Deloitte.

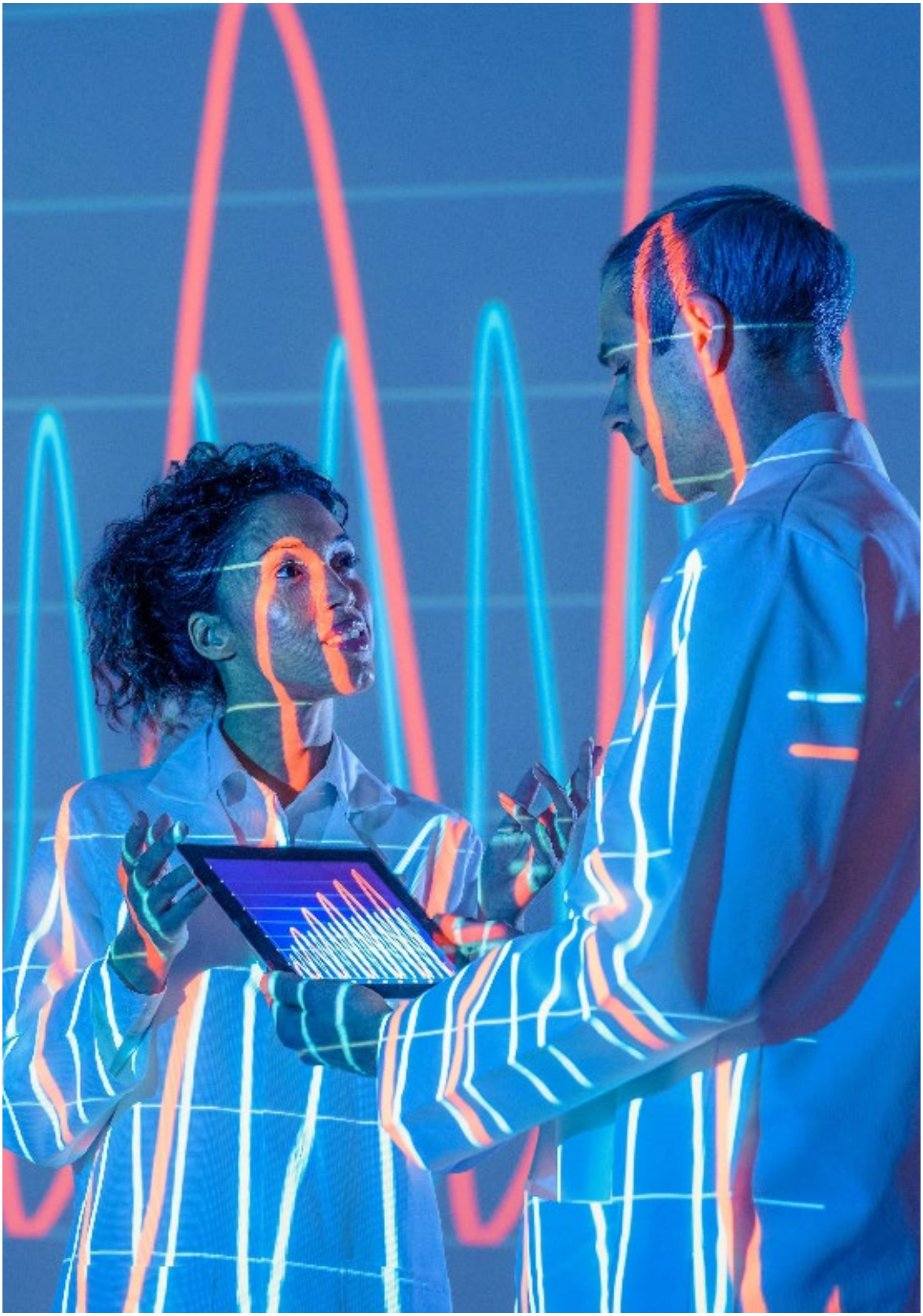
Future of Digital Trust

Driving forces, trends and their implications on our digital tomorrow

MAKING AN IMPACT THAT MATTERS since 1845

"In times of ever-accelerating digital transformation, trust remains the foundation and the only compass we have on our path to the future. We need to get this right and build digital trust in everything we do."

Marius von Spreti, Partner,
Leader Cyber Risk, Deloitte



Introduction

Digital transformation is at the forefront of our minds, now more than ever. The boundaries between our analog and digital world are morphing. Digital is continuously turning out to be more Volatile, Uncertain, Complex and Ambiguous - in short, VUCA (Fig. 1). To combat VUCA, digital trust is key. The unique character of digital trust raises some of the most foundational questions of our time. What forces drive digital trust? What trends will shape our digital tomorrow? How can we successfully build a trusted digital future? How can cybersecurity become the enabler of this future?

Of course, this study cannot answer all these questions completely – digital trust is not this simple. Rather, it requires new thinking and new perspectives on the role and activities of Cyber. Indeed, we see this study as a starting point for engagement and a solid foundation for better strategy and policy-making around digital trust. With our Future Foresight methodologies, we navigate this VUCA world with the aim of finding answers to these urgent questions and building a positive future. Of course, we cannot predict the future. Future Foresight expands our vision of tomorrow and our understanding of the forces shaping our future. It enables us to bring clarity and flexibility into strategies. In doing so, it turns VUCA on its head: from Vulnerability to Vision, from Uncertainty to Understanding, from Complexity to Clarity and from Ambiguity to Agility. This study will give you a glimpse into future foresight thinking, key forces driving the development of digital trust, central trends shaping a trusted digital tomorrow. It will elaborate on major implications these have for all of us as stakeholders in the digital transformation. Join us on a journey into the future – we hope it will be full of insights and impulses for you.

Navigation guide
There are many entryways into the future of digital trust. Depending on your interests, you can you can read the study from front to back cover or jump back and forth between sections in any order.

Fig. 1 – VUCA Framework

Sources: What VUCA Really Means for You. (2014, August 1). Harvard Business Review. https://hbr.org/2014/01/what-vuca-really-means-for-you
Cambridge Dictionary | English Dictionary, Translations & Thesaurus. (2021, February 3). Cambridge Dictionary. https://dictionary.cambridge.org/

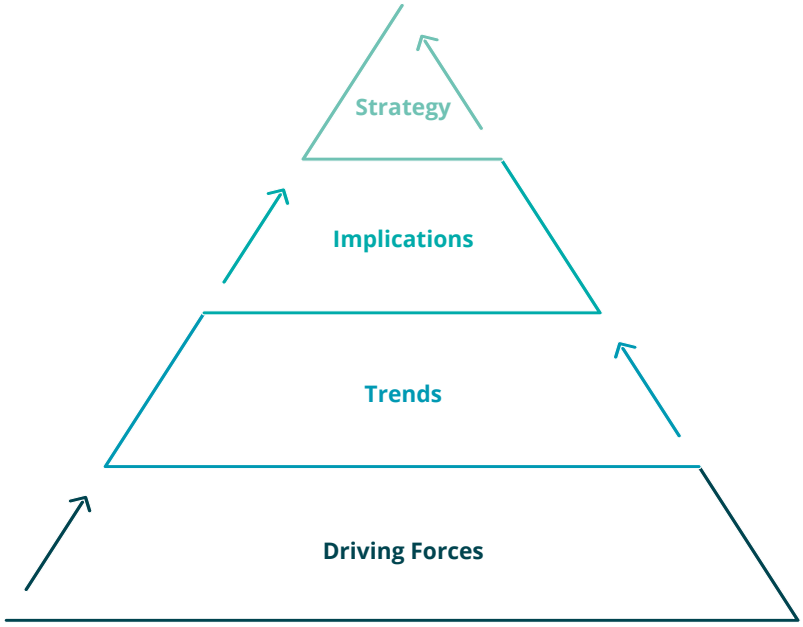
Future Foresight mindset: Setting the framework

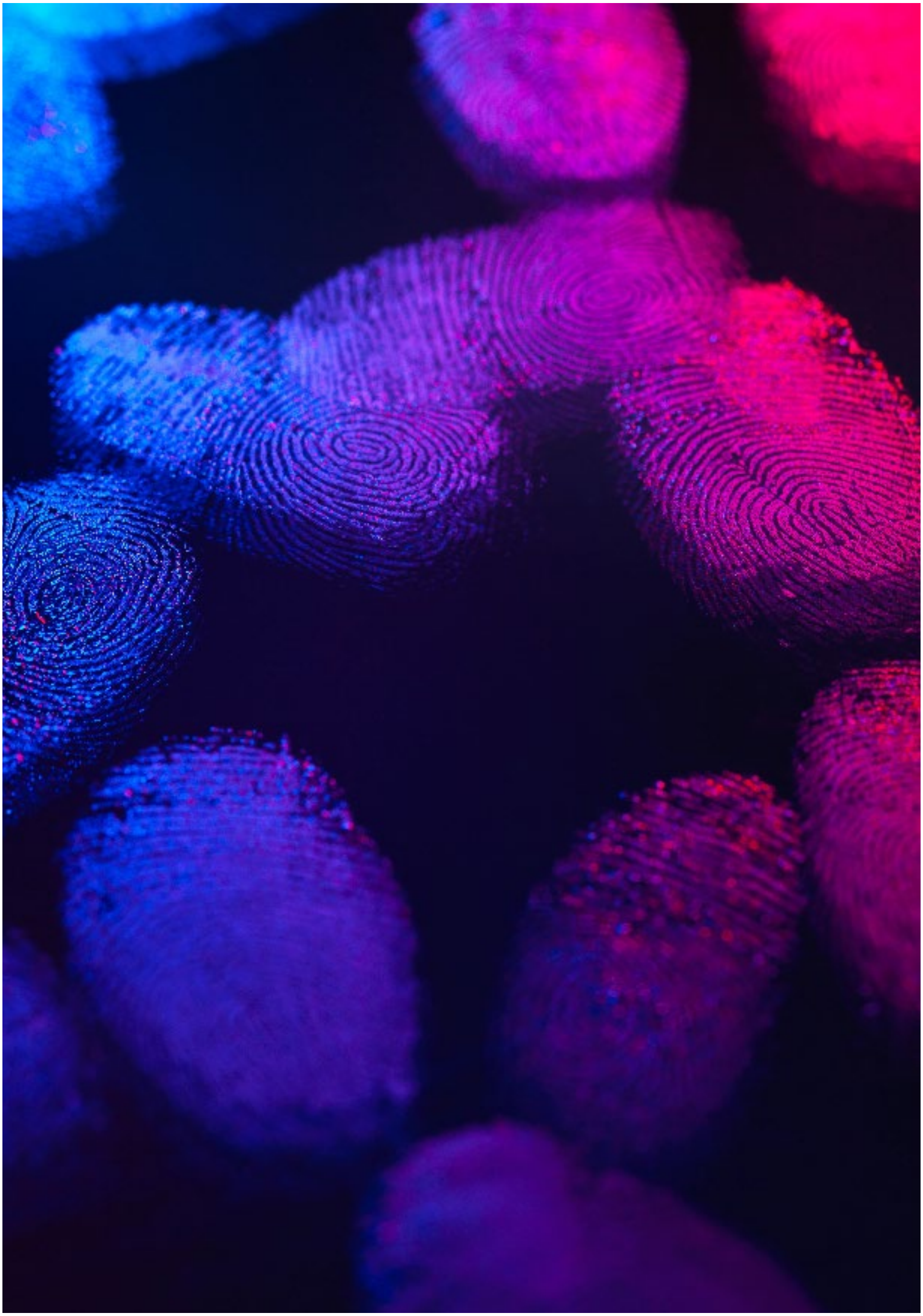
In order to build a successful digitally trusted future, we need to make sense of the continuous developments of volatility, uncertainty, complexity and ambiguity that dominate this field. To understand this environment, it is therefore necessary to reduce and embrace these VUCA-factors. Future Foresight with its unique forward-looking approach does just that by drawing out the driving forces and trends relevant to the future of digital trust.

Driving forces
Driving forces are individual factors that have the potential to impact the future of digital trust. These driving forces can be already established, emerging or on the horizon. The drivers vary in their impact and the uncertainty of their development. They interact with each other and unfold their effects on different levels. We combine cutting-edge AI-based technology with traditional research methods and subject matter expert knowledge and experience.

Trends
To further capture the complex nature of the driver landscape, we identify trends. Trends are overarching developments that hold the potential to shape the future of digital trust. They represent sets of clustered driving forces that are highly interconnected and hence take into account the nature of interaction of the individual forces and its role as a catalyst or roadblock. Overall, trends accelerate our journey into the future by focusing our vision from the complex driver landscape on key determinants of the future. Based on this, we can then gauge the implications these future variables have on digital trust. This enables us to future-proof strategies and policies accordingly (Figure 2). In the spirit of this mindset, we invite you to deep-dive into driving forces and trends, and explore their key implications and strategic impulses in the next chapters.

Fig. 2 – Driver to Strategy Pyramid





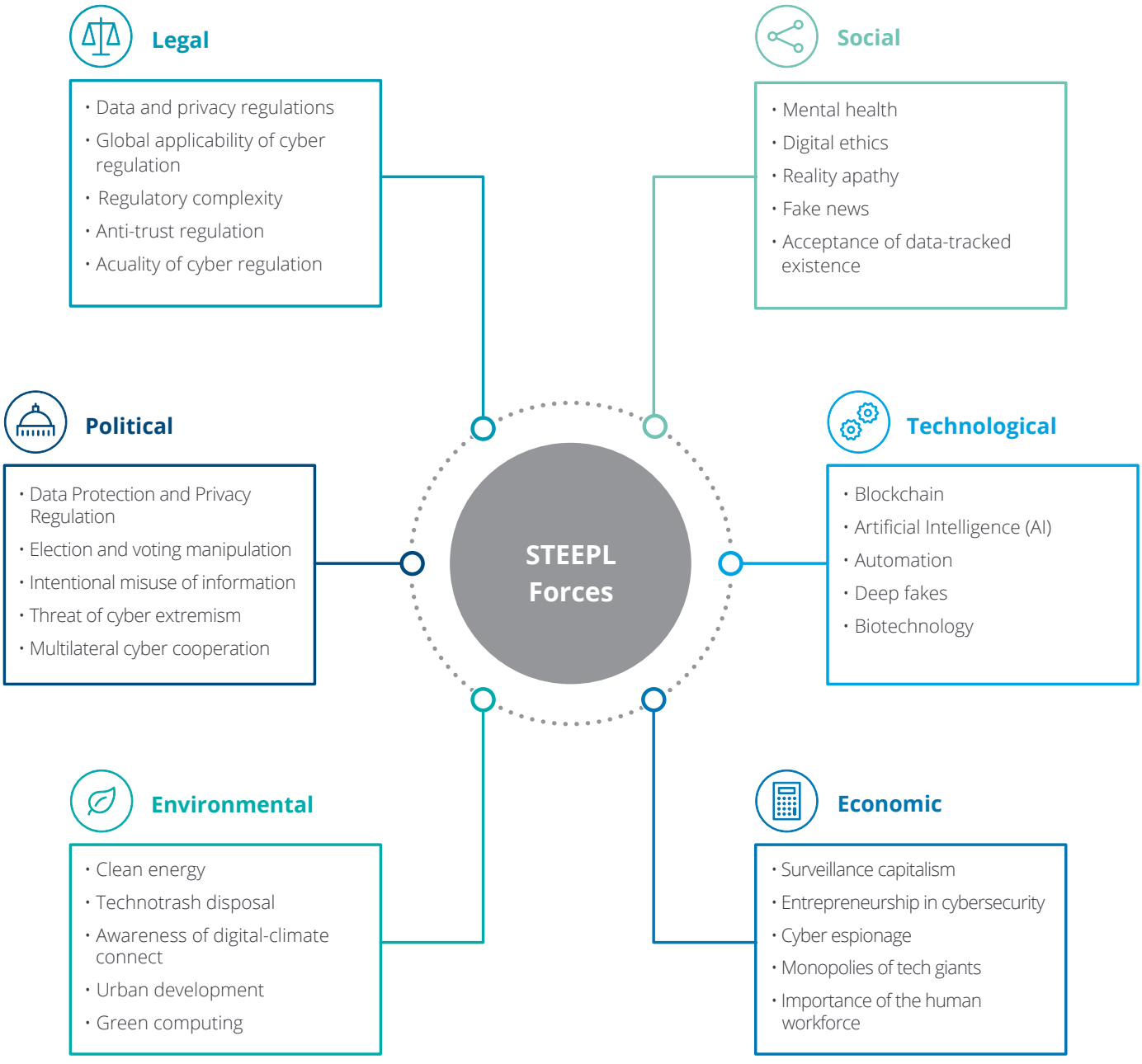
Driving forces: Factors impacting the future of digital trust

A large number of factors with different origins have the potential to shape the future of digital trust. It is necessary to understand these underlying drivers first before we can identify overarching trends. To cut through the complexity of the driver landscape, our approach utilizes AI-based analysis combined with traditional research and expert interviews to find, test and evaluate relevant drivers. In the context of this study on the future of digital trust in 2035, we created a shortlist of 143 such drivers, grouped into the different STEEPL categories of social, technological, economic, environmental, political and legal forces (graphic 3). It is important to note that these categories are not mutually exclusive and collectively exhaustive - individual drivers may fall into more than one category. The STEEPL framework, however, helps to ensure a holistic approach when identifying driving forces. To illustrate the nature of driving forces, we have highlighted selected drivers and their primary STEEPL classifications in Figure 3.

The nature of these driving forces is inherently multifaceted. In order to identify prevalent trends, however, it is key to look at these drivers from different angles by considering their secondary and tertiary STEEPL categories. This requires a multidimensional analysis, as exemplified in graphic 4 for the selected examples of driving forces mentioned above. The plethora of these various complex and interlinked drivers constructs a multitude of overarching high-level developments that shape our digital tomorrow: trends of digital trust.

Fig. 3 – STEEPL Framework

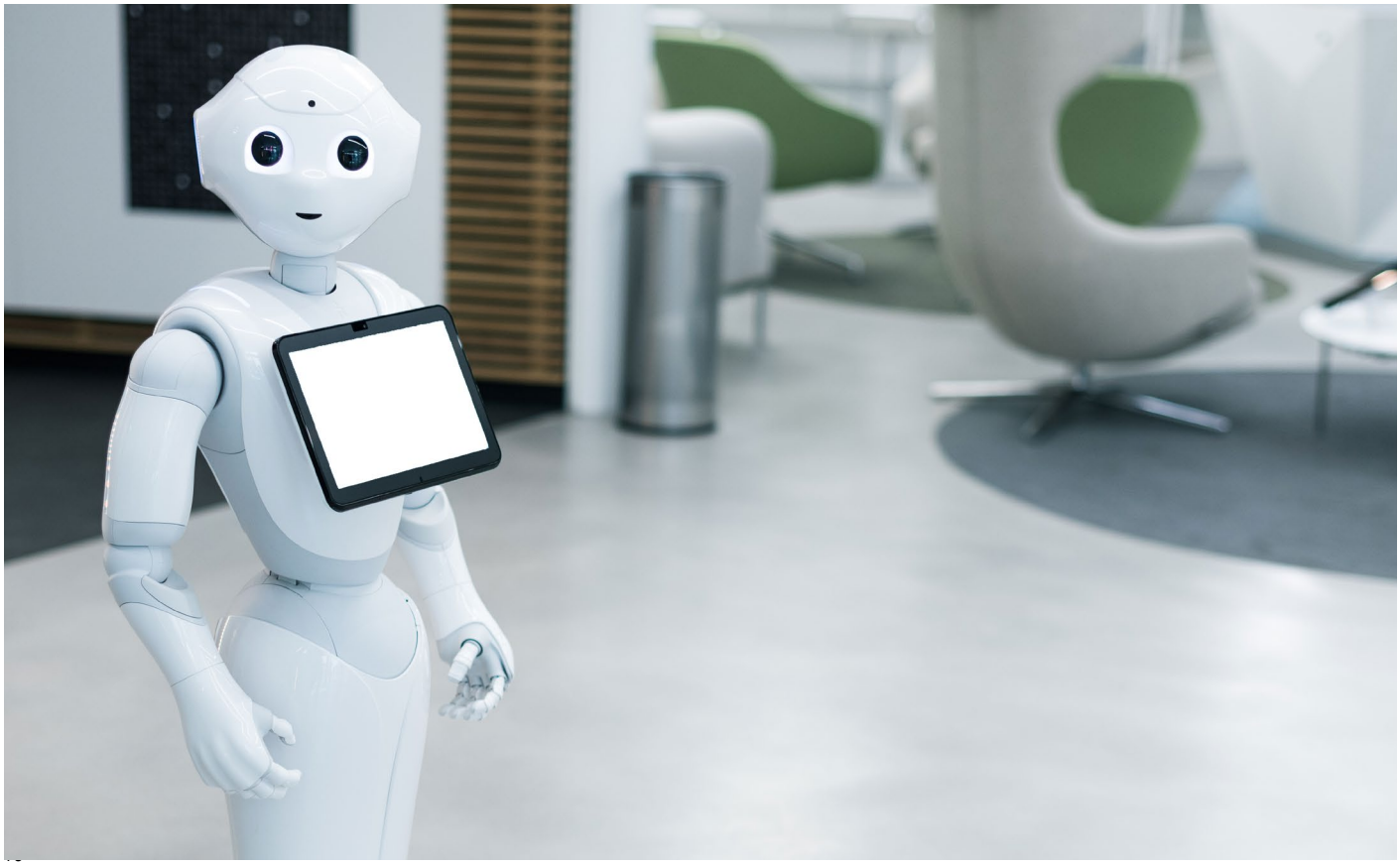
Fig. 4 – Driving Forces Examples

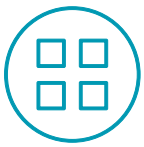


Trends: Overarching developments affecting the future of digital trust

After identifying driving forces for the future of digital trust, it is essential to understand their connection and focus them at a higher level. We have therefore clustered these driving forces into trends, representing overarching key developments that have the potential to determine the future of digital trust. The selected 15 trends highlighted below, by nature of our trend definition, pinpoint new or different perspectives or angles on digital trust. To paint a more intuitive picture of each of these trends, we use exemplary driving forces and personal stories. Visualizing digital trust in 2035 in this way is essential in understanding the multifaceted shading of each of these trends. We therefore invite you to meet Charlie, a European citizen of 2035, who has just received an invitation to a virtual reunion of the graduating class of engineering of 2021. Thinking back to the graduation, Charlie reflects on how digital trust has evolved in these 14 years, both personally and as an engineer. A lot has happened, socially, politically, economically, environmentally as well as from a technological perspective.

Let us fast-forward to Charlie's world in 2035 and portray the different impacts of the identified trends on Charlie's world and the future of digital trust.





1. Primacy of Digital Ethics

The primacy of digital ethics refers to the constant supreme presence and increasing relevance of ethical standards and behavior of individuals, businesses and governmental institutions in the digital environment.

Five selected underlying driving forces for the primacy of digital ethics are social scoring, state censorship, sustainable digital transformation, weaponization of information and data commodification.

Charlie´s world:
In 2035, ethical aspects are a firm component of Charlie's digital environment. Social media platforms screen Charlie´s postings for agreed ethical standards and penalize violations. Newly established governmental authorities check algorithms to prevent discrimination and bias – something Charlie values highly since opting for a non-gendered identity. Charlie firmly believes in this primacy of digital ethics and its implications for trust in the digital environment. However, discussions with Charlie´s colleagues about the differing importance of digital ethics between different countries globally have sharply increased recently. Fueled by ethical concerns, data protection and privacy regulations in the digital sphere are ubiquitous and sometimes slow down innovation, affecting Charlie´s engineering work harshly. Charlie frequently argues with family about whether the resources necessary to uphold the high ethical standards could not be used more efficiently elsewhere. Despite these discussions, Charlie enjoys the trust established by the primary role of digital ethics.

2. Digital Ubiquity

Digital Ubiquity refers to the omnipresence of digital transformation in society, business and the economy as a whole. It is characterized by a shift from the analog to an age in which knowledge, creativity, production and communication are enhanced by digital technologies. It governs the increasing interaction of machines and humans and therefore has the capability to expand the realm of communication from humans to objects.

Five relevant underlying forces that drive the trend digital ubiquity are the globality of cyberattacks, Smart Cities, market concentration of techcompanies, privacy regulations and Artificial Intelligence, Blockchain & other cutting-edge technological advancements.

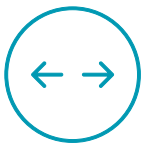
Charlie´s world:
In Charlie's job and personal life in 2035, the digital sphere has swallowed most of the analog age. When planning the day, Charlie uses a digital assistant – a holographic and intelligent robot that advises Charlie on work tasks as well as on grocery shopping and other personal or consumption decisions. Based on Charlie's preferences and realtime data, the digital assistant can take the most efficient and conscious decisions for Charlie. Almost every aspect of daily life is digital and highly interconnected, saving a lot of time and resources. Charlie, however, worries about the security of the digital environment and the lack of human interactions. Connected devices are prone to cyberattacks that can have disastrous consequences for users. And due to the sheer endless digital opportunities to connect, Charlie cannot remember the last physical meeting or meaningful interaction outside of a circle of very close friends and relatives.

3. Hyper Agility

Hyper agility refers to the rapid, connected and dynamic development of society, politics and economy in today's world. The way stakeholders, including individuals, are forced to deal with those developments requires a change in mindset from a rigid interpretation of processes towards extreme degrees of agility. The constant exposure to information technology leads to the interconnection of all parts of life in multilateral dimensions. In every life situation, people see themselves confronted with the necessity to be flexible and fastmoving.

Five exemplary underlying driving forces for the trend hyper agility are: speed of globalization, digital economy, side effects of digitalization, automation, digital innovation.

Charlie´s world:
In 2035, Charlie experiences the speed and impact of digital change faster and stronger than ever before. Hyper agility dominates every aspect of life. The digital services and product developments Charlie interacts with at work are governed by extremely detailed, connected and rapid processes. While this is a challenging environment for Charlie and other humans to navigate, it increases productivity and effectivity. But Charlie notices how this agile complexity also spills over from the economy into politics and society. Charlie worries that the force and agility of this hyper transformation carries the risk of leaving even digitally literate people behind. The coexistence with machines such as digital assistants, wearables and virtual personae has become natural to Charlie, but makes Charlie feel increasingly at the mercy of algorithms. More and more often, Charlie is flying blindly into engineering decisions taken by the machines, unable to divine the reasoning behind them. For Charlie, trust has become a central part of being hyper agile.



4. Polarization

Polarization describes the process of forming one's mindset, characteristics and personality through the multiplicity, complexity and diversity of the information and opinions constantly provided in the digital environment. This encourages the segregation and division of society into contrasting groups with conflicting opinions and mindsets.

Five selected underlying driving forces include fake news, political ideological bubbles, level of inequality, trust in government and poverty.

Charlie´s world:
A distinct characteristic of Charlie's world in 2035 are extreme groupings of like-minded individuals into clubs uninterested in engaging with other opinions. Compared to the early 2020s, Charlie notices that the number of different ideological groups has increased and their opinions have become more extreme. But they also face less challenges from outsiders. Even Charlie's moderate friends and family seem unwilling to move outside their ideological bubbles, consuming only what reflects their already existing opinion with algorithmic accuracy. The society around Charlie has become more and more fragmented and polarized – not just politically, but also socially and economically. Charlie often thinks back to the time where people, including family and friends, engaged in debates or dialogs on controversial questions. Now, contact between people with opposing views is reduced to a minimum. While this is harmonious and comfortable, Charlie misses the heated discussions they had as university students and looks forward to rekindling contact with the other alumni in the graduation class. Instead of being trapped in an algorithmically defined bubble, Charlie has vowed to put more effort into engaging with outsiders.

5. Digital Participation & Ownership

Digital participation and ownership refers to the act of using and proactively becoming involved with new technologies and the virtual world. A resulting difficulty lies in the determination of virtual property rights, the possession of data and allocation of control over a single piece, set of data elements or virtual assets.

Five underlying driving forces include usability of devices, transparency and accessibility for users, participation of non-state actors in cybersecurity, the importance of human rights in the digital sphere and finally, digital user expectations.

Charlie´s world:
In 2035, Charlie has countless opportunities to digitally participate and cocreate. At the level of society and government, governments cooperate with social entrepreneurs in using the steadily improving digital infrastructure to enable Charlie and other citizens to participate in digital legislative processes. Digital governance is a feature of Charlie´s daily life. As an engineer, Charlie works closely with the government and civil society on work projects. Charlie feels that the world has become much more seamless and effortless through the opportunities to participate. Charlie's company, for example, often crowdsources ideas for tricky problems. However, Charlie believes that there is much more potential here, if the polarization issue and the challenge of extending participation reliably beyond the edges of political, social and economic bubbles can be overcome.

6. Digital Dreamification

Digital Dreamification refers to the convergence and integration of the digital world into the physical space enabling consumers to escape from the real world by diving into a virtual, imaginative and illusionist sphere.

Five selected underlying driving forces of the trend dreamification are voice assisted systems, the importance of culture, traditions and values, the cultural value of analog existence and the acceptance of digital substitutes for analog goods and services.

Charlie´s world:
The merging of the digital and analog world has blurred the hitherto clear distinction between online and offline in 2035. For Charlie, this means living in a world where one can very well live a complete life in the digital sphere should one choose to. On new digital platforms, virtual avatars can perform services for other virtual avatars and receive compensation – whether in digital or paper currencies. Charlie enjoys being able to completely reconfigure a person's identity online. As this has restricted the necessity of travelling to holidays, Charlie has colleagues from all around the world working and meeting in their virtual offices. Physical movement in general has become a choice. Charlie´s parents, now confined to a retirement home, are living the dream travelling the world digitally and just sent Charlie a postcard from their digital trip around Australia. Charlie now values any remaining personal contact all the more and cherishes the time spent on analog walks or game nights. This is a much-needed balance to the strains on mental and physical health brought on by digital presence in Charlie´s personal and professional life.

7. Over-Securitization

Over-securitization describes the excessive and uncoordinated investment of resources and services in securitizing information technology, where the continuous investment and over-protection reduces the effectiveness of the measures and can even cause counter productivity.

Five selected underlying forces that drive the trend of over-securitization are user transparency and accessibility for users, offensive and defensive cybercapabilities, data protection and privacy regulation and digital authentication.

Charlie´s world:
14 years after Charlie graduated in 2021, the question of how to mitigate cyberrisks in the digital environment is even more prominent than back then. Charlie's notices with surprise that threats like phishing still work on people in 2035 – Charlie´s company experienced a phishing attempt last month because two competing security programs in the system derailed monitoring and defense functions, creating a dangerous new vulnerability. The 2020s brought the realization that investments in cyber alone will not ensure security. The ensuing flood of cybersecurity products and services has been challenging to navigate under the pressure of digital transformation. The increased legislative appetite for data protection and privacy regulation and global governance of cyberspace has resulted in a security architecture that really confuses Charlie. Charlie feels overwhelmed by even the simplest of the cybersecurity choices necessary for work and private life, and frequently entrusts them to the algorithms behind digital assistants. Thinking back to graduation day in 2021, Charlie has the nagging feeling of having lost control over cybersecurity choices that were once routine for an engineer and digitally literate individual.

8. Digital Cohesion

Digital cohesion can be described as the substantial change in the way humans interact with technology with the aim to enhance their lives. This can be achieved through the collaboration of advanced artificial intelligence technologies with networks to support services that adapt to human behavior in order to better anticipate their needs.

Five underlying driving forces for the trend of digital cohesion include multilateral cybercooperation, sustainable digitalization, digital climate protests, quality of digital infrastructure and digital literacy.

Charlie´s world:
By 2035, digitalization has deeply transformed society, and social cohesion is chiefly determined in the digital sphere. Charlie's social connections are now fully established online and no longer represent merely one more way to connect with others in addition to the traditional physical way. Charlie's digital literacy is a fundamental to transferring social values such as solidarity, empathy and justice into the digital realm. On the other side, digitally less literate citizens struggle to navigate the digital world and be a part of society. Charlie recognizes the danger that more and more people will feel left behind or turn their back on the digital way of life because they cannot accept the inequalities. Charlie is concerned about the already present and emerging grievances among the society that negatively impact the degree of social cohesion in the digital environment and can easily translate into social and political turmoil.

9. Digital Confidence

Digital confidence refers to the aim of creating value through the improvement of trust in digital abilities as a result of closing the skills gap.

Five exemplary underlying driving forces of digital confidence include demand for cybersecurity skills, cybersecurity of digital infrastructures, the closing of the skills gap, trust in political institutions and trustworthiness of information.

Charlie´s world:
In 2035, Charlie and millions of other citizens constantly engage with their highly interconnected digital environment via connected devices like mobile assistants, connected cars, smart homes and smart cities. They feel confident in their analog-digital merged world and have at least a basic knowledge of related fields such as cybersecurity. Charlie´s parents participated in the governmental lifelong learning programs that made them feel confident in the rapidly evolving digital world. Charlie and some friends volunteer as teachers for basic digital literacy at their retirement home, aiming to close this vital skills gap and thus eliminating this part of the generational divide. While the younger generations feel positive and confident about digital progress to tackle new challenges, older generations demand a slowdown and a return to more traditional values. Charlie is starting to feel old, thinking about the upcoming alumni meeting. Charlie can clearly see how the speed of the digital change has already affected various groups of society differently, for example, through digital marginalization. Many, including Charlie, are fearful of a further strengthening of this and of being left behind by the ever more digitally confident younger generations.

10. Conscious Consumer

Conscious Consumer refers to the general awareness of individuals regarding the way their consumption affects the world around them. This consciousness is not limited to the environment but includes an individual's entire lifestyle all the way to data privacy preferences and the awareness of one's own cybersecurity.

Five exemplary underlying driving forces that define and influence the trend conscious consumer are corporate digital responsibility, digital ethics, the importance of integrity and reputation, and clean energy.

Charlie´s world:
Ten years after a public waste crisis in 2025, the producer and consumer behavior has been drastically influenced by an overall increased awareness and also new government guidelines. The establishment of a new ministry of digital sustainability has led to more conscious choices in society and economy. Charlie personally volunteers in an e-trash organization supporting the governmental goal to reduce electronic trash to zero. At work, Charlie already uses a fully recycled digital station. Charlie also programmed a digital assistant to automatically reject products and services that do not have a completely neutral carbon footprint. Charlie´s friends and family share these preferences. For businesses, the demand of the conscious consumer has led to a rethinking of existing business models, including in Charlie´s engineering world. In the digital environment, climate neutrality has become the norm.

11. Human Commodification

Human commodification describes the objectification and downgrading of the individual to a pure service provider who is classified as a good or product which leads to the disappearance of the human aspect within the digital economy.

Five exemplary driving forces of human commodification include the importance of human workforce, data commodification, reality apathy, automation and Industry X.0.

Charlie´s world:
In 2035, the digital economy is more than ever driven by data and machines. In this environment, Charlie often feels the role of humans in the economy and society reduced to two positions: being a production factor or a product itself, as well as a consumer in turn feeding the digital world with data. At Charlie´s workplace, an internal rating system displays high and low performers on a monthly basis to all staff. This has led to extremely high levels of productivity, and the company is now more successful than ever before. At the same time, Charlie feels highly pressured and worries about the growing number of valued colleagues that leave the company. The same scoring is used by Charlie´s health insurance to calculate incentive premiums for healthy living. Charlie also voluntarily provides data on daily social interactions to help the algorithms provide a person with the best possible routine to maximize free time with family and friends and maintain a personal digital-analog balance. Charlie is grateful that this helps anyone sustain a healthy lifestyle at times when it is easy to get lost in the digital jungle.

12. Digital Health

Digital health refers to the health consciousness of individuals regarding psychological and physical effects of a digital-driven lifestyle. This includes the more effective and efficient use of technology to support healthcare and a healthy lifestyle.

Five selected key underlying driving forces of the trend digital health are mental health, digitally assisted health and well-being, quality of life, the digital divide and polarization.

Charlie´s world:
The health of citizens is a top priority for businesses and governments in 2035. Charlie enjoys many technological advancements in the health sector – fridges that suggest healthy meals based on available ingredients and personal health status, health robots in the supermarket that help people plan their meals, or technologies that massively reduce water and space usage in food production. Advances in Artificial Intelligence and biotechnology promise solutions for diseases that were thought to be without cure, and early warning and intervention systems when initial risk factors and symptoms emerge. At the same time, Charlie realizes that the progress of digitalization has also led to serious mental health issues among friends. At times, Charlie personally struggles with the dark sides of digital life - whether it is the constant feeling of being connected, analyzed and categorized or the pressure to not miss out on the latest trend.

13. Revolutionized Security

Revolutionized security describes the emergence of new digital threats that are more complex and volatile leading to a paradigm shift and a new definition of threats and security issues. Security has become interdisciplinary, reaching beyond technological aspects and encompassing various fields and disciplines, and creating a new kind of complexity. Novel threats require new, revolutionized security measures needing to be weighed against the restrictions they cause on freedom.

Five selected driving forces for the trend revolutionized security include cost of cybersecurity solutions, cyberattacks, hacking, cybersecurity of Critical Infrastructure and weaponization of information.

Charlie´s world:
In the 2020s, Charlie experienced a number of large and small scale, AI-powered cyberattacks that severely shook society. Eventually, a ransomware attack on the smart home door system locking Charlie out of the apartment opened Charlie's eyes to the need to rethink security. Charlie decided to protect smart home devices using some of the new security ecosystems on the market. New digital threats and priorities and the need to protect the exponentially growing heaps of data prompted international organizations to focus on regulating the digital sphere. Just this morning, Charlie watched a political discussion on digital borders and noticed how these revolutionized security concerns create a higher willingness within society to accept restrictions of individual freedom in order to improve security. Charlie also feels more secure with revolutionized security technologies but at the same time wonders how far society will go along. Charlie's own parents have already opted out of a few health care services because of such concerns, and are now no longer able to access certain offers of their retirement home. This makes Charlie thoughtful.

14. Identity-making

Identity-making refers to the virtual identity as a form of self-representation which can be influenced by the individual's activity within the digital environment and forms and influences one's mindset, characteristics and personality. In this context, individuals are able to create a digital existence or persona resulting in a shift of emotional and interpersonal dynamics.

Five selected underlying driving forces of identity-making include online opinion manipulation, net neutrality, the influence of social media, quality in algorithms and political and ideological bubbles.

Charlie´s world:
In 2035, Charlie is part of a new popular social media platform for identity enhancement. Virtual Charlie includes personal aspects that an individual would like to improve, creating a constant source of motivation to follow through with plans and resolutions. Recently, the platform showed Charlie playing a difficult Mozart piece on the piano, triggering Charlie to actually learn the piece. Mastering it made Charlie both content and proud. The underlying algorithms collect user information from other social media applications and automatically connect Charlie with matching interests. For example, having mastered the Mozart piece, Charlie now gives piano lessons to others. This way, people can take full advantage of their skills and connect with like-minded individuals. However, Charlie worries about the platforms´ commitment to data protection and privacy amid unending reports of data breaches and hacking and is also worried about the emergence of ideological bubbles on the platforms. Because of the algorithms, users overwhelmingly meet only like-minded folk, creating fragmentation and polarization.

15. Digital Discrimination

Digital discrimination in general refers to the unjust treatment of individuals in the digital environment on grounds of their respective characteristics of these people. The distinct and new component of digital discrimination compared to traditional forms of (cyber) discrimination are the different shapes it can take. Traditional cyberbullying on social media and communication platforms represents only one eminent example of digital discrimination. The different or unfair treatment of individuals based on their personal data that is automatically processed by an algorithm (-bias) represents a second form. To the same extent, net neutrality, digital literacy and the question of equal access to hard- and software as well as infrastructure play an important role in digital discrimination.

Charlie´s world:
In 2035, Charlie experiences the world in the prime time of digitalization. All ongoing developments and newly developed technologies create very comfortable benefits for most people. Charlie is grateful for the advances in digital literacy and digital neutrality such as agenderness. However, technological advancements continuously open up new levels of discrimination. Charlie has noticed that friends with lower and higher voluntary scoring ratings often have different access to products and services. Implicit and explicit cyberbullying is still an omnipresent topic in the social discourse, and algorithms and their biases continue challenging society on new levels. Only last week, Charlie felt bodyshamed by the digital assistant purchasing a new diet plan and a new wardrobe to support Charlie´s desire to find a partner. Charlie´s parents also complain about their lack of access to the newest technology in the retirement home, which limits them in their digital mobility.

Building a trusted digitally transformed future today: Trend implications and cybersecurity as an enabler for digital trust

Cybersecurity is key to attaining a trusted digitally transformed future. If employed sustainably and strategically, cybersecurity can enable us to reap the benefits of digital transformation in the private and public sector as well as in society at large. The landscape of driving forces and their interconnection in overarching trends has reduced the complexity around digital trust. Now it is up to us to reap the benefits this brings in leveraging opportunities and dealing with threats. This requires us to proactively employ the large potential of cybersecurity for digital trust.

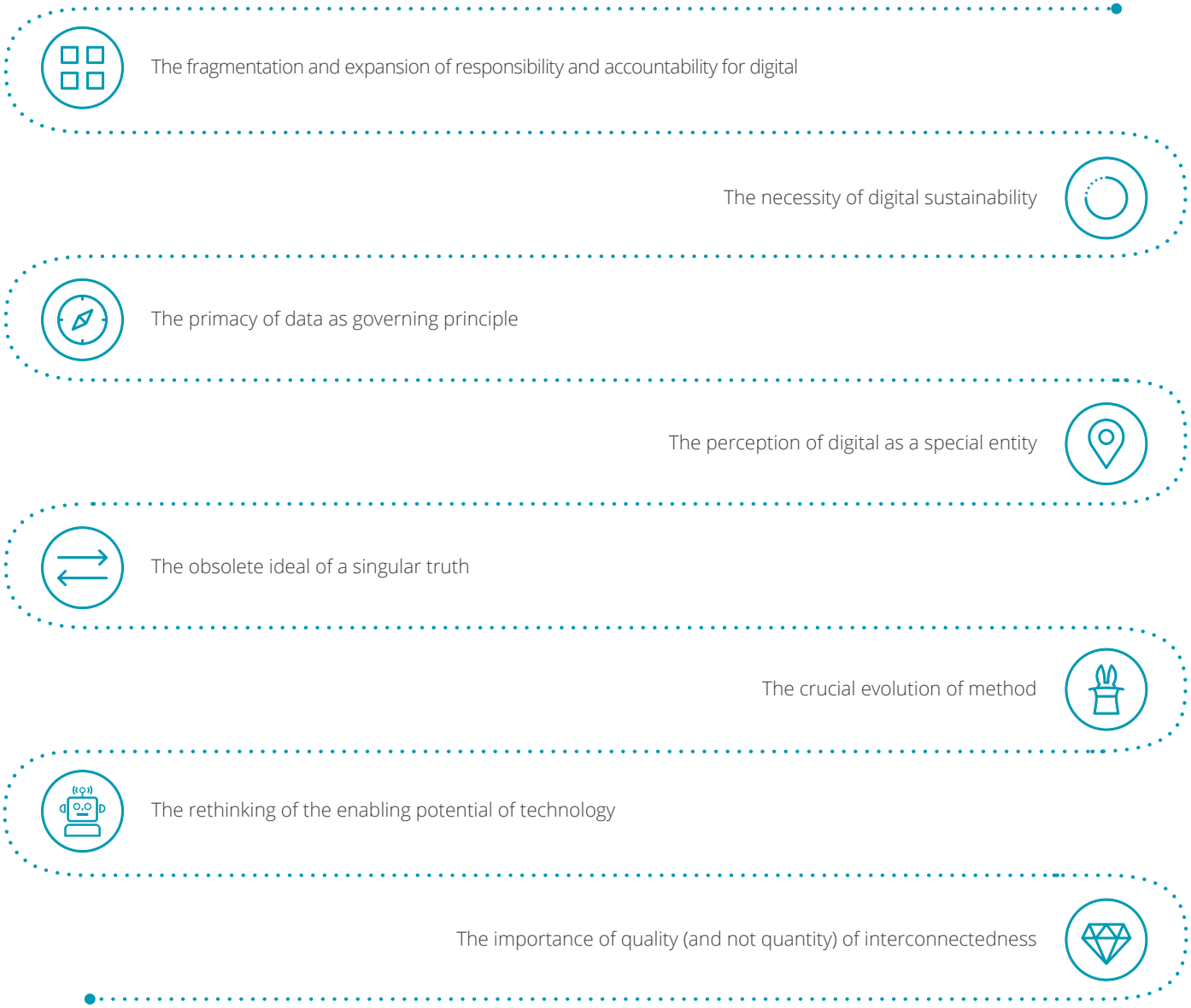
To do so, it is essential to first consider key implications of the interaction of these trends. This allows us to draw out their implications, cutting through their complexity and capturing their uncertainties, thereby laying a solid foundation for strategic planning.

These implications form the individual fields of actions for stakeholders. In this context, they illustrate the consequences that can arise when interconnected trends unfold their impact on the future of digital trust.

Of course, there is a vast field of implications arising in different dimensions. Implications may vary in focus, scope, impact and importance depending on sectors, industries and individual context. Strategies, in turn, must be adapted to this individual situation. That said, there are certain key implications that can be seen across all fields. These key implications are consequently at the core of building a digitally trusted future and formulating cybersecurity strategy to enable this. While not all of them are new, tackling them as prioritized fields of action is crucial for building a successful future.

Based on our 15 key trends, we have highlighted eight of these key implications. While the individual context of actors must be considered, many key impulses arise from looking at what these implications mean for different sectors, industries and core business priorities.

Fig. 5 – Implications Overview



1. The fragmentation and expansion of responsibility and accountability for digital

Based on the interplay of trends such as the primacy of digital ethics, digital cohesion and digital ubiquity, a responsibilities and accountability for the digital is expanding and fragmenting rapidly. Actors previously not responsible or accountable for digital trust are acquiring responsibility for ensuring a trustful digital environment, including cybersecurity as an enabler of digital trust. At the same time, accountability is being extended to a wide variety of stakeholders within both private and public sector organizations. Actively driving this diversification of roles and stakeholders will be key for a digitally trusted future.

"Distributing the cyber task on several shoulders is not a new trend in the public sector, it is already implemented in the political and organizational structure of the government world. The growing complexity of the topic requires stronger and well-orchestrated interaction between all stakeholders in the military forces, civil government – state and local – but also in the interface to society and the business world. Only if it is agreed that we are part of one big cyber-orchestra, will we be able to counter the adversaries."

Peter Wirnsperger,
Lead Civil Government

2. The necessity of digital sustainability

Building on a combination of trends including conscious consumer, digital health and digital dreamification, sustainability is spilling over from the analog into the digital sphere and reaching new dimensions there. As in the physical world, this goes far beyond but still includes environmental concerns. Digital Sustainability delineates in particular the undeniable requirement to construct a trusted digital ecosystem that finds a balance to political, social, economic, legal, technological and environmental concerns, for example with regard to digital healthcare or privacy. Navigating the resulting trade-offs is key in a forward-looking cybersecurity strategy.

"Trust and transparency are key for sustainable management. Integrating sustainability practices within an organization's enterprise applications enables leaders to better manage financial and non-financial processes in an integrative and trustful manner. Tracking and tracing the implementation of sustainability measures digitally will be integral to measuring its impact. At the same time, this will make sustainability measures transparent and satisfies the ever growing regulative and stakeholder information requirements."

Viola Möller,
Senior Manager Strategic Risk

3. The primacy of data as governing principle

With the continuously growing amount of increasingly diverse types of data, data primacy is transforming from a guiding to a governing principle of digital trust. Expanding much beyond the legal questions of data privacy and regulation, data governance is moving to the center stage of digital trust. Data Ownership is shaped by the connection of a variety of trends, including digital participation and ownership, human commodification and identity-making. To enable a trusted digital transformation, this must be acknowledged proactively in cybersecurity strategies.

"The rules by which our data is used in digital sphere must ensure the protection of personal rights. Data protection is an important foundation for harnessing the technological benefits while at the same time safeguarding our personal rights, which define us as a free society."

Stefan Buchholz,
Partner Cyber Risk

4. The perception of digital as a spatial entity

As digital transformation progresses, the digital sphere is increasingly taking form as a distinct spatial entity. The mapping of this entity by private and public as well as civil society stakeholders is taking more and more sophisticated shapes. In this process, the boundaries between the analog and the digital become increasingly blurry. At the same time, the perception of the digital as a space in its own right becomes more and more distinct. This acknowledgement goes hand in hand with the necessity to realize that this development of space must be managed. As the symbiosis of various trends such as over-securitization, revolutionized security and digital confidence accelerates these changes, cybersecurity plays a central role in managing cyber space.

"The only constant in the digital space is change – standstill is dead. We – as organizations and as individuals - must adapt to this exponential speed of change as the new normal. Otherwise, we will not have a future in the digital space. For this, digital trust is key. This is the new law."

Christian Düwel,
Senior Manager Cyber Risk

5. The obsolete ideal of a singular truth

Driven by the catalyzing effects of combined trends such as polarization, hyper agility and identity-making, (dis)information spread, intake, verification and prioritization are becoming increasingly uncontrollable and diversified in nature. Established institutions and organizations of trust increasingly bear the responsibility of shedding light on the different shades of the "correct answer". The ideal of a singular truth is outdated. This brings a multitude of opportunities to diversify our narrative on digital trust in the present and the future, but also holds the challenge of disinformation and its use for political or economic purposes. Cybersecurity strategies must answer to this.

"Trust is the cornerstone and primordial design principle of Blockchain. Some call Blockchain the trust machine. It has a disruptive potential in that it eliminates intermediaries who used to fill the void of trust in non-Blockchain scenarios, and thus gives rise to unforeseen new business models."

Sven Buschke,
Senior Manager Blockchain Institute

6. The crucial evolution of method

The interaction of such trends as hyper agility, digital confidence and digital ubiquity requires a transformation in our thinking about methods. Models, methodologies and approaches are increasingly being hailed as the solution for making digital transformation successful. However, methods and models are tools that must evolve, in line with evolving business models, to keep up with the exponential speed and development of digital transformation to continue being useful in building a trusted future. Building on this principle in cybersecurity is a key component in establishing strategies for digital trust.

"Especially in "times of calm and happiness", building digital trust should be part of every institution's DNA. This allows a company to take a leap of faith when an emergency or crisis strikes. Emergency and crisis management actually demand the same degree of agility and speed as digital transformation. However, hasty decisions resulting from this must be avoided for the sake of reliability and credibility of actions taken. This is how companies can achieve the ultimate goal of building a trustworthy future under emergency and crisis conditions."

Max Kaiser,
Manager Cyber Risk

7. The rethinking of the enabling potential of technology

Technology enables us to reach further. This is not a new idea. However, the technology's potential to do so is developing rapidly. The sheer complexity of fast-paced technological developments and their open availability on the market is resulting in a disabling potential that can do anything from influencing to paralyzing stakeholders. Walking the tightrope between the enabling and disabling potential of technology is key in building digital trust. The interplay of trends such as revolutionized security, digital ubiquity and human commodification results in the necessity to rethink the often unchallenged, enabling potential of technology. This is necessary to ensure conscious and informed decision-making on the use of technology as a tool in cybersecurity and beyond. This in turn will allow public and private stakeholders to leverage the enabling potential of technology more fully and comprehensively and build tailored, smart and differentiated problem solving approaches.

"We are on the way to a cashless society. The acceptance of digital payments not only depends on the convenience, but also on the trust in secure and relia-ble payment processing technology. This must be ensured by legislation and the payment service providers."

Daniel Hellmann,
Director Cyber Risk

8. The importance of quality (and not quantity) of interconnectedness

With trends such as digital ubiquity, digital confidence and digital cohesion interacting constantly, interconnectedness is expanding its place at the forefront of everyone´s mind. Within this, the focus is shifting from the quantity of such interconnectivity to the quality of the resulting interconnectedness. The changing form of connections between humans and between humans and machines accelerates this development. (Digital) trust is a key component in building and managing these connections successfully. Cybersecurity is therefore a key enabler for making this transformation a fruitful one for both the private and public sector.

"Cloud accelerates global interconnectedness and enables users to access resources on demand from anywhere with any device. While this allows new business models and changes the way of working and living, the quality – and also the security – of these connections is key to maintaining digital trust."

Ellen Dankworth,
Director Cyber Risk

Conclusion

Building a trusted digital tomorrow requires us to start today. This study intends to serve as a foundation and starting point for this construction work. This is not going to be simple. Understanding the many different driving forces and trends and their implications is the first step to building successful policies and strategies for digital trust. To implement these in the long-run, private, public and civil society stakeholders need to not only cooperate, but bring together interdisciplinary expertise across political, social, economic, technological, legal and environmental fields. The key implications highlighted here give a first field of actions in this undertaking. To successfully and proactively tackle these implications, stake-holders must change the conversation: away from looking backward at what has been or should have been done in the past; forward to a vision of digital trust built on clarity and understanding, enabled by strategic agility. In short, a conversation that turns VUCA on its head. This study is intended to be a first step in this direction. We are ready to go ahead and make an impact that matters on digital trust – will you join us?

"The future needs a new, positive narrative on digital trust. Future Foresight lays the foundation for this by capturing and focusing inherent complexities and uncertainties. This puts all of us as stakeholders in digital transformation in the extraordinarily powerful position to change the conversation on digital trust. And to consequently build the digitally trusted tomorrow we would like to see."

Peter Wirnsperger
Lead Civil Government

Appendix

Future Foresight, the analysis of future developments, aims to expand our vision on and understanding of the forces shaping tomorrow. Deloitte has developed approaches to structure Future Foresight thinking to achieve valid and useful results. This includes a variety of different methodologies to constructively engage with the future, such as horizon-scanning, trend-sensing, wildcard analysis, future readiness assessments and – in cooperation with the Deloitte Center for the Long View – scenario analysis. While Future Foresight does not attempt to predict the future, it enables stakeholders and decision-makers to engage with the future and proactively shape it, instead of merely reacting to it.

For this study, we followed our basic Future Foresight trend-sensing approach:

Step 1: Definition of the focal question

In order to set the focus of the study, the focal question was defined in a first step. Its purpose is to pinpoint the factors and topics relevant to the study and to ensure a common understanding of the future of digital trust. Part one of the study was guided by the following research question: "What drivers and trends will form the future of digital trust in society and economy between now and 2035?" The question guiding part two was: "How can we make cybersecurity an enabler for a sustainable and trustworthy digital transformation?"

Step 2: Identification of drivers

In a second step, future drivers were identified and analyzed. The overarching goal of this second step is to create a shortlist of the most relevant driving forces, i.e. variables affecting the future of digital trust. A threefold process was followed to identify key driving forces. In a first step, we utilized Deep View, our AI-based trend-sensing and analysis tool. Deep View uses a proprietary natural-language processing software to conduct extensive analyses of articles, blogs, M&A transactions and patents. Deep View reads and understands the output of more than half a million sources within seconds, creating trend-based knowledge maps of interrelated current and developing topics. Complementary to the AI-based analysis, we conducted traditional desk research and expert interviews to combine human and machine intelligence. To ensure the holistic character of the drivers list, we employed the STEEPL framework, focusing on social, technological, economic, environmental, political and legal factors.

Step 3: Clustering of trends

In a third step, we clustered the identified driving forces into trends by analyzing their interrelationships and linkages across the different STEEPL categories. This way, we identified 15 over-arching trends that represent interconnected sets of underlying variables.

Step 4: Analyzing trend implications and deriving cybersecurity Future Impulses

For this study, the final step aimed at engaging with the identified trends to analyze their key implications and to derive selected future impulses for the role of cybersecurity as an enabler of digital trust in the future. Implications are defined as the opportunities and challenges potentially arising from the identified trends. A workshop with a diverse and senior Deloitte Cyber leadership team examined the trend implications and generated cross-industry cybersecurity Future Impulses.

For more information on our Future Foresight methodologies or further Future Foresight studies, visit our Future Foresight website or contact us.

Fig. 6 – Future Foresight Trend Sensing Methodology

Overview over the methodological process followed for the future of digital trust study

Your contacts

We look forward to a vibrant exchange of experiences and approaches – get in touch with us to find out more.

Marius von Spreti
Partner | Cyber Risk Lead
Tel: +49 89 29036 5999
mvonspreti@deloitte.de

Peter Wirnsperger
Partner | Lead Civil Government
Tel: +49 40 32080 4675
pwirnsperger@deloitte.de

Max Kaiser
Manager | Cyber Risk
Tel: +49 40 32080 4017
mkaiser@deloitte.de

Contributors
Annina Lux, Maximilian Lobbes, Stefan Buchholz, Ellen Dankworth, Katharina Pfeil, Max Kaiser, Anton Göbel, Franziska Biberacher, Marga Wenner, Tim Oerter

Deloitte.

Issue 08/2021