.g. avatar harassment, hateful comments or the visual appearance of an avatar) be avoided in a spatial web?

3 METHODOLOGY

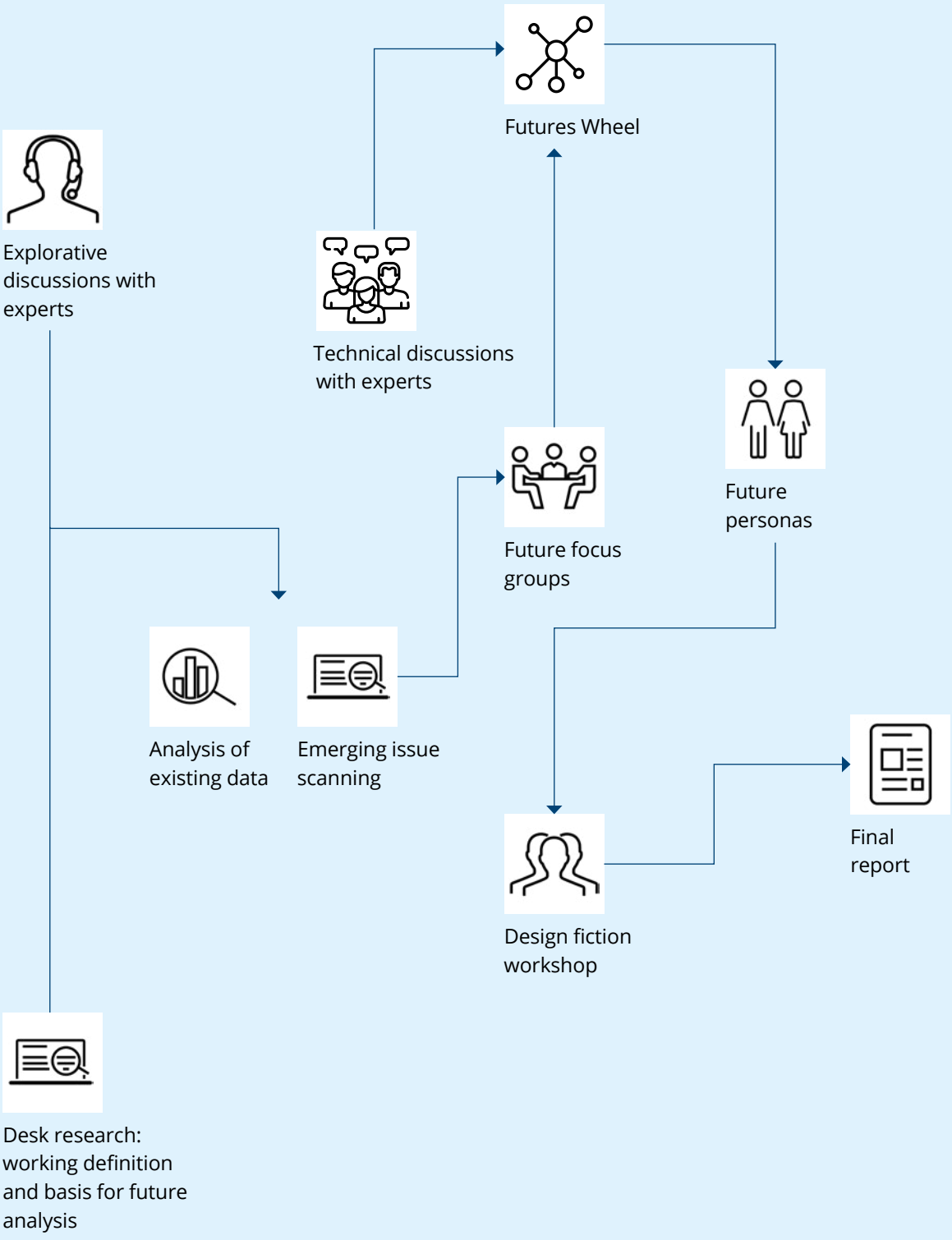


This study is based on a comprehensive repertoire of established scientific methods such as expert interviews, desk research and secondary data analysis. Established foresight and participatory methods were also used, for example, a futures wheel workshop and working out application scenarios within the future spotlights framework as well as a design fiction workshop with young designers to discuss potential design approaches aimed at building (or destroying) trust. Consequently, explorative and future-oriented as well as dialogue-oriented foresight methods are founded on a solid empirical basis that follows the research dynamics and simultaneously captures development perspectives.

Note on the full version of this study

Further information about the participating experts, the datasets used and their analysis is found in Section 7 of the full version of the study. The full version of the study can be downloaded on the website vorausschau.de (German version only).

Figure 5: Methodological steps in preparing the study



Source: © own representation, Prognos AG and Z_punkt 2021.

4 LIST OF SOURCES

Allmendinger, Jutta (2019): Das Vermächtnis – Wie wir leben wollen und was wir dafür tun müssen. Ergebnisse 2019. DIE ZEIT, infas, WZB, online at: https://live0.zeit.de/infografik/2019/Vermaechtnis-Studie_Broschuere_2019.pdf (accessed on 15/12/2019).

Allmendinger, J.; Wetzel, J. (2020). Die Vertrauensfrage: Für eine neue Politik des Zusammenhalts. 1st edition. Berlin: Duden.

Ball, M. (2021). A Framework for the Metaverse. Online at: https://www.ballmetaverse.co/research/a-framework-for-the-metaverse (accessed on 15/11/2021).

Beckert, Jens (2018): Woher kommen Erwartungen? Die soziale Strukturierung imaginierter Zukünfte. Jahrbuch für Wirtschaftsgeschichte / Economic History Yearbook, Volume 59, Issue 2. Berlin: De Gruyter Oldenbourg.

Beugelsdijk, S.;Smulders, S. (2009). Bonding and bridging social capital and economic growth. Tilburg: Tilburg University.

Cardenas, J. C.; Carpenter, J. (2008). Behavioural development economics: Lessons from field labs in the developing world. The Journal of Development Studies, 44(3), pp. 311-338.

CNN (2022). What ist Web3 and why does it matter? Online at: https://edition.cnn.com/videos/tech/2022/02/05/web-3-explainer-magic-wall-nobilo-vpx.cnn (accessed on 08/02/2022).

Contract for the Web (2019). Online at: https://contractfortheweb.org/ (accessed on 21/04/2021).

Dator, James (undated). What Futures Studies is, and is not. University of Hawaii. Online at: http://www.futures.hawaii.edu/publications/futures-studies/WhatFSis.pdf (accessed on 25/01/2021).

Deloitte (2020). The Spatial Web and Web 3.0. Online at: https://www2.deloitte.com/content/dam/insights/us/articles/6645_Spatial-web-strategy/DI_Spatial-web-strategy.pdf (accessed on 25/11/2020).

Die Zeit (2021). "Gewöhnung macht leichtsinnig" (Interview with risk researcher Ortwin Renn). Online at: https://www.zeit.de/wissen/gesundheit/2020-08/ortwin-renn-coronavirus-risikoforschung-angst-ansteckung-leichtsinn/komplettansicht (accessed on 11/05/2021).

Dietvorst, B. J.; Simmons, J.; Massey, C. (2015). Algorithm Aversion: People Erroneously Avoid Algorithms after Seeing Them Err. Journal of Experimental Psychology: General 144, no. 1 (2015), pp. 114–26.

Dincer, O. C.; Uslaner, E. M. (2010). Trust and growth. Public Choice 142, 59. Berlin/Heidelberg: Springer Science+Business Media.

Enste, D.; Suling, L. (2020). Vertrauen in Wirtschaft, Staat, Gesellschaft 2020: Vertrauensindex: Europäische Länder im Vergleich (No. 5/2020). IW Policy Paper.

Federal Ministry of Education and Research (BMBF) (2020). Karliczek: Wir starten strategische Initiative zum Quantencomputing. Online at: https://www.bmbf.de/bmbf/shareddocs/pressemitteilungen/de/karliczek-wir-starten-strategi-nitiative-zum-quantencomputing.html (accessed on 30/07/2021).

Federal Ministry of Finance (2020). Investitionen in ein modernes Land. Online at: https://www.bundesfinanzministerium.de/Monatsberichte/2020/03/Inhalte/Kapitel-2b-Schlaglicht/2b-Investitionen_pdf.pdf;jsessionid=6E08353D2D76944288D4EE1691F11587.delivery1-master?__blob=publicationFile&v=3 (accessed on 11/05/2021).

Fleishmanhillard (2020). Techlash 2020. Online at: https://fleishmanhillard.com/wp-content/uploads/2021/03/Techlash-2020-Why-the-Technology-Sector-Needs-to-Lean-in-Now-on-Consumer-Expectations.pdf (accessed on 25/01/2021).

Hartmann, M. (2020). Vertrauen – die unsichtbare Macht. Berlin: Fischer Verlag.

Hatak, I. (2011). Kompetenz, Vertrauen und Kooperation: Eine experimentelle Studie, Forschungsergebnisse der Wirtschaftsuniversität Wien. Berlin: Peter Lang International Academic Publishers.

Lewicki, R. J.; Bunker, B. B. (1995). Trust in relationships. Administrative Science Quarterly, 5(1), pp. 583–601.

Luhmann, N. (2014). Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität. 5th edition. Stuttgart: UTB.

Marx, I. (2020). Klarnamenpflicht. Mit offenem Visier. Tagesschau.de. Online at: https://www.tagesschau.de/inland/schaeuble-klarnamenpflicht-soziale-netzwerke-101.html (accessed on 04/02/2021).

Mayer, R. C.; Davis, J. H.; Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. The Academy of Management Review, 20(3), pp. 709-734.

Merten, M. (2021). Alles wird meta. ada. Online at: https://ada-magazin.com/de/alles-wird-meta (accessed on 24/11/2021).

Peter, S.; Riemer, K.; Hovorka, D. (2020). Artefacts from the Future: Engaging Audiences in possible Futures with Emerging Technologies for better Outcomes. In: Proceedings of the 28th European Conference on Information Systems (ECIS). An Online AIS Conference, 15–17 June 2020.

Prognos AG; Z_punkt GmbH The Foresight Company (2020b). Zukunft der Wertvorstellungen der Menschen in unserem Land. Online at: https://www.vorausschau.de/SharedDocs/Downloads/vorausschau/de/BMBF_Foresight_Wertestudie_Langfassung.pdf?__blob=publicationFile&v=1 (accessed on 06/10/2021).

Ramge, T. (2020). Augmented Intelligence. Wie wir mit Daten und KI besser entscheiden. Ditzingen: Reclam.

Rene, G. (2019). An Introduction to The Spatial Web. Medium. Online at: https://medium.com/swlh/an-introduction-to-the-spatial-web-bb8127f9ac45 (accessed on 01/02/2021).

Rudelle, J. (2019). Warum das offene Internet Grenzen für die Big Techs braucht. Horizont. Online at: https://www.horizont.net/medien/kommentare/regulierung-warum-das-offene-internet-grenzen-fuer-die-big-techs-braucht-176915 (accessed on 21/04/2021).

Schaich, A.; Neef, A. (undated). Future Personas. Den Kunden der Zukunft erlebbar machen. Whitepaper Z_punkt. Online at: https://z-punkt.de/de/themen/den-kunden-der-zukunft-erlebbar-machen (accessed on 25/01/2021).

Shirky, C. (2008). Here comes Everybody. The Power of Organizing without Organizations. New York: Penguin Press.

Security Affairs (2021). US Govt kicked off 'Hack the Army 3.0' bug bounty program. Online at: https://securityaffairs.co/wordpress/113116/security/hack-the-army-3-0.html (accessed on 03/02/2021).

Slovic, P. (1987). Perception of Risk. Science. Vol. 236, Issue 4799, pp. 280-285.

Speck, U. (2020). Vertrauen ist das Schmiermittel der Globalisierung. Neue Zürcher Zeitung. Online at: https://nzz.ch/meinung/kolumnen/vertrauen-ist-das-schmiermittel-der-globalisierung-ld.1544415 (accessed on 05/05/2021).

Stalder, F. (2017). Kultur der Digitalität (2nd edition). Berlin: Suhrkamp.

Süddeutsche Zeitung (2022). Am eigenen Leib. Online-Belästigung im Metaverse. Online at: https://www.sueddeutsche.de/kultur/metaverse-vr-virtual-reality-microsoft-sexuelle-belaestigung-1.5519527 (accessed on 15/02/2022).

Tagesschau.de (2021). Zukunftsideen der Tech-Konzerne. "Metaversum" als Internet-Nachfolger? Online at: https://www.tagesschau.de/wirtschaft/technologie/metaversum-silicon-valley-internet-101.html (accessed on 02/12/2021).

The Economist (2020). The Metaverse is coming. Technology Quarterly. Online at: https://www.economist.com/technology-quarterly/2020/10/01/the-metaverse-is-coming (accessed on 01/02/2021).

The Economist (2021). What is the metaverse? Online at: https://www.economist.com/the-economist-explains/2021/05/11/what-is-the-metaverse (accessed on 10/11/2021).

TH Köln (2015). "Nutzungszahlen sind die neue Währung" (Interview mit Isabel Zorn). Online at: https://www.th-koeln.de/hochschule/nutzungszahlen-sind-die-neue-waehrung_22617.php (accessed on 10/05/2021).

Wittenhorst, T. (2019). Gegen Hetze im Netz. Schäuble fordert Klarnamenpflicht. Heise.de. Online at: https://www.heise.de/newsticker/meldung/Gegen-Hetze-im-Netz-Schaeuble-fordert-KlarnamenPflicht-4425451.html (accessed on 19/10/2021).

Zak, P. J.; Knack, S. (2001). Trust and growth. The economic journal, 111(470), pp. 295–321.

Strategic Foresight Campaign Office

Torstraße 49, 10119 Berlin, Germany

Phone: +49 30 818777158
Email: kontakt@vorausschau.de
presse@vorausschau.de
Internet: vorausschau.de

Contact Future Office

Michael Astor
Supervision and overall project management at Prognos AG

Anna Hornik
Project management at Prognos AG

Dr Christian Grünwald
Project management at Z_punkt GmbH

Imprint

Publisher
Prognos AG
European Centre for Economic Research and Strategy Consulting
Goethestraße 85, 10623 Berlin

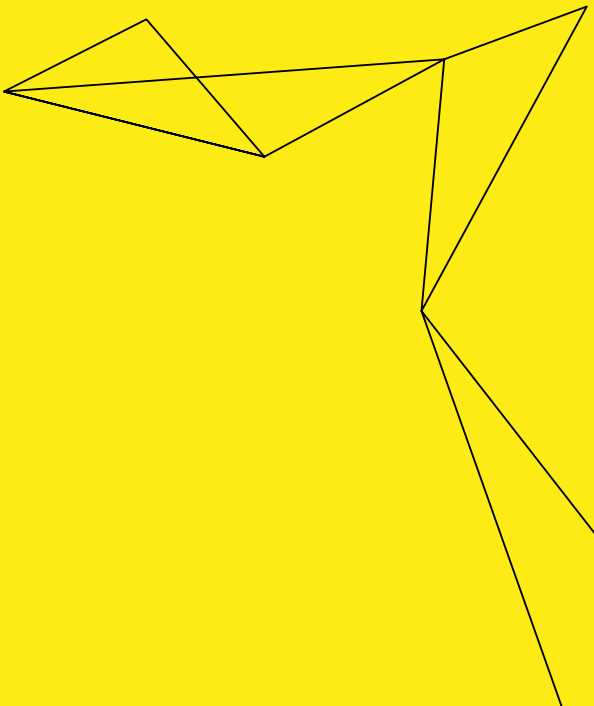
Z_punkt GmbH
The Foresight Company
Schanzenstraße 22, 51063 Köln, Germany

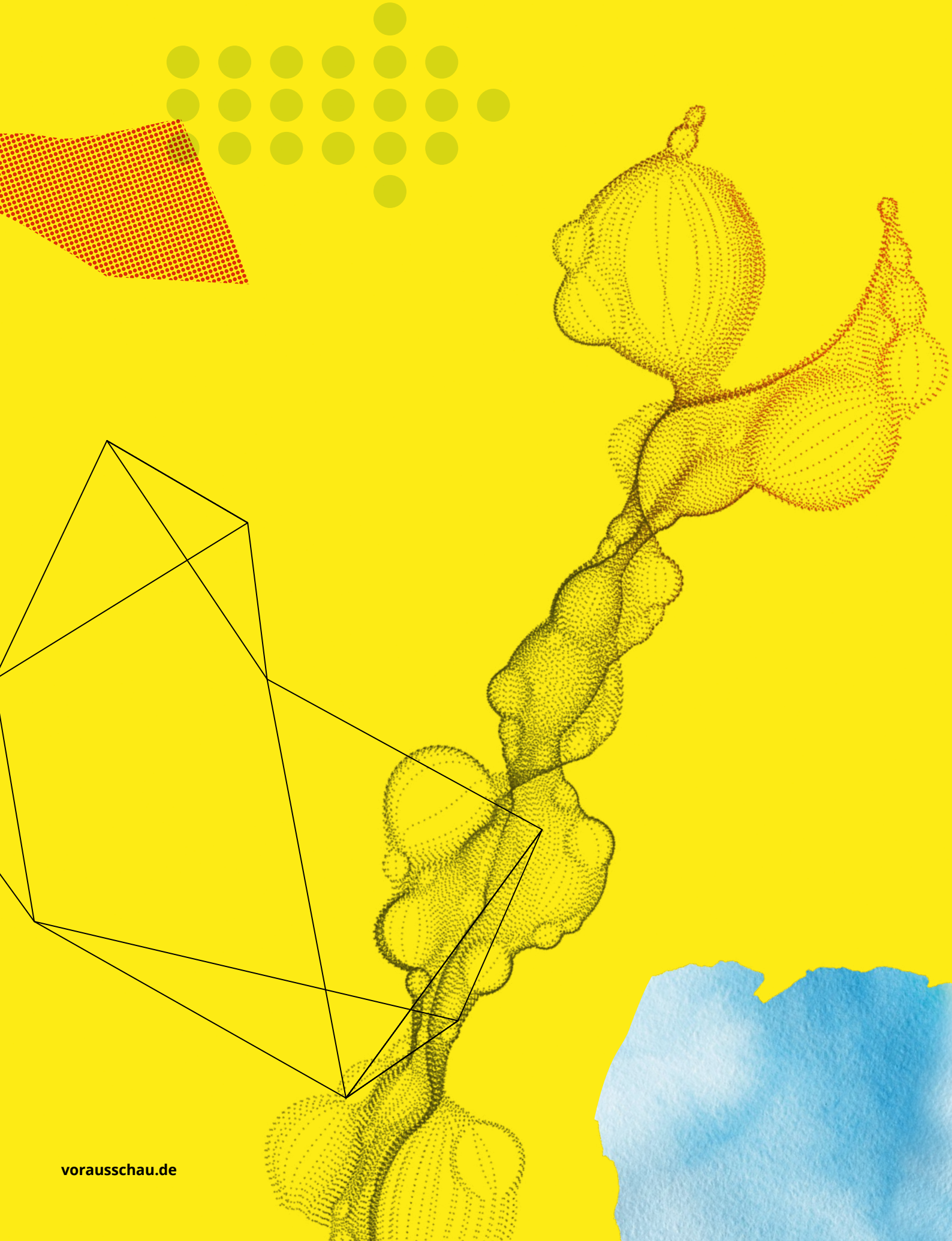
Version
October 2022

Text
Prognos AG
Z_punkt GmbH

Design
familie redlich AG – Agentur für Marken und Kommunikation
KOMPAKTMEDIEN – Agentur für Kommunikation GmbH

This publication is issued free of charge by Prognos AG and Z_punkt GmbH. It is not for sale and may not be used by political parties or groups for electioneering purposes.





vorausschau.de