
Ruling the future
of digital trust and
cyber(security) 2035
Writing the story of a successful
digital tomorrow
Capgemini invent

Table of contents

01 Introduction

Ruling the digital. Writing the story – Building digital trust and cyber(security).

Rule the digital.

Arguably, the world has seen various paradigm shifts before – monumental changes that have redefined how we see, think about, and do things. The sheer complexity of "the digital world," the impermanence of its development stages, and the utter disruption caused by its innumerable angles lead to a never-before-seen degree of what is often perceived as complete chaos. However, the digital world is not unruly. It can – and must – be governed. That is where Strategic Foresight can help and therefore has never been more relevant.

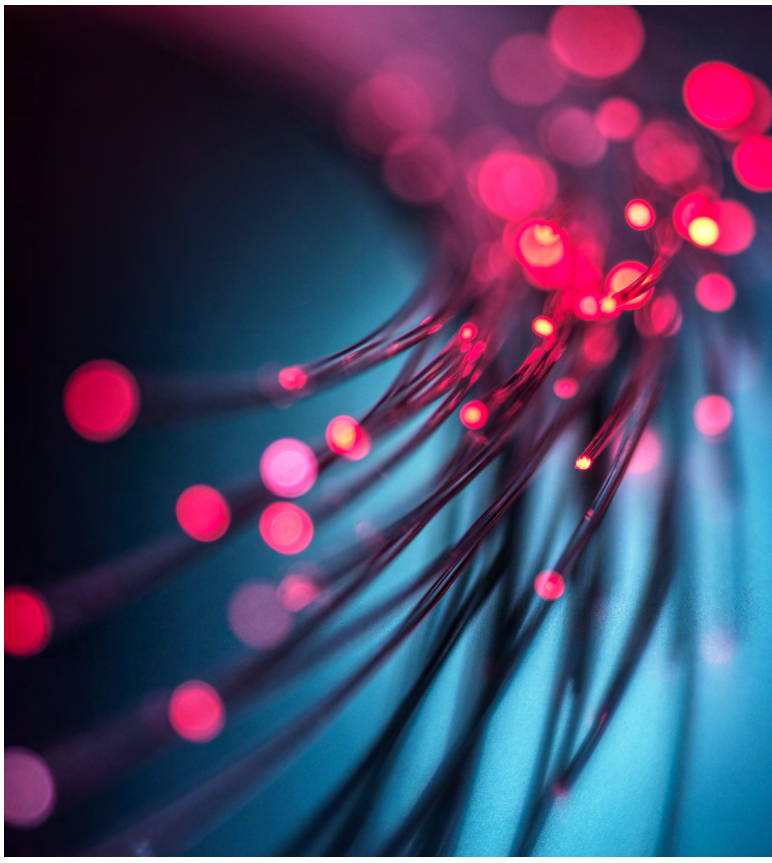
To do so, we must understand it and all its facets, their interaction, and their impact. We must look at the factors that drive change, at the aspects and circumstances that cause turbulence, and at the resulting short-, medium-, and long-term change. Unlike often claimed, Strategic Foresight is not the solution here – but it is the means to get there. No methodology of Strategic Foresight will magically predict the digital future. It is not simply misleading and short-sighted, but highly dangerous to claim or believe so. What Strategic Foresight methodologies will help us do is to uncover driving forces and their relationships with each other, to untangle complex compounds of factors and developments. As Ramírez and Wilkinson so pointedly put it: "learning with, rather than from, scenario planning."[1] This also applies to other Foresight methodologies. Strategic Foresight can help us to re-think and re-perceive how we see, think about and do "digital". It allows us to rule our digital future.

Write the story.

The amount of stories to be told about the present – let alone the future – of digital is countless. Not all of these stories are success stories. This study has one central goal: to lay the foundation for a positive digital future story. A story we write ourselves for a future we build ourselves. It focuses on two things: scanning and analysing the various driving forces at work in the digital world, and thinking alternative future scenarios of how this world could turn out. These alternative stories of the future then form the foundation for a conversation on what story we want to write on the future – our preferred future, the vision we work for and towards.

Build digital trust and cyber(security).

A key question in the endeavor to capture the digital is how to frame this fast-paced, ever-changing field. We believe it is vital to approach it from two angles: the people-centric dimension of "digital and trust", and the more technologically-centric dimension of "cyber and security". In this context, we deliberately use the term "cyber(security)" to reflect the broader scope of our analysis: while security remains a core topic, the concept of cyber encompasses far more – including digital infrastructures, resilience, sovereignty, and innovation. Needless to say, both of these angles are intrinsically linked, and attention needs to be paid to the connection between the two dimensions. While our analysis focuses on Europe, it is important to place these considerations within a global context, as digital transformation and its implications transcend borders. Ruling both of these in a meaningful, interconnected way will allow us to first write, then build a positive digital tomorrow – across all fields and topics. We look forward to constructing the future we want – and need – with you!

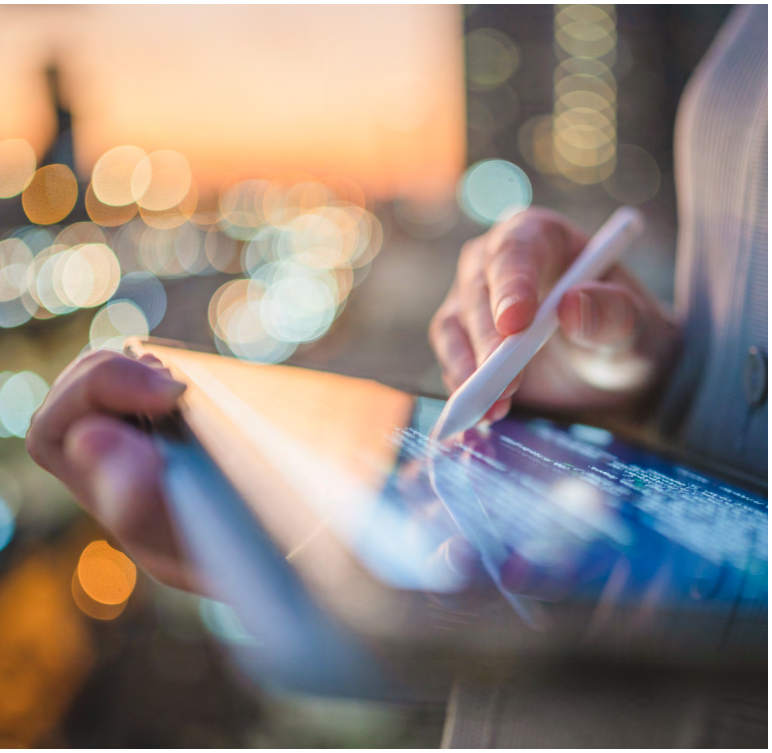


[1] Rafael Ramírez and Angela Wilkinson, Strategic Reframing: The Oxford Scenario Planning Approach (Oxford: Oxford University Press, 2016), p. xiv.

02

Ruling the digital with Strategic Foresight

How to write the story of a successful digital tomorrow.



Strategic Foresight is uniquely positioned to support us in building positive futures. While scenario planning is perhaps the most widely known methodology of the field, others are no less interesting.

Our Capgemini Invent Foresight Force specialises in a variety of Foresight methodologies, including horizon scanning, trend-sensing, risk- and threat-sensing, wildcard mapping, risk and threat scenario definition and scenario planning, as well as Foresight flight testing and future planning & roadmapping based on these methodologies. Each of these has its own raison d'être. With this study, we aim to pinpoint significant changes and highlight possible futures as a basis for strategic decision-making around digital trust and cyber(security) towards 2035. We therefore decided to focus on horizon scanning and scenario planning.

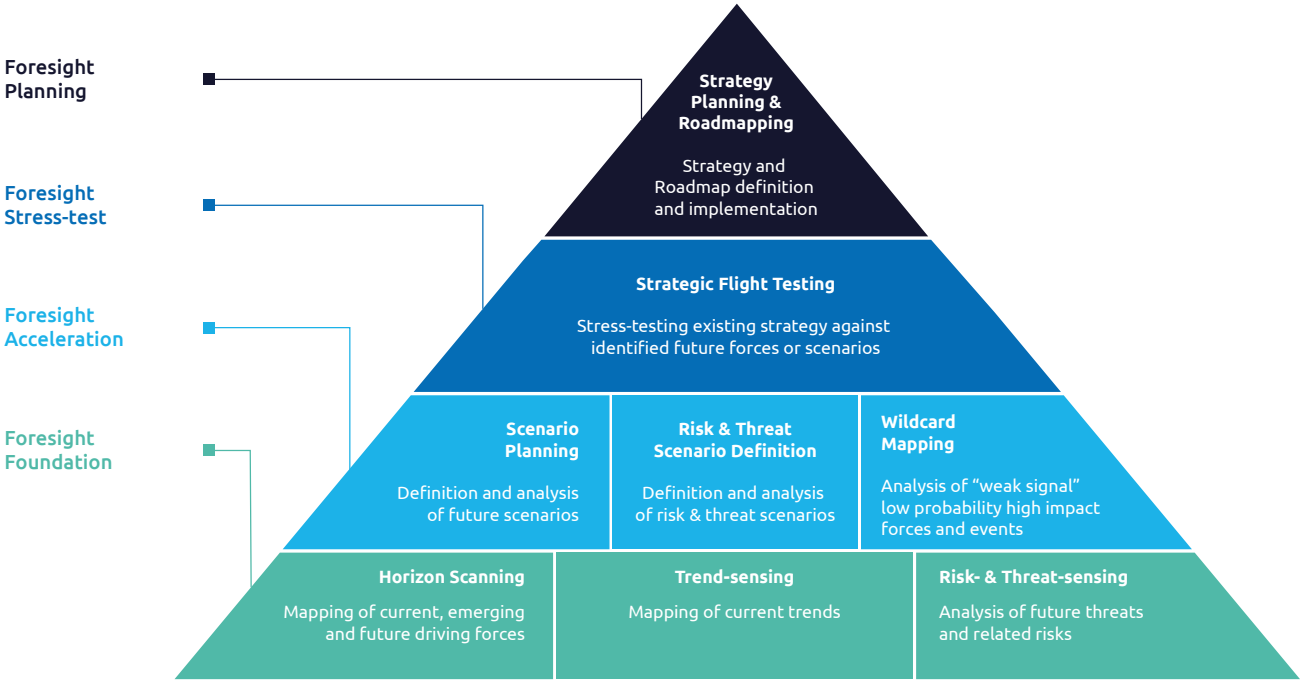
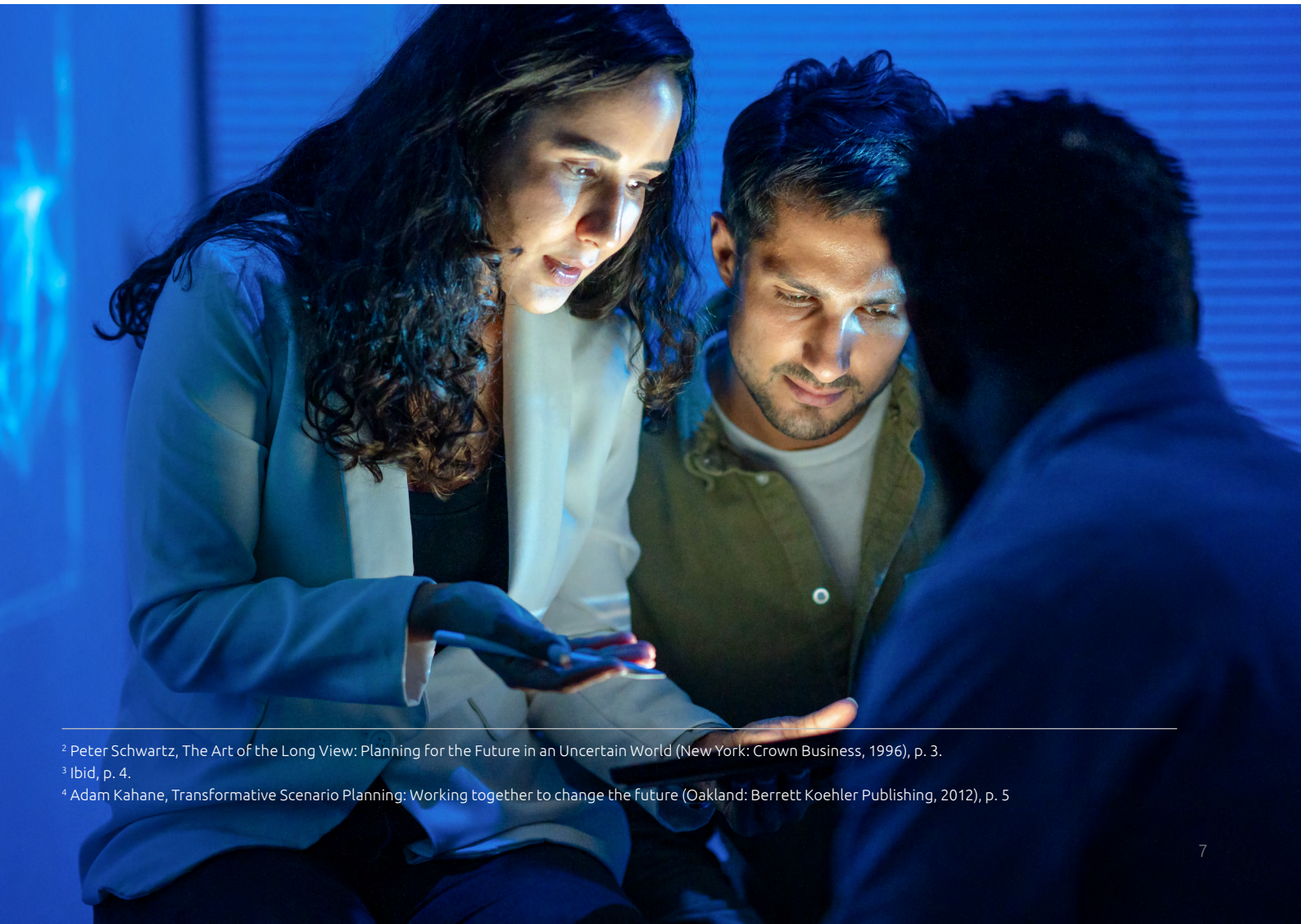


Figure 1: Our Capgemini Invent Strategic Foresight Portfolio

Horizon Scanning is the structured investigation of driving forces around a defined topic within a given timeframe and set geographic scope. These driving forces are current, emerging, and future factors of a social, technological, economic, military, legal, and environmental nature that could have an impact on the defined topic.

Scenario Planning articulates different possible pathways of our future. These different scenarios allow us to recognize, reperceive and adapt to the changes of our present environment.[2] Scenarios in this sense are therefore "a tool for ordering one´s perceptions about alternative future environments in which one's decisions might be played out."[3] They are not a prediction, and most certainly not a solution. They are a step in a transformation, driven by strategists and decision-makers. As Kahane highlights: "The scenario method asks people to talk not about what they predict will happen or what they believe should happen, but only about what they think could happen."[4] Scenarios allow us to paint the future in different colours based on carefully analysed drivers, and to determine what these different versions of tomorrow would mean for us, what vision we are working towards.

Strategic Foresight thus enables us to perceive and re-perceive the change that has already happened around us, is currently happening, or is likely to happen in the future. It allows us to clearly see and put into relation to each other the myriad of factors that drive or impact these changes and consequently determine our future. Through this, we are not just able to cope with the so-called "VUCA" world we are living in – a world characterized by volatility, uncertainty, complexity, and ambiguity. It also enables us to make better strategic decisions for a positive future – bolder ones, kinder ones, more sustainable ones, and more adaptable ones. It helps us envision the future and to define concrete measures to get us there. Strategic Foresight allows us to invent the digital, trustworthy, and secure future we want to see.



[2] Peter Schwartz, The Art of the Long View: Planning for the Future in an Uncertain World (New York: Crown Business, 1996), p. 3.
[3] Ibid, p. 4.
[4] Adam Kahane, Transformative Scenario Planning: Working together to change the future (Oakland: Berrett Koehler Publishing, 2012), p. 5

03

Driving the future

A horizon scan on driving forces impacting the future of digital trust and cyber(security) 2035.

In order to build a positive future of digital trust and cyber(security), we need an understanding of those forces driving digital trust and cyber(security) in Europe until 2035.

Horizon scanning, the analysis of driving forces, ensures a holistic 360° vision on current, emerging, and future developments in this field. It enables a cross-industry, interdisciplinary view and reduces blind spots. Driving forces can be social, technological, economic, military, political, legal, or environmental (STEMPLE) variables that hold the potential to impact our future. They form the foundation of Strategic Foresight.

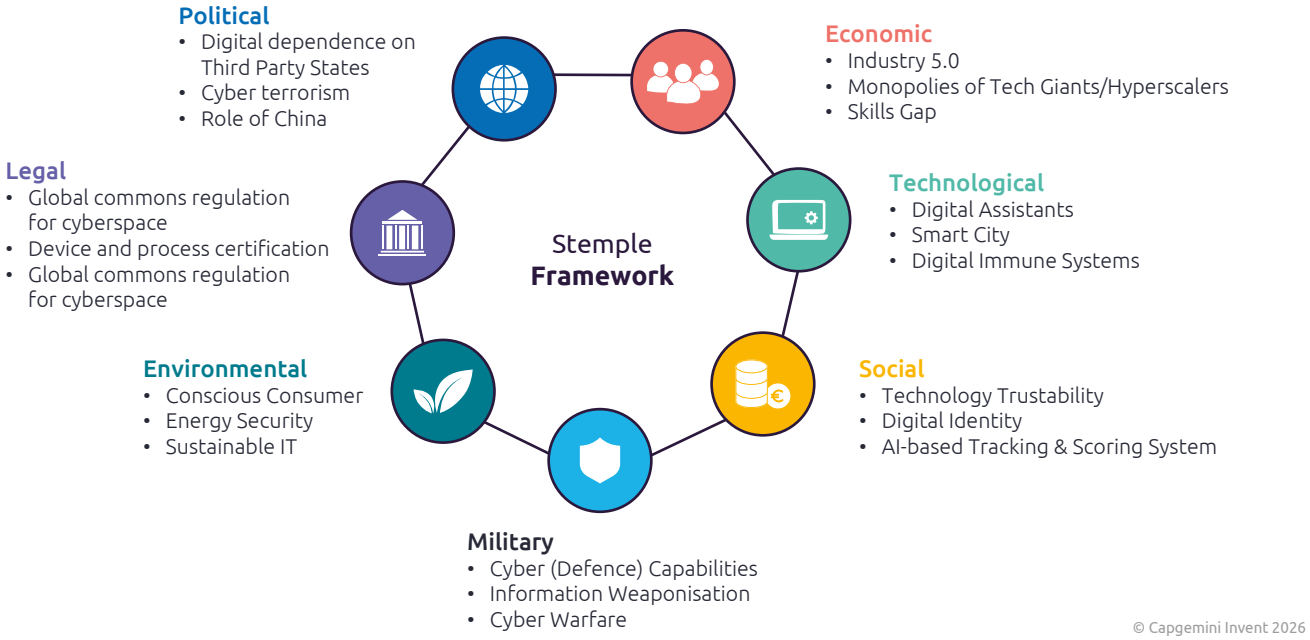


Figure 2: The STEMPLE Framework exemplified - Ensuring a holistic 360° view on the future of cyber(security)

For the future of digital trust and cyber(security), we shortlisted 101 such driving forces across all STEMPLE categories. These drivers emerged in our technology-based research, traditional research, and expert conversations and were vetted and selected by our Foresight team based on their relevance for the future of digital trust and cyber(security). Of course, there are many more factors impacting this complex field – however, to capture the complexity and ambiguity around digital trust and cyber(security) while reducing the noise, focussing on key driving forces is necessary. To refine this focus, we then rated each of these driving forces according to its individual impact on the future of digital trust and cyber(security) as we approach 2035, and on the uncertainty attached to its individual development. This resulted in a driver landscape matrix with three zones of drivers: the focus zone (top right), narrative zone (top left), and the accessory zone (bottom).

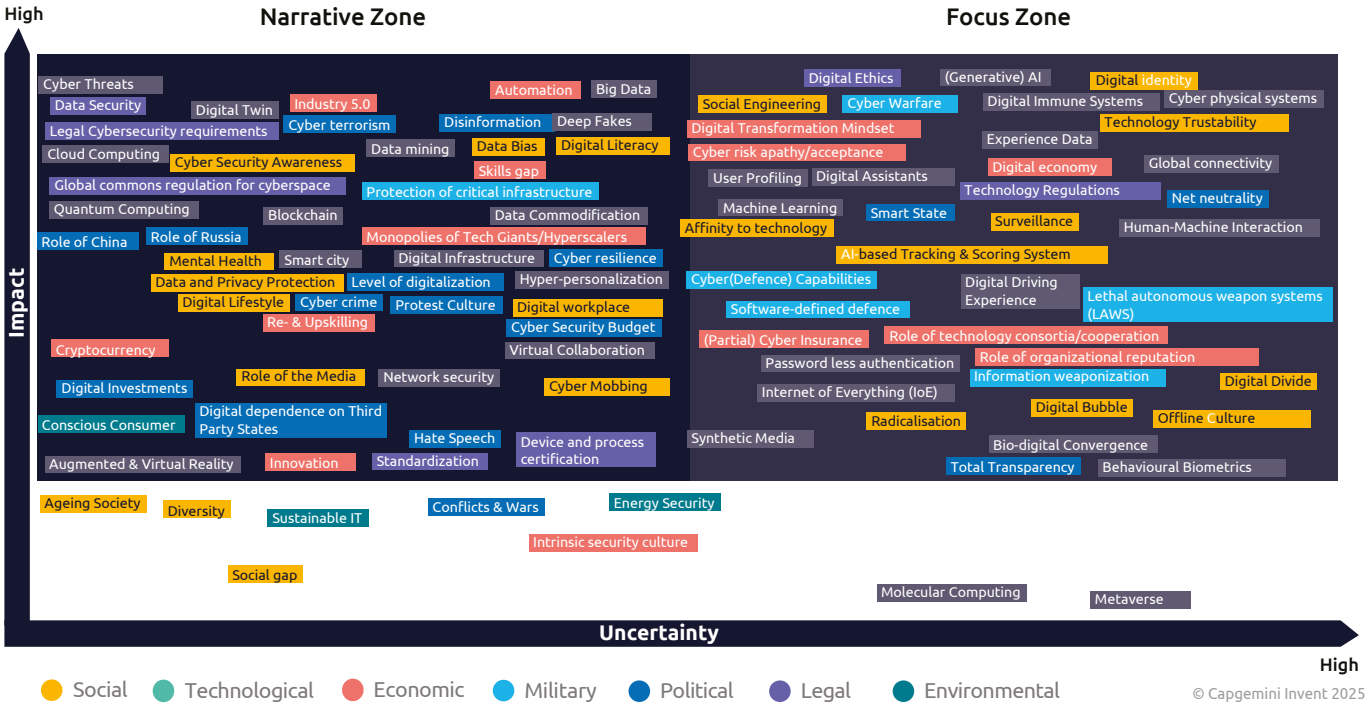


Figure 3: Horizon Scanning - The focus, narrative and accessory zone of the future of digital trust and cyber(security) driver landscape

The Focus Zone - highly impactful and highly uncertain driving forces

This group of driving forces includes those drivers with a high impact on digital trust and cyber(security) 2035 and a high uncertainty in how they could develop in the future. These are driving forces that are particularly volatile, uncertain, complex and ambiguous. They are central to proactively shaping the future. They form the structure of our future world with their function as a "switch" for their individual possible developments. The focus zone included 42 shortlisted driving forces across all STEMPLE categories. In the following, we have highlighted three of these drivers that caused particularly interesting debates among our experts in more detail.

1. Cyber physical systems

Cyber physical systems (CPS) seamlessly connect the virtual and real worlds, incorporating sensors, actuators, and computing elements to enhance efficiency and responsiveness in various domains. CPS share deep similarities with the Internet of Things (IoT). For simplicity reasons and the purpose of this article, IoT devices are also considered as CPS. Examples for CPS are industrial control systems (ICS), smart homes, and home appliances.

The advent of cyber physical systems raises critical questions about digital trust and cybersecurity. As CPS consists of hundreds, sometimes thousands, of devices, the attack surface for malicious actors increases. Many of these devices run lightweight, unstandardized operating systems vulnerable to exploits. The maintenance of a CPS, including software development and patching poses a huge challenge to security teams.

Furthermore, privacy concerns arise due to the connectedness of CPS with the real world. A hacked "smart" device might be misused for spying on individuals using built-in cameras and microphones. Data collected by those devices might also be misused to create profiles (key word: profiling) which in return can be sold for profit or used for identity theft.

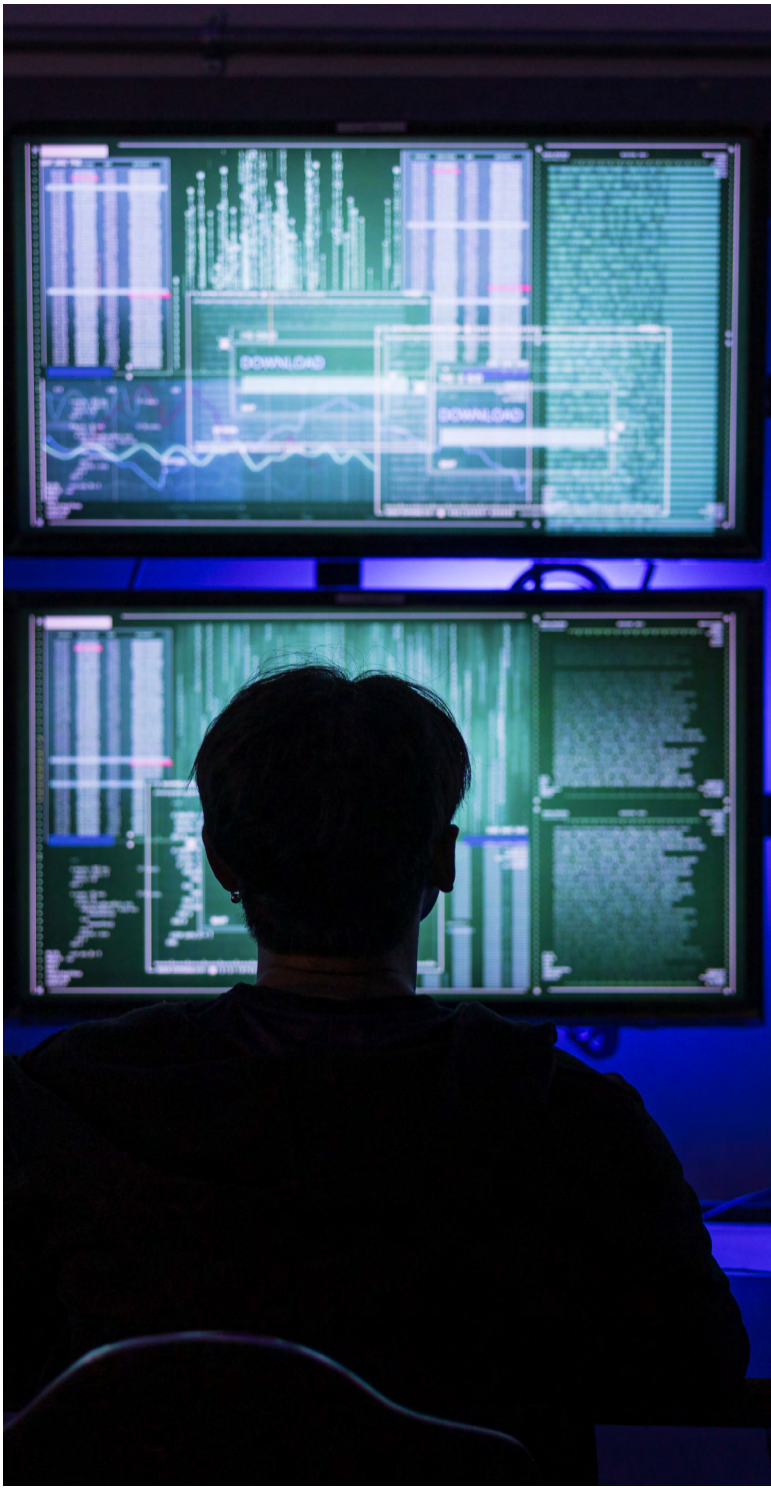
Industries across the spectrum are feeling the transformative impact of cyber physical systems. Manufacturing, healthcare, transportation, and energy sectors stand out as the most affected, witnessing increased automation, improved operational efficiency, and enhanced decision-making capabilities.[5] However, this interconnectedness also exposes these industries to heightened cybersecurity threats, necessitating robust protective measures.

2. Cyber warfare

Cyber warfare refers to the use of digital attacks by one nation or organization to disrupt a wide array of digital and network systems of another, with the aim of creating significant damage or disruption. The spectrum of cyber warfare tactics is broad, including attacks on infrastructure such as power grids or telecommunications, espionage to steal sensitive information, propaganda efforts, and the disruption of military systems. Unlike traditional warfare, the cyber domain reduces barriers to entry and increases anonymity for aggressors, enabling small-scale actors or non-state groups to mount significant challenges against more powerful nations with reduced risk to themselves. One of the most notorious examples of cyber warfare was the Stuxnet worm, discovered in 2010. Believed to have been developed by the United States and Israel, it was used to damage Iran's nuclear program by causing physical damage to centrifuges used in the enrichment process.

Cyber warfare can serve as both a standalone strategy or a complement to conventional military operations. For instance, the Estonian Defense Forces´ Cyber Command, established following the country´s own experience with cyberattacks, is mandated to shield national digital infrastructure and execute strategic cyber operations.[7] Cyber warfare presents a unique set of challenges for international law and norms, as it is difficult to trace and attribute attacks, and the line between state-sponsored actions and independent cybercriminals can be blurry. The Tallinn Manual on the International Law Applicable to cyber warfare, developed by a group of international experts, attempts to address some of these issues by applying existing international law to cyberspace.

The evolving nature of technology means that cyber warfare tactics and defenses are in constant flux, with artificial intelligence and machine learning set to play a crucial role. Given the impact of future communication technologies, all companies within critical infrastructures must prioritize digital trust and cyber(security). This has prompted nations to heavily invest in cyber defenses and specialist training, acknowledging the vital role of cybersecurity in national security.



[5] Thielemann, K., `Follow a 6-phase roadmap to secure cyber-physical systems`, Techtarget, 2023, https://www.techtarget.com/searchsecurity/post/Follow-a-roadmap-to-secure-cyber-physical-systems (accessed April 2024).

[6] Sanger, E., `Obama Order Sped up Wave of Cyberattacks Against Iran`, Atlanticcouncil, 2012, https://www.atlanticcouncil.org/blogs/natosource/obama-order-sped-up-wave-of-cyberattacks-against-iran (accessed April 2024)

[7] Kaska, K., `The Cyber Defence unit of the Estonian Defence League`, CDU_Analysis.pdf (ccdcoe.org), (accessed April 2024).

3. Digital immune systems

In an era of countless cyber threats and rapid technological advancements, digital immune systems (DIS) have emerged as a proactive and holistic approach to cybersecurity. Inspired by the human immune system, a DIS encompasses methodologies and tools for software design, development, automation, operations, and analytics. It leverages these components to craft an exceptional user experience and mitigate system failures that can affect business performance.[8]

Once a DIS is successfully implemented in an organization, it can proactively identify emerging threats in real time. Once a threat is detected, the DIS uses behavioral analytics, artificial intelligence, and automation to assess a situation and initiate immediate responses. Each incident is automatically analyzed and iteratively ensures the continuous improvement of responses and the entire resilience of the organization. Leveraging modern technologies such as Artificial Intelligence and Machine Learning, digital immune systems can adapt to evolving threat landscapes and scale effortlessly to accommodate the dynamic nature of digital environments.[9]

The advent of digital immune systems can have a profound impact on digital trust and security, ushering in a paradigm shift in how organizations and individuals perceive and approach cybersecurity. Yet there are still a few hurdles to overcome. Organizations need to make sure that their infrastructure is suitable for a DIS. They need to establish a reliable strategy for regular risk assessments and audits, and above all, they need to provide adequate training for employees to drive adoption and improvement.

The Narrative Zone – highly impactful and certain driving forces:

This group of driving forces includes those drivers with a high impact on digital trust and cyber(security) 2035 and a low uncertainty in how they will develop in the future. The driving forces of the narrative zone give a common development outline in our foresight work. In our scenario planning, they are used as story blocks for the alternative future narratives. The narrative zone included 50 shortlisted driving forces across all STEMPLE categories. Here are three drivers from the narrative zone, whose relevance for the future of digital trust and cyber(security) is described in more detail.

1. Legal Cybersecurity requirements

Legal Cybersecurity requirements encompass statutes, regulations, guidelines, mandatory directives, norms, industry frameworks, and penalties pertaining to the safeguarding of networks, information systems, and obligations for reporting security breaches and incidents.[10] Those requirements had already played, and will play, an even higher role for **digital trust and (cyber)security** in the future, as they had not only given obligations for security measures, but also opportunities to reach a higher security level for public institutions, companies, and even individuals.

While individuals are mainly protected through the GDPR and AI Act, current and future regulations, especially regarding **Artificial Intelligence** and **Social Media/ Metaverses**, may cause unprecedented challenges for developers and network providers.

Additionally, there will be a stronger need for regulations for **critical infrastructure companies** regarding a compliant usage of new technologies but also an appropriate protection from associated threats.[11]

Legislators, therefore, must always be up to date to be able to formulate targeted and tailored specifications to protect the **public sector** as well, from common cyber threats up to cyber warfare. While doing so, legislators must be aware that specifications will need to change quite frequently, as the internet has **developed and changed very rapidly** and additionally,

[8] Perri, L., ´What Is a Digital Immune System and Why Does It Matter?´, Gartner; https://www.gartner.com/en/articles/what-is-a-digital-immune-system-and-why-does-it-matter (accessed March 2024).

[9] Gupta, M. ´How Organizations Can create A Digital Immune System´, Forbes; https://www.forbes.com/sites/forbestechcouncil/2023/12/12/how-organizations-can-create-a-digital-immune-system/?sh=502b7c1213f1 (accessed March 2024).

[10] Law Insider, Cybersecurity Requirements definition; https://www.lawinsider.com/dictionary/cybersecurity-requirements (accessed March 2024).

[11] BSI, Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 1.0); https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/1-0/it_sig-1-0.html (accessed March 2024).

is still very young, respectively.[12] [13]Therefore, it is questionable whether a period of five years regarding corresponding updates of laws, regulations, and policies will be sufficient in the future as it is currently the case in policies such as ITSiG 2015 – 2021 or NIS 2017 – 2022.[14]

2. Deep fakes

Deep fakes refer to AI-based techniques that synthesize media, including superimposing human features on another person's body or manipulating sounds to generate a realistic human experience.

The term "deep" in deep fakes is influenced by deep learning, an area of AI that uses many-layered artificial neural networks.

Recent developments have seen a significant increase in deep fake incidents. Between 2019 and 2020, the amount of deep fake online content increased by 900%, with forecasts suggesting that as much as 90% of online content may be synthetically generated by 2026.[15] In March 2022, for example, a deep fake video of Ukrainian President Volodymyr Zelensky was quickly debunked, but it highlighted the potential geopolitical consequences of such technology.[16]

Deep fakes pose a serious threat to digital trust and cybersecurity. They are perceived as an unprecedented threat to democracies and online trust, through their potential to back sophisticated disinformation campaigns. Deep fakes have opened up a new dimension for cyberattacks, ranging from sophisticated spear phishing, to the manipulation of biometric security systems.

To address these challenges, robust AI-powered detection tools, improved authentication protocols, and public awareness campaigns are essential to safeguard against potential harm and maintain trust in digital content and security systems.

Deep fakes pose a significant risk across various industries. The crypto sector is the main target, representing 88% of all deep fake cases detected in 2023, followed by fintech at 8%.[17] The entertainment industry has also seen an increase in the use of deep fakes, with the technology being used for both positive and negative purposes. Deep fakes represent a significant challenge in the digital age. As they become more sophisticated and widespread, industries, governments, and individuals must be vigilant and proactive in understanding and mitigating their potential risks by leveraging mentioned technologies, as well as performing verification checks that only the true person would pass.

3. Cybersecurity budget

Cybersecurity budget refers to the financial resources allocated by an organization or state for protecting its digital assets. It's a critical investment because it safeguards against cyber threats, thereby preventing financial losses, reputational damage, and legal consequences.

Historically, cybersecurity budgets have seen a steady rise. In 2024, European spending on cybersecurity increased by more than 12% and is forecasted to reach $84 billion by 2027.[18] This growth reflects the escalating cyber threats and the increasing recognition of cybersecurity's importance.

Several factors drive the allocation of cybersecurity budgets. The evolving threat landscape, legal cybersecurity requirements, and supply of cyber insurance are among the leading factors. Moreover, the increasing complexity of IT infrastructure and geopolitical or economic uncertainties also influence budgeting decisions.

As digital transformation initiatives expand the attack surface, industries across the board are likely to adapt their cybersecurity budgets. Particularly, sectors with a high degree of digitization and those handling sensitive data, such as finance, healthcare, and IT, are expected to invest significantly in cybersecurity.

[12] OpenKRITIS, IT-Sicherheits¬gesetz 2.0; https://www.openkritis.de/it-sicherheitsgesetz/ausblick-it-sicherheitsgesetz-2-0.html (accessed March 2024).

[13] BSI, EU-Richtlinien zur Netzwerk- und Informationssicherheit; https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/NIS-Richtlinie/nis-richtlinie_node.html (accessed March 2024).

[14] Cyber Risk, The NIS 2 Directive; https://www.nis-2-directive.com/ (accessed March 2024).

[15] Bueermann, G., Perucica, N., How can we combat the worrying rise in deepfake content?; https://www.weforum.org/agenda/2023/05/how-can-we-combat-the-worrying-rise-in-deepfake-content/ (accessed March 2024).

[16] Hutson, M., Detection Stays One Step Ahead of Deepfakes—For Now; https://spectrum.ieee.org/deepfake (accessed March 2024).

[17] Sumsub, Sumsub Research: Global Deepfake Incidents Surge Tenfold from 2022 to 2023; https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/ (accessed March 2024).

[18] International Data Corporation (IDC), European Security Spending is Forecast to Grow at Double Digits in 2024, in Response to Constant Cyberthreats, Says IDC; https://www.idc.com/getdoc.jsp?containerId=prEUR251983724 (accessed April 2024).

The Accessory Zone – lower impact driving forces with low to high uncertainty:

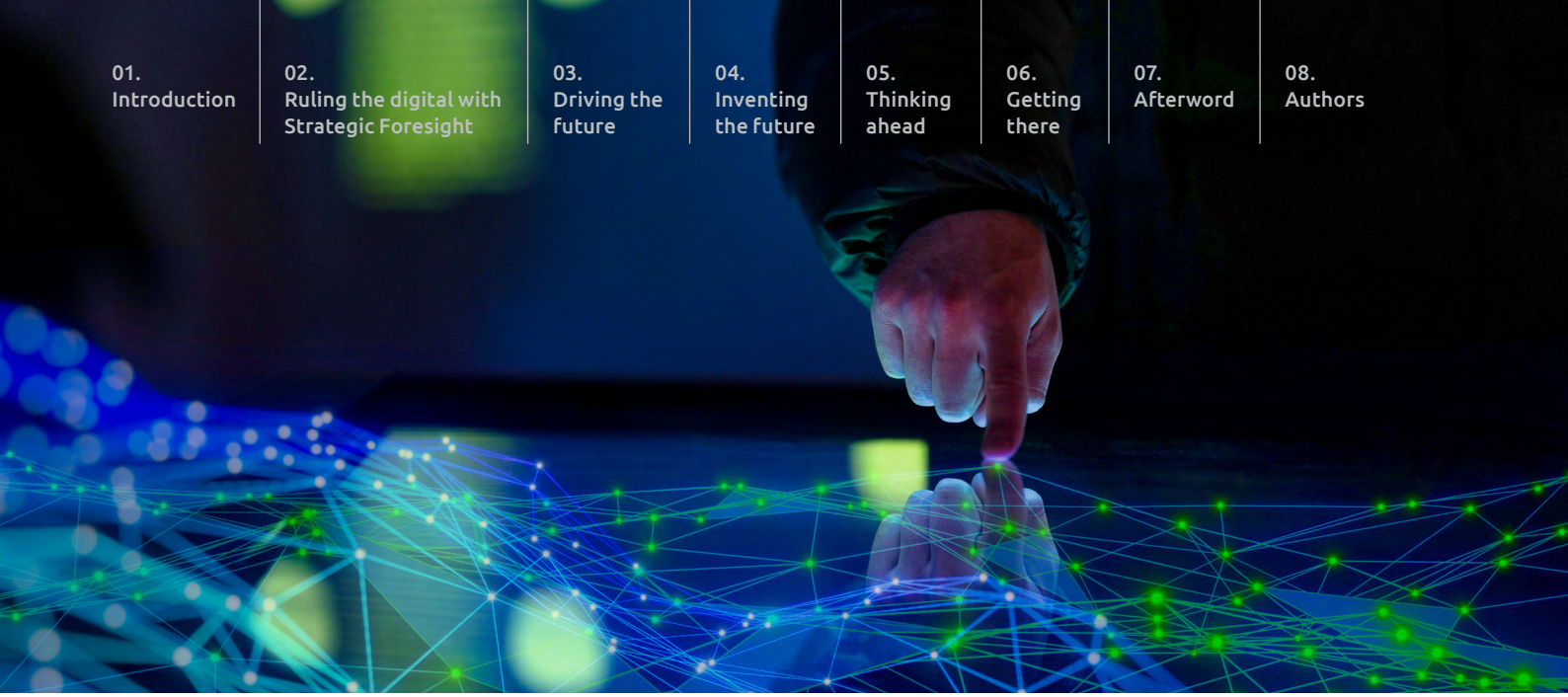
This group of driving forces includes those drivers with a lower impact on the future of digital trust and cyber(security). We group these drivers together irrespective of their uncertainty level, as their lower impact rating means they will be slightly deprioritized (but not forgotten!) in the strategy-making to follow. For example, in our scenario planning, they will be used as additional input for detailed scenario narratives. The accessory drivers are those that construct the edges of our future world by adding supplementary potential or depth to the narrative and focus drivers. The accessory zone includes 9 shortlisted driving forces across all STEMPLE categories, such as Metaverse, Energy Security, and Ageing Society.

Each of these three zones plays a different role in constructing future-ready strategy. By definition, this horizon scan allows us to capture the uncertainty related to individual factors around European digital trust and cyber(security). Understanding these forces at play and their interaction is vital in pinning down the factors contributing the highest volatility, which is essential if we are to create a clear view of what lies ahead for the future of digital trust and cyber(security). This process massively reduces the complexity around the future of digital trust and cyber(security) – and how we can impact it. To do just that, we took our understanding from the horizon scanning to the next level by supplementing it with Scenario Planning.

04.

Inventing the future

Four scenarios on digital trust and cyber(security) 2035.



Scenario Planning is a Strategic Foresight methodology aimed at translating the forces forming our future into alternative future worlds. Through Scenario Planning, we capture critical uncertainties that are usually excluded but crucial for effective strategy-making. The basis of this process is the holistic driving forces and trends that have been identified. The process brings together a diverse range of stakeholders and constructs a joint basis for strategic action. It is a unique forward-focused methodology to anticipate uncertain change and prepare strategic response, combining an academically rigorous methodology with innovative interaction formats and tools. As Peter Schwartz, one of the pioneers of Scenario Planning, put it very aptly, scenarios are "a tool for ordering one´s perception about alternative future environments in which one´s decisions might be played out".[19] As such, scenarios help us in our endeavour to build a positive future by allowing us to reperceive and reframe the way we look at the future.[20]

In our scenario analysis of the future of digital trust and cyber(security) 2035, we therefore developed four alternative future scenarios to serve as a basis for strategic conversation, and ultimately, strategic action. To do so, we applied our five-step scenario process in a scenario workshop with our Foresight team and our cybersecurity experts. In this workshop, we defined four future scenarios:

1. Digital Dream
2. Cybernated Kingdom
3. Hybrid Hell
4. Wild Wicked Web

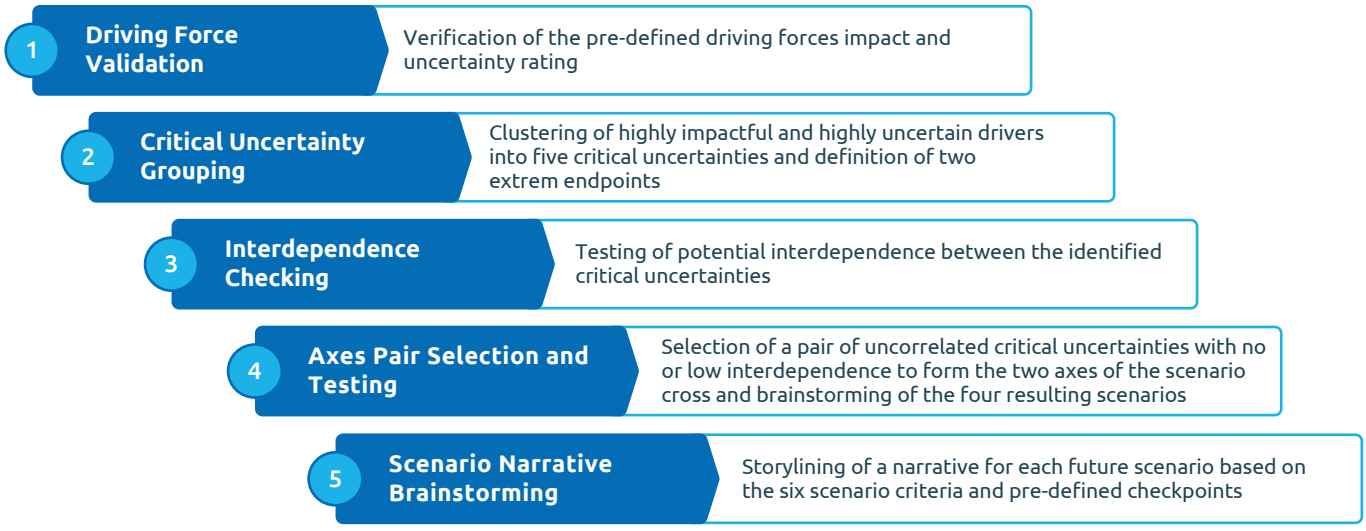


Figure 4: Our five-step scenario workshop process

[19] Schwartz, The Art of the Long View, p. 4.

[20] Ramirez, Rafael; Wilkinson, Angela, Strategic Reframing: The Oxford Scenario Planning Approach (Oxford, 2016), pp. 3-4.

These four scenarios emerge by combining two independent critical uncertainties around the future of digital trust and cyber(security) that emerged in our scenario workshops. Critical uncertainties are clusters of highly uncertain and highly impactful driving forces from our Focus Zone that hold the potential to determine our future and steer our tomorrow in one direction or another. As such, they pose key questions whose answers are able to tip developments in cyberspace in one direction or another.

The two selected critical uncertainties for the future of digital trust and cyber(security) were the questions of:

- How strong is the New cybersecurity Normal in terms of the fulfillment of needs against cyber threats? The New cybersecurity could either be **robust** or **weak**.
- How does the digital individual exist in cyberspace? The digital individual could either have a **limitless** or **leashed** experience.

The combination of these two questions and their four endpoints in a 2-by-2 framework results in a frame structuring our four scenarios.

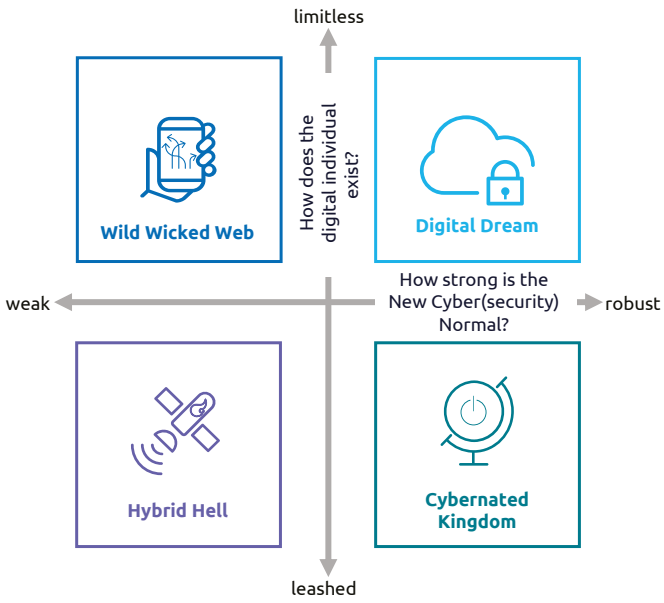


Figure 5: Scenario axes pair with four scenarios on the future of digital trust and cyber(security) 2035

Each of these scenarios fulfils six criteria: they are all plausible, relevant, challenge our perception, contain an inherent logic, balance negative and positive aspects of their story while being divergent from the remaining scenarios and engage stakeholders.

These four scenarios are set in 2035 and map vastly different stories of what cybersecurity could look like at this point.

Scenario 1 - Digital Dream

This scenario is characterised by robust cybersecurity and a limitless existence of the digital individual.

2035 – we are living the digital dream. The nightmare of rampant, large-scale cyberattacks with heavy costs for the economy, state, and society in the mid-2020s has faded to a distant memory by 2035. States, economies, and individuals all collaborate seamlessly and securely in the digital and analogue world. With one verified digital identity for each individual, living and working in the digital world has become easy for everyone in Europe. The economy has been blooming – European countries have established themselves as a digital heaven for secure and future-oriented business. With the Europe-wide emergence of Smart States, citizens and governments benefit from innovative technologies in governance. Nevertheless, the voices warning of isolationist tendencies in Europe are becoming louder and louder, warning of the effects of Europe becoming isolated digital islands.

Economy

Following massive targeted cyberattacks on the economy, the private sector quickly realised that a secure and trustworthy digital sphere was the only way to ensure successful business. This led to an unprecedented push for digital integration and cybersecurity initiatives by the private sector. Supported by clear and concise government regulation and cybersecurity subsidies on a European and national level, companies were able to leverage innovative technologies such as Quantum Computing and Artificial Intelligence to build their security. In 2035, their digital immune systems are healthy and strong. The effect on business is tremendous. European countries have established themselves as a safe digital heaven where innovation flourishes and solutions are built across industries. This has led to a massive labour migration of highly trained individuals to European countries. "Secured in Europe" has become the new quality trademark for products and services globally. Nevertheless, companies worry about the increasingly adept cyberattacks. The dark side of digital remains, and it is becoming increasingly hard to combat new attack vectors.

Public Sector

When disastrous targeted disinformation campaigns powered by Artificial Intelligence destabilised the national politics of various European countries in the mid-2020s, governments realised they could not survive in this emerging dark digital reality. Following a groundbreaking collaborative security initiative with the private sector, European countries managed to build a secure and trustworthy digital space for all, for example through the establishment of one secure digital identity for each individual. With critical infrastructure well protected, large cyberattacks have become a rarity in Europe. This digital environment also gave rise to Smart State solutions that put the citizen first and enable efficient and effective governance for regional, national, and local governments. As a consequence, governmental action is thriving, for the benefit of society and the economy at large. This allows governments to concentrate on vital issues efficiently and diligently, such as tackling climate change. Software-defined defence has redefined military strategy, and Europe has never been so secure militarily. The conflicts of the 2020s are in the past. However, the public sector is fully reliant on private sector technologies, and the voices cautioning about this utter dependency have become louder and louder. While digital ethics are a key pillar of European life in 2035, critics have warned that the increased security might lull actors into a false sense of security, leading to attacks with unprecedented impact.

Society

European citizens are living the digital dream. Groundbreaking initiatives such as one verified digital identity have led to a secure digital lifestyle. Digital health campaigns and digital literacy initiatives have resulted in a high level of understanding, wellbeing, and skill in the European population. The positive effects of the digital revolution – from Smart State to digital workplace – are making individuals' lives more convenient, more efficient, and more balanced. For example, secure innovation in the medical field has highly increased early recognition of physical and mental illnesses, and the use of trustworthy AI has enhanced treatment options. Being offline has received new value and recognition in society. Citizen happiness is high and shows itself in high political and economic participation. Individuals drive their ideas, multiplying the power to find solutions for prevalent challenges such as climate change. With labour migration into Europe, European countries have become a much more diverse and tolerant place. However, since the introduction of the digital identity, protests have increased on the accusation of state surveillance. While most believe this new world to be a driver of (digital) freedom, the dilemma between security and freedom is a frequent topic of debate.

In this future world, the digital dream has become reality, a positive paradigm shift for the public and private sector as well as society. Digital trust and cyber(security) are a pillar of the new digital normal. However, questions remain on new possible attack vectors and the trade-off between security and freedom.

Scenario 2 - Cybernated Kingdom

This scenario is characterised by robust cybersecurity and a leashed existence of the digital individual.

The year is 2035. Years of devastating cyber criminality, cyber mobbing, hate speech online, and other digital transgressions have led to a clamp-down on digital activity by governments. Access to the digital world is highly restricted and monitored heavily by digital ministries in Europe. Both individuals and companies act securely in this heavily fortified digital kingdom, with digital trust at its centre. While individual freedoms are restricted in cyberspace, the benefits of a secure and safe digital environment are widely acknowledged by both society and the private sector. As society navigates the complexities of the digital age, the Cybernated Kingdom stands as a beacon of stability and security in an ever-evolving digital landscape. Nevertheless, voices calling for an end to digital surveillance are rising, and digital isolation is starting to be seen as a severe threat to economic growth.

Economy

From 2025 to 2035, the dynamic economy undergoes and drives a paradigm shift towards a tightly regulated and secure digital environment. Now, the economy serves as the cornerstone of a rapidly advancing transition towards a secure cyberspace in the Cybernated Kingdom, recognizing the societal needs following severe cyberattacks on individuals and organizations. The economy adapts to the dangerous environment during the early 2030s and offers tailored all-in-one solutions for a wide spectrum of society and organizations. However, the stringent regulations imposed by European and state legislators pose significant challenges for businesses. Driven by the imperative to mitigate cyber threats, organizations adopt robust cybersecurity guidelines enforced by both governmental authorities and private entities. Quick adaptation to increasingly precise and detailed regulations becomes the new rule of the game. Voices dissenting against the restriction of individuals in cyberspace are often disregarded, their arguments swiftly countered with reference to past severe cyberattacks.

The pervasive fear of cyber threats and risks in society leads to a high demand for easily understandable and comprehensive solutions, resulting in a genuine boom in hiring within the cybersecurity industry. These entities invest heavily in cyber defense, developing groups of skilled professionals to safeguard against digital threats. However, the focus extends beyond software solutions; there is a heightened emphasis on training employees in cyberspace. C-level executives in the Cybernated Kingdom not only discuss cybersecurity but also rigorously prioritize it as number one. The risk of a cyberattack and the associated loss of millions are no longer acceptable. Consequently, the way of working for employees primarily engaged in computer-related tasks becomes more restricted but also more secure. Continuous authentication and zero-trust measures become commonplace.

In this future world, the Cybernated Kingdom safeguards the digital crown jewels of the economy, society, and the public sector. People and businesses require strong, EU-wide, stringent regulations and laws, and they receive just that. However, this security-based approach relies on restricting one's own existence in cyberspace, which is sometimes questioned through critical reflection.

Public Sector

The public sector and legislators play a pivotal role in shaping the Cybernated Kingdom. European digital ministries implement stringent, restrictive cybersecurity guidelines and policies to ensure a secure and safe cyberspace. These guidelines include mandatory certifications for all digital services and products to ensure a high level of security. They adhere to the approach of "better safe than sorry," responding to society's active demand for regulatory improvements following cyberattacks on companies and private individuals during the 2020s. Governance in the digital world is now tightly regulated, with laws aimed at mitigating cyber risks and maintaining societal stability. The states invest in highly trained cyber defense units coordinating countermeasures, enforcing a common early warning system for cyberattacks, strengthening their capabilities to fend off cyberattacks and safeguard national security. The state itself is now considered impregnable and heavily protected

against cybercrime. However, longer wait times for state services are common for those subjected to the stringent authentication and identity requirements, which, although now largely digital, sometimes prolong the process.

European governments have successfully transitioned from lagging behind to catching up on an international scale and take pride in the level of digital trust and cyber(security) achieved, viewing it as a testament to their ability to protect and serve their citizens in the digital age. Additionally, the state actively educates and informs its citizens about the dangers in cyberspace through large-scale awareness campaigns, which have high priority and consequently receive substantial budgets from the government. Radio, television, and public-facing marketing campaigns are commonplace to enhance the digital literacy of the population.

Society

While individual freedoms are constrained in cyberspace by the government, the digital workplace flourishes, offering excellent opportunities for remote work and digital collaboration. There is a strong emphasis on achieving work-life balance, as individuals embrace the convenience and efficiency of digital technologies while cherishing moments of analogue connection. The wake-up call from the late 2020s, resulting from the ambivalence of the digital world such as cyberattacks and organized AI-driven fake news campaigns, has heightened societal awareness and underscored the importance of cybersecurity measures. Consequently, society, following a brief sense of helplessness, has demanded increased government intervention and remains willing to trade personal freedoms in cyberspace for security. Targeted awareness campaigns and free seminars offered by the government are positively received, enlightening the population about the dangers online.

The people rely on digital touchpoints in real life and find comfort in the interconnectedness of the digital and analogue worlds, achieving a harmonious balance between the two. The Cybernated Kingdom, with its high security standards and stringent regulations, enables a wide range of digital opportunities, such as those in healthcare, transportation, and educational offerings. Schools are firmly integrated into the digital strategy and meet the highest data protection requirements through secure cloud solutions. Additionally, awareness of cyber risks is instilled in the youngest through the new school subject “Cybersecurity.”

However, the restriction is not welcomed by everyone. While the majority of the population is protected, the blocked parts of the web and the steady decline of open-source websites infuriate some internet users. Information that was easily and publicly accessible ten years ago has gradually been restricted due to misuse and is now sometimes difficult to find. Nevertheless, pride in the level of digital trust and cyber(security) prevails in society, instilling confidence in the digital infrastructure.

Scenario 3 - Hybrid Hell

This scenario is characterised by weak cybersecurity and a leashed existence of the digital individual.

Welcome to the Hybrid Hell! We find ourselves in the year 2035, and the online experience paints a dark picture of European cyberspace, because the digital existence is uncontrolled and dangerous, often jokingly referred to as the "Internet Inferno." During the 2020s, European lawmakers drastically underestimated the dangers of the cyberspace and now find themselves confronted with an uncontrolled cyber realm exploited ruthlessly by well-organized groups of cybercriminals. Large-scale cyberattacks on companies and the theft of consumer data are commonplace and no longer surprise society. As society grapples with the consequences of unchecked cyberspace, the need for collective action and effective governance becomes increasingly urgent. However, such efforts are implemented poorly, often limited to merely restricting digital services. With governance structures crumbling and cyber threats proliferating, society, organizations, and the public sector find themselves trapped in a nightmarish Hybrid Hell.

Economy

As governance structures crumble, cyberspace descends into chaos, providing fertile ground for cybercriminals and malicious actors. Organizations bear the brunt of the increased number of cyberattacks. Particularly during the late 2020s, significant security vulnerabilities within companies became evident and were ruthlessly exploited by well-organized cybercriminal groups. Recognizing the high potential of poorly prepared companies, the number of cybercrimes climbs drastically every year. Large-scale cyberattacks on the economy become commonplace, causing regular disruptions.

By 2035, companies that heavily invested in cybersecurity before this time emerge as winners, having successfully implemented necessary countermeasures. Conversely, those that acted too hesitantly during the late 2020s find themselves vulnerable in 2035. Their business operations are regularly disrupted by ransomware attacks and phishing campaigns, leading some companies to bankruptcy. In response to the uncertainty in cyberspace, many implement a strict "return to office" policy, which limits employees' ability to work from home when sensitive data is involved. Furthermore, companies increasingly rely on physical documents and face-to-face meetings to exchange sensitive information.

Public Sector

The Hybrid Hell of 2035 — European states are confronted with their years of inactiveness. Governments find themselves grappling with the fallout of uncontrolled cyberspace. Radicalization online, fueled by fake news campaigns generated by artificial intelligence, is leaking into governments, with right-wing ideologies gaining traction and aggravating societal divisions. In the absence of effective governance, cyber warfare rages on multiple fronts, further destabilizing fragile geopolitical landscapes. Consequently, many European states are mobilizing task forces with high priorities and allocating substantial resources to address this governance vacuum.

The digital identities of European citizens are insecure, leading to widespread cybercrime, cyberbullying, and hate speech. The digital identities, a once envisioned savior as an escape and prevention, in which much investment was made, fail to meet the requirements in 2035. The entire digital infrastructure of European countries lags behind international standards, giving in to the overwhelming surge of criminal activities from cyberspace. Consequently, the government restricts digital services out of fear of further attacks. Educational institutions, still largely undigitized, suffer greatly as a result. Governments concede defeat on this front, leading to high levels of frustration in society and highlighting the digital gap. What remains are mere useless governmental digital guidelines for safe technology, which are miserably outdated and inadequate to confront the present threat in 2035.

Society

With unclear guidelines and insecure technology, individuals are compelled to self-censor and curtail their digital activities. With no apparent resolution to the turmoil in cyberspace, people seek refuge in analogue spaces in pursuit of safety and security. Analogue islands emerge as havens, providing sanctuary from the tumult of the digital realm. The once-promising potential of technology has yielded to a nightmare, where the advantages of digitalization are overshadowed by the pervasive threat of cyberattacks and digital insecurity. This distrust has led to increased social isolation, as many people avoid digital communication tools, enhancing social divide between those who rely on digital technology and those who avoid it in favour of face-to-face interactions.

Society sets a strong focus on safeguarding personal data, as individuals have fallen victim too often to identity theft through stolen passwords on multiple occasions, further weakening trust in digital technologies.

In this future world, the Hybrid Hell is the result of years of misguided measures and underestimation of the dangers in cyberspace, where European states only know how to help themselves with drastically restricting the presence in the cyber existence. The return to analog forms of interaction increases in the face of constant fear of cyberattacks. The Hybrid Hell claims its first victims, who no longer believe in the positive effects of digitization.

Scenario 4 - Wild Wicked Web

This scenario is characterised by weak cybersecurity and a limitless existence of the digital individual.

We are living in the year 2035 and find ourselves in a Wild Wicked Web. Society has accepted cyber risks and has become apathetic towards frequent cyberattacks, which now fill the news channels on a regular basis. Both the government and the economy have completely neglected to prepare for the dangers of the cyber realm and are now paying the price for it. Individuals are left to fend for themselves in the cyberspace, experiencing a sense of autonomy. As society grapples with the complexities of digital existence, the need for a balanced and proactive approach to cybersecurity becomes increasingly apparent, driving discussions around digital ethics and the responsibilities of individuals, organizations, and states in safeguarding the digital realm.

Economy

Also the economy experiences the challenges coming from the limitless existence in weak cyberspace. During the years 2025 to 2035, the economy experienced a significant divergence in cybersecurity approaches. On one end of the spectrum, certain companies fully embraced the concept of unrestricted exploration in cyberspace, pushing boundaries without hesitation. These entities prioritize innovation and market agility over stringent security measures, accepting cyber risk as an inevitable aspect of digital existence. This “New Cybersecurity Normal,” characterized by vulnerability and frequent breaches, is mitigated by cyber insurance in case of emergencies, allowing the trade-off between digital agility and compromised security measures to function. Conversely, other organizations recognized the paramount importance of cybersecurity and implemented robust security measures accordingly. They excel in deploying effective measures, resulting in a secure environment, although with drawbacks in terms of employee work processes. Constant authentication requirements and productivity-reducing measures are poorly received by employees, leading to significant frustration and, in some cases, high turnover rates due to dissatisfaction with the restrictions.

Major beneficiaries of the lagging infrastructure in Europe are non-European hyperscalers and large tech corporations, which thrive on the lagging European digital infrastructure, providing secure digital islands and fostering a sense of dependence on these entities for cybersecurity infrastructure.

Public Sector

In the dynamic digital ecosystem of 2035, the public sector finds itself grappling with the harsh realities of lacking behind in basic cybersecurity infrastructure. Technological advancements have empowered individuals with limitless access to information and connectivity, but cyberattacks continue to outpace defensive measures. Government agencies and institutions are confronted with mounting challenges in safeguarding sensitive data and critical systems from malicious cyber threats.

Outdated systems, inadequate resources, and a lack of cybersecurity expertise leave government agencies vulnerable to a myriad of cyber threats, ranging from ransomware attacks to data breaches and state-sponsored cyber espionage. A recent breach of a government database containing sensitive citizen

information underscores the dire consequences of lax cybersecurity practices. The breach, attributed to a sophisticated cyberattack, compromised the personal data of millions of individuals, eroding public trust in government institutions and underscoring the urgent need for improved cybersecurity measures. Recognizing the problem of losing control over cyberspace but being nearly powerless to address it, online radicalization is increasing, serving as fertile ground for disinformation campaigns and polarization.

Among the constant flood of cyber threats, the public sector is forced into a perpetual state of reactive defense, scrambling to patch vulnerabilities and mitigate the fallout of cyber incidents as they occur. However, the reactive nature of cybersecurity efforts often proves insufficient in addressing the root causes of systemic vulnerabilities, leaving government systems perpetually on the brink of compromise. In response to the helplessness against increasingly frequent attacks, many European states have initiated national cybersecurity awareness campaigns. These campaigns aim to educate citizens and government employees on best practices for cyber hygiene and incident response.

Society

The society enjoys limitless connectivity and digital empowerment in 2035, but the cybersecurity normal remains a source of concern rather than assurance. For private individuals, the digital landscape of 2035 is characterized by a paradoxical blend of total transparency and heightened cyber risk. Many individuals have embraced the concept of multiple online identities as a means of expressing their digital individuality, navigating a world where personal data has become a commodity in the burgeoning experience data economy.

Despite advancements in technology, cybersecurity defenses are inadequate, leaving society vulnerable to exploitation and manipulation by malicious actors. A series of high-profile data breaches involving major social media platforms and online retailers further erodes public trust in the digital ecosystem. Individuals become increasingly reluctant to share personal information online, fearing the repercussions of potential data breaches and cyberattacks.

In response to the alarming state of cybersecurity, a new ethos of digital citizenship emerges. Individuals recognize the urgent need for collective action to address cybersecurity challenges and advocate for greater accountability and transparency in the digital sphere.

New generations grow up with an inherent understanding of the risks and benefits of digital technology, but widespread apathy towards frequent cyberattacks prevails. While some individuals prioritize security measures, others adopt a laissez-faire attitude, resigned to the inevitability of breaches. Cyber insurance for individuals has become standard practice, offering a semblance of protection in an increasingly volatile digital landscape.

In 2035, this Cybernetic Chaos highlights the ambivalence of the digital world to society. While cyber access is unlimited, it becomes evident that without clear regulations from the European Union, cyberspace is evolving into the Wild West. The public sector, overwhelmed by the digital realm, lags far behind international standards. The economy is left to fend for itself and becomes increasingly reliant on foreign providers for secure infrastructure.

05

Thinking ahead

Impact-Tree for the future of digital trust and cyber(security).

The complex landscape of driving forces of the future of digital trust and cyber(security) and the four scenarios bring a variety of implications. In the development of a future-proof strategy, it is important to capture and illuminate these in a structured manner.

This not only allows for capturing the significant volatility, uncertainty, complexity, and ambiguity of today and tomorrow, but also enables the translation of insights from driving forces and scenario analysis into strategic fields of action and individual priorities for management authorities, organizations, and other stakeholders.

For this purpose, our Strategic Foresight Team has developed the so-called Impact-Tree. The Impact-Tree is a method of representing implications in our Strategic Foresight approach. By connecting the 101 assessed drivers, the Impact-Tree highlights 9 strategic action areas with a total of 23 fields of implication. Each of these fields presents 2, 3, or 4 – totalling 74 – selected priority action options. Thus, the Impact-Tree takes initial steps in concrete strategy development. This strategy can and must be individually adapted to the various cybersecurity authorities and organizations, as well as other stakeholders in cybersecurity and their respective specifics.

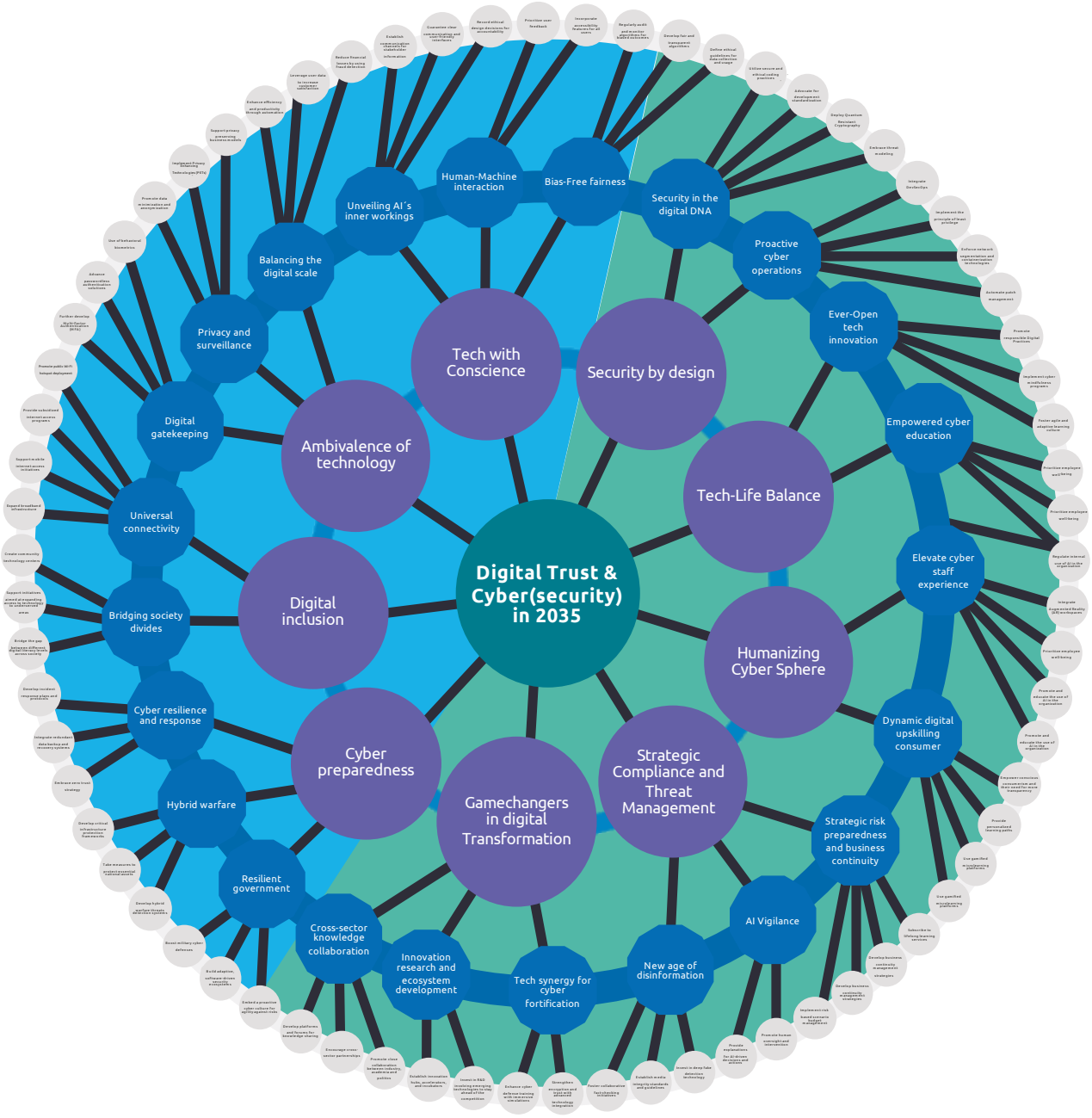
The basis for the Impact-Tree is, in the first step, the comprehensive 360° driving forces analysis using the STEMPLE approach. The socially, technologically, economically, militarily, politically, legally, and ecologically identified and validated driving forces are mainly grouped thematically into strategic fields of action within the focus and narrative zones. This allows for a clear presentation and division of the Impact-Tree and strategic fields of action into two zones, which provide information about the influence and uncertainty of the respective strategic fields of action. For example, the driver clusters from the focus zone mainly contain drivers that have been assessed as having high impact and high uncertainty regarding their development for the future of cybersecurity. Dealing with these action areas in further strategy development differs, for example, from action areas with low uncertainty and high impact. For these, there are often already strategies from the past that need to be analysed and considered. For the future of cybersecurity, we have defined 9 fundamental strategic fields of action – four in the focus zone and five in the narrative zone: Tech with Conscience, Security by Design, Tech-Life Balance, Humanizing Cyber Sphere, Strategic Compliance and Threat Management, Gamechangers in Digital Transformation, Cyber Preparedness, Digital Inclusion, Ambivalence of Technology.

Building on this, we have defined initial individual fields of implication for each of the nine strategic fields of action. These implication fields delve deeper into the strategic fields of action and clarify various core topics within each thematic field. They allow for a more targeted strategy definition and easier implementation of the resulting strategy through a clean thematic breakdown of individual strategic fields of action. For example, the strategic field of action area “Cyber Preparedness” is broken down into three fields of implication: Cyber Resilience and Response, Hybrid Warfare, and Cyber Armor for Organizations. In total, 23 such implication fields populate the Impact-Tree for the future of cybersecurity.

Subsequently, for each of these fields of implication, two, three, or four selected priority fields of action were identified. Thus, the Impact-Tree for the future of digital trust and cyber(security) includes a total of 74 selected priority fields of action. These provide initial selected impulses for a future-oriented setup of cybersecurity by 2035. For example, the field of implication “Cyber Resilience and Response” presents the following three fields of action: develop incident response plans and protocols, integrate redundant data backup and recovery systems, and embrace a zero trust strategy.

The Impact-Tree naturally does not paint a complete or all-encompassing picture. Instead, it provides a fundamental overview of focused, strategically essential thematic levels and selected action options. At a glance, interrelated future themes of cybersecurity can be located and addressed in a clear and structured manner. It should also be noted that the contents of the Impact-Tree are not absolutely distinct, and synergies and interfaces can be explored in the further strategy process. Depending on the project, it may be helpful or necessary to expand the Impact-Tree from different perspectives and further elaborate it based on organizational needs in the context of ongoing strategy development. The Impact-Tree provides a solid, foundational starting point for this.

Future of Digital Trust & Cyber(security) Impact Tree



Focus Topic
The focus topic is the central focus question of the Impact Tree

Strategic fields of action
The strategic fields of action represent the thematic grouping of drivers, mainly per zone

Fields of implication
Implication fields are thematic areas of the strategic fields of action

Selected priority fields of action
In addition to the diverse strategic options for action, we focus on priority fields of action, derived from the areas of implication of the strategic fields of action

Focus Zone
The focus zone contains drivers that were assessed as having a high impact and a high degree of uncertainty regarding their development for the future of digital trust and cyber(security)

Narrative Zone
The Narrative Zone contains drivers that were assessed as having a high influence and low uncertainty regarding their development for the future of digital trust and cyber(security)

Figure 6: Impact Tree

06

Getting there

Strategic Foresight implications for the future of digital trust and cyber(security).

Nora Preisker / Affinity to Technology

CSO & Deputy Managing Director Germany, Capgemini Invent

Affinity to Technology – or, putting it differently, the deep connection and familiarity that individuals, societies, and organizations have with technology – is already a cornerstone of our society, and the rapid evolution of new technologies boosts and intensifies this trend even further. Building a stronger tech affinity of our society requires trust by those integrating technologies into the digital realm, trust in the technologies themselves, and the need for establishing a secure cyber realm.

The increasing integration of Generative AI technologies, Augmented Reality, or the Internet of Things into our daily lives and work environment will reinforce our interaction with the digital world. Our society not only becomes more interconnected, but also strongly affected by immersive technologies that blur the boundaries between real and virtual life.

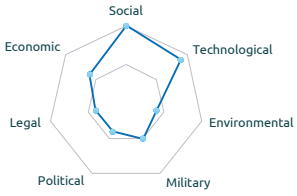
In the next decade, tech affinity can be a catalyst for groundbreaking innovation in all sectors, increase the operational efficiency of public and private organizations as well as individuals, and improve the societal experience through the development of state-of-the-art technologies. This technological immersion also poses challenges like privacy risks, cybercrime, social imbalances, and ethical dilemmas. These risks demand careful consideration, solid cybersecurity concepts, and robust regulatory frameworks. However, as a society affine to tech trends and developments, we can accept, apply, and manage the risks new technologies pose and thereby aim towards a harmonious coexistence of humans and technology, bringing together the best of both worlds.

Affinity to Technology – Focus Zone

Affinity to Technology

Affinity to technology refers to the degree of attraction, interest, and comfort that individuals have towards utilizing and engaging with technological tools, devices, and innovations. This affinity is a crucial factor in understanding how individuals interact with and adopt new technologies, as well as their willingness to embrace and integrate them into their daily lives.
For example, individuals with a high affinity to technology may readily adopt new gadgets and software, while those with a lower affinity may exhibit hesitancy or reluctance to engage with technological advancements.

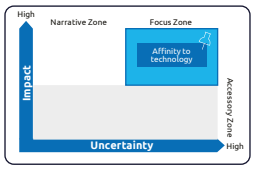
Stemple Categories



Affinity to technology is mainly influenced by the social and technological dimension. The social dimension plays a significant role as individual attitudes, values, and norms within a society largely determine the extent of affinity towards technology. For example, cultural values and the acceptance of new technologies can influence affinity. The technological dimension is also crucial as advancements and innovations in technology can impact an individual's affinity.

Relevance

Affinity to technology could have high relevance for the Future of Digital Trust and Security. Individuals' affinity to technology significantly influences their trust and confidence in digital systems and their willingness to engage with digital security measures. A study by the Pew Research Center (2021) found that individuals with higher affinity to technology are more likely to embrace digital tools and platforms, potentially impacting their perceptions of digital trust and security. Therefore, Affinity to technology could play a crucial role in shaping the future landscape of digital trust and security, as individuals' comfort and engagement with technology are connected with their perceptions of trust and security in the digital realm. Additionally, the relevance of Affinity to technology could be further enhanced by potential developments in technology that may impact digital trust and security, such as the widespread adoption of new technologies or the emergence of cybersecurity threats.



1990
The development of the World Wide Web revolutionizes how people access information, communicate, and utilize technology.

2023
The Apple Vision Pro enables the seamless use of augmented reality to interact with and enhance digital content within your physical space.

Exemplary Development

2019
The integration of 5G technology enables faster and more reliable wireless connections, further advancing technology usage.

2035+
Nano implants enable seamless integration of technology into the human body, revolutionizing the interaction with technology.

Figure 7: Driver Card for Affinity to technology

Felix Middendorf / Digital Mindset

Vice President | Head of Business Technology Germany, Capgemini Invent

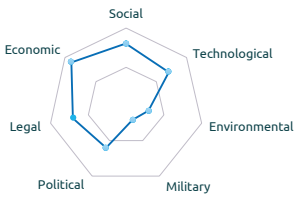
Trust in the digital sphere and cybersecurity require many different aspects. Of course, smart technology and adaptive organizations are important to keep us and our data safe, but adopting and fostering a digital mindset will be paramount. I am convinced that people and their digital mindsets will make the difference. They will define if we are not only able to catch and keep up with paradigm shifts and new technologies, but also if we can drive and design them for our benefit. To succeed, we need to acknowledge that digital technology will continue to change – both itself, the world around us and, by transition, also ourselves. We do not need to like this, but we need to accept that the pace of change will not stop or slow down. Only if we allow ourselves to let go and embrace opportunities for change, we can make progress in this infinite game. Of course, change also brings risk. Leveraging a digital mindset, we leverage data to calculate these risks and also to track the success of the changes at hand. Attackers will continue to find new vectors, defenders need to acknowledge that eventually there will be breaches and prepare for them. Hence, we have to allow ourselves to fail and to do so rather earlier than later, enabling iterative improvements as well as a positive culture of learning. Of course, well-established and risk-averse organizations and industries might have a harder time adapting than new players without legacy. But the good news is: it is all in our heads!

Digital Mindset – Focus Zone

Digital Mindset

A Digital Mindset reflects a flexible and proactive way of interacting with the digital world for individuals and organizations. It means being open to new ideas and understanding how digital progress and security work together. This mindset is important for recognizing the need for solid security measures that keep digital platforms secure and reliable. It also means being aware of cyber threats and taking steps to prevent them. As technology keeps changing, having a Digital Mindset is key for people and organizations to protect sensitive information and maintain trust online. It is pivotal in recognizing the need for robust security protocols as integral to maintaining the integrity and reliability of digital platforms. Furthermore, it involves a comprehensive awareness of potential cyber threats and the implementation of preventative measures to mitigate risks.

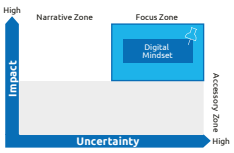
Stemple Categories



The Digital Mindset is influenced by social dimensions, as the collective willingness to embrace change fosters the adaptability for Digital Trust and Cyber(security). Technological forces also shape this mindset, with rapid advancements necessitating a reevaluation of the approach to digital threats and data protection. Legal dimensions ensure that there is a framework for dealing with data breaches, contributing to a comprehensive strategy for cybersecurity readiness.

Relevance

The Digital Mindset could stand as a critical driver for Digital Trust and Cybersecurity, serving as the cornerstone for the development and maintenance of secure digital environments. It could be argued that the cultivation of a Digital Mindset might significantly impact an individual´s or organization´s ability to anticipate, respond to, and recover from cyber threats. In the context of Digital Trust, a proactive Digital Mindset may enhance the ability to establish and maintain trust in digital interactions and transactions. As the digital landscape evolves, it is conceivable that the Digital Mindset could become increasingly relevant in identifying and mitigating risks, thereby fostering a safer and more reliable cyber ecosystem. Therefore, nurturing a Digital Mindset may be essential for ensuring the ongoing resilience and security of our digital lives. With the digital landscape continually evolving, a Digital Mindset would be critical for ensuring that individuals and organizations might be equipped to protect sensitive information and uphold trust in digital interactions.



1990
The ILOVEYOU Virus: One of the first major email viruses, highlighted the need for a digital mindset among users and professionals.

2022
Cyber Insurance market grows as cyber threats, highlighting a digital mindset that recognizes cyber security risks as a significant factor in the digital economy.

Exemplary Development

2018
The EU's General Data Protection Regulation came into force, making data protection and privacy a global concern and fostering a digital mindset that values personal data security.

2035+
The Digital Immunity Passport: A global system verifying individuals' cyber security knowledge and practices, promoting a digital mindset prioritizing personal responsibility in digital hygiene.

Figure 8: Driver Card for Digital Mindset

Christian Schmidt-Brockhoff / Cybersecurity Threats

Senior Director | Business Technology Germany, Capgemini Invent

"Without security, everything else is nothing." This was recently stated by former Chancellor Scholz at the 2024 Munich Security Conference regarding the Russia-Ukraine conflict. Although he primarily addressed military security, this now inevitably includes cybersecurity and defense against digital attacks.

Cyberattacks are already commonplace today, affecting both federal agencies and public institutions, as well as private sector companies. The nature and quality of attacks have become significantly more professional in recent years, not only due to current geopolitical tensions but also due to increased use of ransomware and extortion of significant ransom payments. Hacking has become a business model, and a lucrative one at that.

In the future, it is expected that the quality of attacks will further increase through the use of AI, while the attack surface will also greatly expand due to factors such as the cloud becoming a de facto standard and the interconnectivity of IoT and OT. Phishing attacks will become hyper-realistic by using Generative AI and deepfakes, making it insufficient for current awareness training to prevent them. AI-generated malware can be created faster, easier, and without deep technical knowledge, and is additionally more difficult to identify by traditional security software. Similarly, "adversarial attacks" on AI can noticeably and imperceptibly alter their behaviors.

At the same time, the use of AI also presents opportunities, such as earlier detection of attacks and triggering automated, efficient countermeasures. The use of machine learning and AI in the context of roles and access rights can reduce access rights to the bare minimum according to the need-to-know principle. For example, through the implementation of intelligent policy engines to implement a zero-trust architecture.

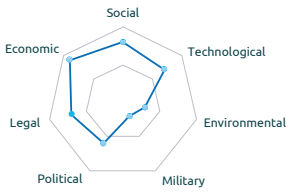
Companies, as well as governments and agencies, must prepare for the changing threat landscape and continue to enhance their cybersecurity capabilities. A clear cybersecurity strategy, understanding of critical assets, risks, and attack vectors, and derived security objectives and action areas remain crucial for efficient and targeted cybersecurity.

Cybersecurity Threats – Narrative Zone

Cybersecurity Threats

A cyber threat is an activity that aims to compromise the security of an information system by altering the availability, integrity or confidentiality of a system or the information it contains, or to disrupt digital life in general. Cyber attackers can be categorized into groups based on their motives and advanced methods. They try to gain access to devices and networks for various reasons, such as stealing computing power, stealing or modifying information, slowing down the network or demanding ransom. Some focus their attacks on specific individuals or organizations, while others attack weak systems indiscriminately. In general, each type of cyber attacker has a specific target.

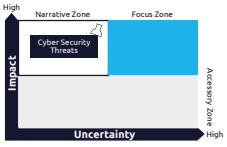
Stemple Categories



Cybersecurity threats are mainly influenced by technological forces, since the protection against them require robust protection measures and challenge the resilience of interconnected systems. Economically, these threats require investment to protect economic interests and can significantly impact market stability. Militarily, the rise of digital warfare requires advanced cybersecurity measures for national defense strategies to protect against espionage and coordinated attacks.

Relevance

Cybersecurity threats are changing the landscape of digital trust and security. The German Federal Office for Information Security (BSI) notes a shift in ransomware attacks to smaller organizations and public services, directly impacting citizens by disrupting essential services and risking breaches of personal data. The BSI also reports a worrying increase in software vulnerabilities, with an average of almost 70 new vulnerabilities per day - a 25% increase on the previous period, with around one in six being critical. In addition, the proliferation of generative AI tools such as ChatGPT is increasing the sophistication of cyberattacks by creating more convincing phishing campaigns and deepfakes, challenging existing defenses and highlighting the need for greater cyber resilience.Cybersecurity threats could have a profound impact on digital trust and security, undermining public confidence in online services and forcing both the private and public sectors to develop more resilient protection mechanisms.



1969
The first computer virus is used in 1969 at the University of Washington Computer Center.

2023
Cyber attacks are considered the top global risk according to the Allianz Risk Barometer.

Exemplary Development

2005
The NotPetya attack is considered the most costly cyberattack, with an estimated damage of 8 billion dollars.

2035+
The school subject cybersecurity is being introduced in German schools to raise awareness of digital crime issues.

Figure 9: Driver Card for Cyber Security Threats

Timo Graf von Königsmarck / Smart State

Managing Director Germany, Capgemini Invent

The concept of a Smart State is no longer a futuristic ideal but a tangible reality, redefining the very essence of governance and societal connectivity. This evolution can be a major leap forward, driven by the continuous progress of advanced technologies. At its core lies data-driven decision-making, an approach that wields information as the foundation for enlightened governance and efficient public service delivery. Within this envisioned Smart State, the citizen stands at the centre of all initiatives. Public services are no longer a one-size-fits-all solution but are tailored to meet the diverse needs of all individuals – whether they are citizens, citizens with disabilities, or refugees. This is a world where engaging with government services is as seamless as interacting with a sophisticated AI-driven virtual assistant, designed to understand and respond to a wide range of citizen needs and preferences.

The backbone of the Smart State of the future is digital trust and cyber(security). These are not mere afterthoughts or boxes to be checked but are ingrained in the DNA of every service, process, tool, and piece of infrastructure that the Smart State operates.

But what builds the road to this future? Collaboration is key. The creation of a Smart State is a symphony that requires the cooperation of various stakeholders – governments working hand-in-hand with tech innovators, research institutes, and the very fabric of society itself. This collaborative effort is crucial in guaranteeing a fair distribution of technological benefits and mitigating risks, thus circumventing any potential for societal disparity. A Smart State is a state that is deeply committed to fostering digital trust and fortifying cyber(security). The Smart State of the future can be an example of what can be achieved when technology and human-centric governance converge.

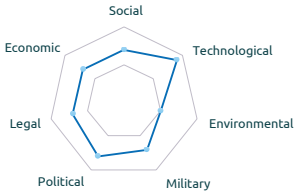
How does a future Smart State look like for you?

Smart State – Focus Zone

Smart State

A smart state leverages advanced technologies, such as information and communication Technologies (ICT), to enhance the efficiency, transparency, and services of the government. By strategically applying digital innovations, data analytics, connected infrastructure, and citizen engagement, a smart state aims not only to optimize administrative processes but also to establish modernized and citizen-centric governance. This approach seeks to improve the well-being of citizens, promote economic innovations, and pave the way for a sustainable development trajectory in society.

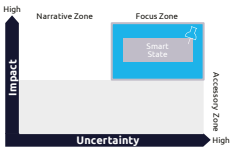
Stemple Categories



Smart State is primarily influenced by technological and political dimensions. Technologically, advancements are essential for digitizing government processes and implementing smart systems. Politically, policy-makers must create supportive legal frameworks and foster innovation. Examples include e-Government initiatives that require both tech solutions and political regulations for data protection. These dimensions are interdependent, as technology drives policy and vice versa.

Relevance

A smart state could be an important driver for the future of digital trust and cyber (security). By using advanced technologies such as blockchain and artificial intelligence, such a smart state could take concrete measures to improve cybersecurity and develop innovative approaches to threat detection. For example, the integration of blockchain technology could reduce uncertainties regarding data protection and data integrity. At the same time, AI-driven security measures could detect anomalies in real time and respond proactively to potential threats. An intelligent state could also promote trust in digital matters by using the possibilities of big data to gain more transparency about needs and thus better decision-making bases. This makes political decisions more predictable. This can lead to more tailored measures being taken. However, a future risk could also be that a smart state over-exerts its power by using technology and data in a way that compromises the individual freedoms and privacy of citizens by using extensive surveillance technologies or misusing collected data.



1966
The first electronic assistance system called Anti-lock braking system (ABS) is installed in a car.

2000
Drivers start relying on digital technology for route guidance (GPS), paving the way for further digital integration.

2021
Apex.OS, a comprehensive OS for autonomous driving, integrates all four mobility disruptors: autonomy, connectivity, electromobility, and shared mobility.

Exemplary Development

2035+
Fully autonomous vehicle fleets have been developed that integrate seamlessly into the traffic system, minimize accidents and protect the environment.

Figure 11: Driver Card for Smart State

Steffen Reidt / Blockchain for Digital Identities

Senior Director | Business Technology Germany, Capgemini Invent

In the landscape of future digital trust and cyber(security) 2035, several key drivers underscore the necessity for robust digital identities. Air-tight communication is becoming essential as individuals, organizations, and assets seamlessly interact through digital channels, and digital identities can further enable this while granting the needed level of security. The rising number of identity fraud incidents highlights the urgency for secure and self-sovereign data sharing, empowering individuals to have control over their personal information. Regulatory frameworks like eIDAS are also pushing for the adoption of digital identities, and the sum of these drivers makes secure digital identities increasingly important when looking towards 2035.

The positive impacts on the future of digital identity lie in eradicating identity theft and fraud and fostering trust in digital transactions. As a cornerstone, digital identity systems aim to establish trust across all demographics and enable self-sovereign data sharing for everyone. This doesn't only apply to individuals but also to machines and organizations; digital identities can provide the basis for secure communication ecosystems.

Investment in robust infrastructure is paramount. Governments and industries in Europe need to commit to developing a scalable foundation for global digital identities. Ensuring equitable access, particularly addressing demographic and educational gaps, is

crucial for widespread adoption. Collaboration for international standards is necessary to guarantee the successful use of digital identities across borders and sectors. European norms, already leading in this space, should set standards for organizations, but this will require substantial investments for further development and implementation.

Educating and engaging stakeholders across sectors is the critical starting point. Policymakers, industry leaders, and the public need to comprehend the benefits and challenges associated with digital identities. Incentives, ranging from funding to regulatory support, are vital in motivating collective action. Launching pilot projects across diverse sectors, such as finance, healthcare, and government services, is needed to demonstrate the practical benefits, gather real-world data, and refine approaches based on tangible experiences.

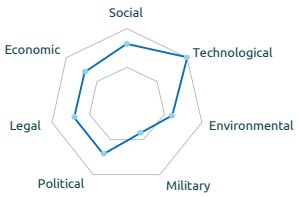
Digital identity's impact extends across various industries. In banking and finance, it revolutionizes KYC (Know Your Customer) processes, enhances fraud prevention, and, if used to its full potential, promotes financial inclusion. In healthcare, it ensures the secure sharing of medical records and verifies patient identities. Government services benefit from streamlined processes for documentation, voting, and public service access. Industries like energy and utilities can leverage digital identities for secure communication between pieces of infrastructure to support initiatives such as the decentralization of energy sources.

Blockchain for Digital Identities – Narrative Zone

Blockchain for Digital Identities

Blockchain in connection with Digital Identity refers to the integration of blockchain technology into systems that manage and authenticate digital identities. In this context, blockchain serves as a decentralized and immutable ledger that securely records and verifies digital identity information. By leveraging blockchain for digital identity management, individuals gain greater control over their personal data, while organizations benefit from enhanced security, transparency, and efficiency in identity verification processes.
For example, blockchain-based digital identity solutions can enable secure and tamper-proof verification of credentials, such as passports, driver's licenses, and academic certificates, reducing the risk of identity theft and fraud.

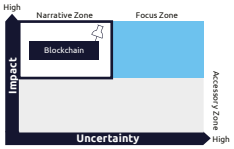
Stemple Categories



Blockchain, focused on Digital Identity, is primarily influenced by the Technological, Legal, and Social dimensions. Technologically, Blockchain securely stores identity data, enhancing trust. Legally, compliance with regulations like GDPR ensures privacy. Socially, acceptance and adoption are crucial, necessitating education and awareness campaigns for widespread trust and confidence.

Relevance

Blockchain with a focus on Digital Identity could hold significant relevance for the Future of Digital Trust and Cyber(security). The immutable nature of blockchain ensures that identity data remains secure and cannot be altered or manipulated without detection, reducing the risk of identity theft and fraud. Additionally, blockchain-based digital identity solutions empower individuals with greater control over their personal data, mitigating concerns over privacy and data sovereignty.



While the potential benefits of blockchain for digital identity are promising, uncertainties remain regarding scalability, interoperability, and regulatory compliance. However, with ongoing advancements and innovation in blockchain technology, coupled with increased awareness and adoption, the relevance of blockchain for the Future of Digital Trust and Security is expected to continue to grow exponentially. Therefore, Blockchain and Digital Identity could have a high relevance for the Future of Digital Trust and Security.

2008
Bitcoin-Whitepaper of pseudonym Satoshi Nakamoto introducing the blockchain technology.

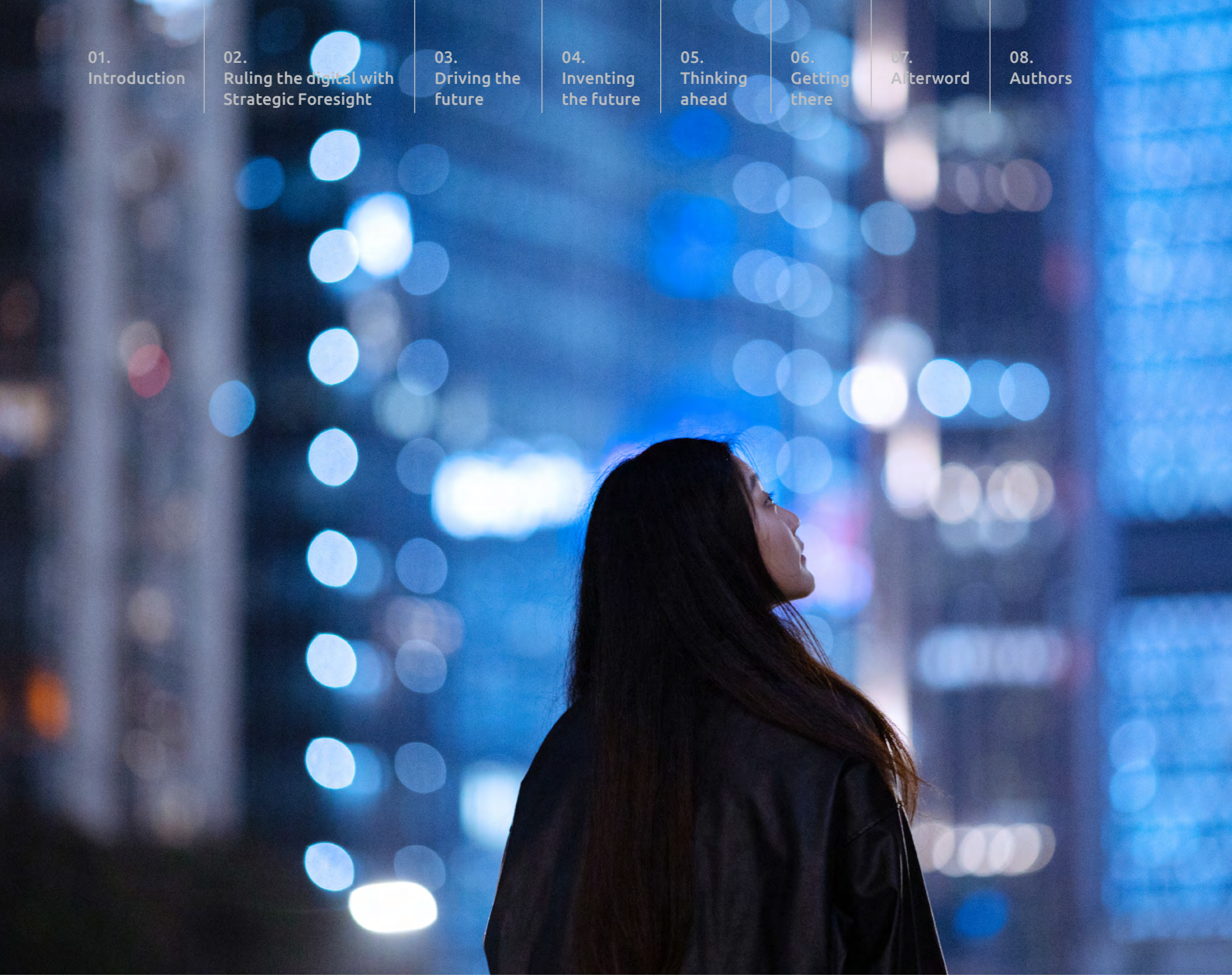
2024
The European Union adopts the new Digital Identity Framework.

Exemplary Development

2021
In response to the COVID-19 pandemic, countries and organizations begin to implement blockchain-based vaccine passports to verify individuals' vaccination status securely.

2035+
Biometric blockchain identity solutions are widely adopted, to offer highly secure and tamper-proof digital identities.

Figure 13: Driver Card for Blockchain for Digital Identities



Anna Schäfer / Internet of Everything

Director | Business Technology Germany, Capgemini Invent

Recently, Internet of Things (IoT) went through a decade of technological advancements, growth, and industry-wide adoption. Today, companies from large corporates to small startups are managing millions of connected devices and collecting daily data points ranging from smart homes, autonomous vehicles, up to industrial machinery.

While IoT is focusing on physical assets and "device-to-cloud" propositions, Internet of Everything (IoE) aims to seamlessly interconnect and orchestrate things, processes, people, and data. As the era of "Internet of Everything" is further expanding, companies are more and more establishing open IoT ecosystems by pooling capabilities from different partners to deliver best-in-class customer value and unlock new data monetization or revenue streams. However, the interconnected nature of IoT devices amplifies the effect that each and every one of these millions of connected devices offers an entry point for cyberattacks and data breaches. To maneuver this challenging landscape effectively, organizations must act today and invest in resilient and proactive security measures to safeguard sensitive data, its confidentiality, and the integrity of systems at all times.

Especially in sectors such as transportation, manufacturing, life sciences, healthcare, and energy, where IoT has become a commodity, the priorities for companies are focused around incorporating security features at every stage of the product development,

from design to deployment, and on implementation of encryption and authentication protocols rigorously.

Recently, the urgency to act has been elevated, as regulators such as the European Union are implementing new standards through the Cyber Resilience Act, which came into force in December 2024, and the Data Act, which applies from September 2025, to address growing cybersecurity threats and harmonize data handling and protection across the EU.

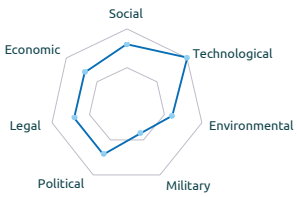
In order to position themselves for sustainable success in tomorrow's world of "Internet of Everything", companies must act now on the following priorities: (a) investment in robust cybersecurity measures, (b) build digital trust among consumers and ecosystem partners, (c) and upskill their workforce with extensive cybersecurity expertise.

Internet of Everything (IoE) – Focus Zone

Internet of Everything (IoE)

The Internet of Everything (IoE) builds upon the foundation of the Internet of Things (IoT) by seamlessly integrating people, processes, data, and physical devices into a vast interconnected network. This hyperconnectivity blurs the lines between the digital and physical worlds, fostering greater efficiency and sparking innovation across various industries. IoE facilitates data-driven decision-making, benefitting not only governments but also businesses, as it empowers them with invaluable insights for more informed choices. Personalized and convenient services, enriched by real-time feedback, enhance the quality of life and user experiences. Nevertheless, with the expansion of interconnected systems, security becomes a paramount concern due to the broader attack surface. The proliferation of data can pose challenges in terms of effective data management, potentially overwhelming existing infrastructures. This digital transformation may also disrupt traditional job markets, necessitating workforce adaptation and reskilling efforts. Additionally, ethical dilemmas arise as the collection of personal data raises questions about privacy and surveillance.

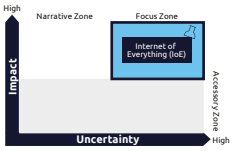
Stemple Categories



Internet of Everything is primarily influenced by the technological and economic dimensions. Technological advancements, such as the evolution of communication technologies and the miniaturization of sensors, make the extensive connectivity of devices possible. Economically, IoE is driven by the potential for increased efficiency and cost reduction across various industries, prompting substantial investments from both

Relevance

The Internet of Everything could be a relevant driver for securing digital trust and cyber security. Its key benefits, including improved data accuracy, enhanced monitoring, and predictive maintenance could lead to more efficient lives, convenience, and higher safety. For instance, smartwatches enable individuals to easily monitor their health in real-time, gaining valuable insights. IoE also promotes more efficient resource utilization, potentially resulting in cost savings. Moreover, it strengthens security by providing real-time monitoring and alerts for suspicious activities. Additionally, IoE's interconnected nature enables personalized recommendations, tailoring experiences to individual preferences. However, addressing potential security vulnerabilities and the expanded attack surface is crucial through the implementation of robust cybersecurity measures.



2010
Proliferation of smart home devices revolutionized how people interact with their living environments.

2026
Emotion-responsive smart homes that adapt to the people's physical as well as emotional needs by using IoT sensors and AI.

Exemplary Development

2016
Smart city initiatives adopt IoT technologies for traffic management, waste management and energy efficiency, enhancing sustainability.

2035+
Interactive public spaces that adapt to the number of visitors and weather by changing their lightning, soundscapes and landscapes for an enhanced experience.

Figure 14: Driver Card for Internet of Everything (IoE)

Tom Kussmann / Social Engineering

Senior Manager | Business Technology Germany, Capgemini Invent

In the labyrinth of cybersecurity, one aspect that continues to intrigue experts and practitioners alike is the phenomenon of social engineering. As we envision the landscape of digital trust in Europe by 2035, it becomes evident that understanding and harnessing the power of social engineering will be paramount.

Social engineering remains a compelling area of study for 2035 due to its ever-evolving nature. As technology advances, so do the tactics employed by cybercriminals. Anticipating these shifts and fortifying our defenses against them will be crucial in maintaining digital trust.

Social engineering holds the potential to shape our future positively by fostering a culture of cybersecurity awareness. Through education and training, individuals and organizations can become more resilient to manipulation tactics. Moreover, leveraging social engineering techniques ethically can enhance user experiences and facilitate seamless interactions in the digital realm.

To harness the potential of social engineering, we must invest in robust cybersecurity education and awareness programs. Additionally, developing sophisticated detection and mitigation strategies to counter emerging threats is imperative. Challenges lie in striking a balance between security measures and user convenience, as well as addressing the ethical implications of manipulating human behavior.

Every sector is affected by social engineering, and every individual relying on digital infrastructure is susceptible to the impacts of social engineering. However, critical infrastructure, financial institutions, and governmental organizations are especially targeted due to the potential ramifications of successful attacks.

Capgemini Invent is emphasizing the importance of integrating social engineering awareness and mitigation strategies into organizational cybersecurity frameworks. We help our clients by conducting regular assessments, training sessions, and simulations to help build resilience against social engineering attacks.

Industries dealing with sensitive data, such as healthcare, finance, and telecommunications, are likely to face heightened risks from social engineering attacks. Additionally, as IoT and AI technologies proliferate, sectors reliant on interconnected systems may become increasingly vulnerable targets.

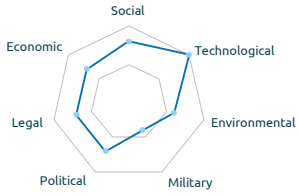
In conclusion, the future of digital trust in Europe hinges significantly on our ability to navigate the complexities of social engineering. By proactively addressing challenges and adopting a holistic approach to cybersecurity, we can pave the way for a more secure and resilient digital ecosystem by 2035.

Social Engineering – Focus Zone

Social Engineering

Social Engineering refers to a manipulative practice where attackers exploit human interactions to gain access to sensitive information or systems. This approach aims to leverage human behaviors and social dynamics to bypass security mechanisms. Social engineering techniques can take various forms, including phishing, spear-phishing, pretexting, and other tactics that seek to induce victims to perform undesirable actions or disclose confidential information.
In cybersecurity, preventing and raising awareness about social engineering attacks are crucial to ensuring the security of organizations and individual users.

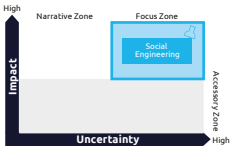
Stemple Categories



Social engineering has its main focus on the social dimension. It uses human psychology and social interactions to trick people into performing certain actions or disclosing confidential information. The technological dimension also plays a crucial role, as attackers can use advanced technologies such as deepfake or social media scrapping tools to make their deceptions more effective.

Relevance

Social engineering is a crucial factor that strongly influences both cyber security and trust in digital interactions. An example of social engineering could be the sending of fake emails inviting people to click on malicious links and thus disclose personal data. In terms of Digital Human Trust, there is uncertainty about whether people can trust authentic and secure interactions in the digital world. One example could be the creation of fake social media profiles to collect personal information and abuse the trust of users. This could lead to financial damage or data breaches. The future of social engineering remains uncertain as attackers are constantly developing new tactics. There is a possibility that social engineering will continue to increase in the future, especially with the advancement of digitalization and increased online activity. Therefore, continuously adapting security measures and increasing awareness of social manipulation is crucial to counter these threats. Because human behavior will always remain a weak point for attackers.



1984
Kevin Mitnick conducts one of the first social engineering activities by pretending to be an employee of a telecommunications company

2019
Attackers gain access to Twitter's internal systems and publish fraudulent tweets with profiles of celebrities including Barack Obama and Elon Musk

Exemplary Development

2016
Evaldas Rimasauskas pretends to be the CEO of American Tech companies and gains around 100 million US dollars through phishing technique

2035+
Attackers create a holographic image of a CEO and manipulate employees in online conferences to obtain sensitive data.

Figure 15: Driver Card for Social Engineering

Daniella Domoskos / Generative AI

Manager | Enterprise Data and Analytics Germany, Capgemini Invent

AI and GenAI are at the forefront of a transformative shift in digital trust and cyber(security) as we look towards 2035. Their exceptional ability to analyze current data and forecast future trends offers us a proactive stance to address cyberspace challenges. As these technologies continue to learn and evolve, they promise to revolutionize our approaches to digital security, positioning themselves as pivotal for what lies ahead.

The impact of AI and GenAI in enhancing cybersecurity and digital trust cannot be overstated. AI's capability to filter through extensive datasets to identify potential cyber threats before they escalate is remarkable, enabling us to strengthen our defenses preemptively. Additionally, AI's role in enhancing digital trust through advanced authentication methods, personalized experiences, and transparent privacy measures is exhilarating. Its adaptability offers a reliable safeguard against the uncertain landscape of future cyber threats, maintaining the security and integrity of our digital domains.

Addressing the ethical aspects of AI in cybersecurity presents a significant challenge. We must carefully balance the vast security advantages of AI with the imperative to uphold personal freedoms and privacy. Establishing a future that employs AI responsibly

necessitates a comprehensive legal framework, strict oversight, and continuous dialogue among stakeholders. Equally important is preparing our workforce for the upcoming AI-driven transformation in cybersecurity, highlighting the importance of education and skill enhancement.

A digitally secure and trustworthy future relies on a collective effort to improve AI literacy and advocate for ethical AI implementation. It is crucial for entities across sectors and individuals to actively pursue knowledge about AI's capabilities and ethical considerations. Experimenting with AI and GenAI in public sector projects could provide critical insights, showcasing their effectiveness in improving public services and cybersecurity infrastructure.

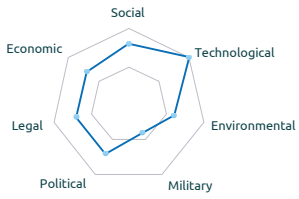
The public sector can significantly benefit from AI by advancing public services, government cybersecurity, and citizen trust. Nonetheless, it must address challenges like ensuring AI transparency, accountability, and preventing an increase in the digital divide. Through early and inclusive dialogues with diverse stakeholders, the public sector can effectively navigate these obstacles. By doing so, it can set a precedent for responsible AI and GenAI use, creating a foundation for a secure and reliable digital ecosystem.

GenAI – Focus Zone

GenAI

The term generative AI refers to computational techniques that are capable of generating seemingly new, meaningful content such as text, images, or audio from training data. The widespread diffusion of this technology with examples such as Dall-E 2, GPT-4, and Copilot is currently revolutionizing the way we work and communicate with each other.
Generative AI systems can not only be used for artistic purposes to create new text mimicking writers or new images mimicking illustrators, but they can and will assist humans as intelligent question-answering systems. The more users will familiarize themselves with these novel applications, the more they will trust or mistrust them as well as use or disuse them.

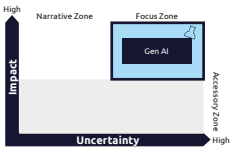
Stemple Categories



Generative AI is significantly influenced by the technological and economic dimensions. Technological-ly, advancements in machine learning, computational power, and data availability are pivotal for the development of generative AI models. Economically, the potential to disrupt and innovate across industries, from entertainment to pharmaceuticals, by drastically reducing costs and time for content creation and R&D, spurs investment into generative AI technology.

Relevance

Generative AI is redefining the cybersecurity landscape as tools like ChatGPT have expanded beyond creative applications to important cybersecurity functions. They are being used to automate threat detection, generate secure code and improve incident response. Conversely, the same technology poses new risks, such as the development of sophisticated phishing schemes or the circumvention of security protocols using advanced tactics such as reverse psychology. So, while GenAI can significantly boost digital trust, it also requires increased vigilance to protect against its potential to amplify cyber threats. Regarding digital trust, 70% of generative AI users in Germany trust content that is generated by gen AI. The expected growth of the generative AI market with a projected CAGR of over 24.4% by 2030 suggests a transformative impact on digital trust. However, this growth is not without its challenges. Ethical considerations as well as privacy and security concerns surrounding generative AI could influence the level of trust users place in digital systems.



1964
One of the first primitive generative AI was ELIZA. It was a text chat bot created in the 1960s by Joseph Weizenbaum.

2023
GPT-4 is released in March 2023, capable of generating texts up to 25000 words

Exemplary Development

2018
Groundbreaking Generative pre-trained transformers (GPT), a type of large language model, was introduced by OpenAI.

2035+
Personalized medicine uses generative AI to create precise treatments based on patient data, making healthcare more efficient and cost-effective.

Figure 16: Driver Card for GenAI

Juri Denecke / Software-defined Defence

Senior Manager | Public Sector Germany, Capgemini Invent [Dec 2022 - March 2026]

The digital domain has become a defining factor in shaping the defense landscape – in Germany and beyond. Scenario planning is one essential tool to navigate this complexity, but it must be paired with decisive technological transformation. Software and artificial intelligence are no longer optional; they are foundational to operational leadership and escalation dominance, both today and in the future.

"Software Defined Defense" (SDD) stands as the key paradigm for continuous capability development and interoperability for our allied troops. To build digital trust and ensure cyber resilience, heterogeneous capabilities are needed: digitally enhanced legacy platforms and agile, commercially developed, software-centric systems. These must be adaptable, rapidly updatable, and secure – without compromising robustness or operational value in harsh conditions.

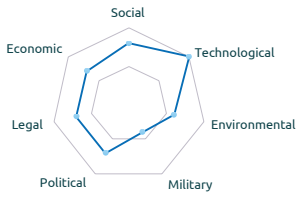
Decoupling hardware from software is a critical but complex requirement. Security-by-Design, Zero Trust, and Security-by-Default principles must be embedded from the outset. Yet, transformation from within existing structures remains challenging. It demands investment, strategic foresight, and comprehensive organizational change across both our armed forces and the defense industry – to write and build a secure digital future.

Software-defined Defence (SDD) – Focus Zone

Software-defined Defence (SDD)

Software-defined Defence focuses on leveraging software as a central driving force for enhancing defense mechanisms and digital security. It aims to harness the potential of software for continuous improvement and expansion of defense capabilities, while simultaneously ensuring the integrity, confidentiality, and availability of digital systems and data. By embracing SDD, the interoperability of systems can be enhanced, targeted adjustments to platforms made, and cyber resilience strengthened, thus contributing to the overarching goals of Digital Trust and Cybersecurity. The emphasis lies on creating a flexible, interoperable IT platform that enables rapid development, testing, quality assurance, and regular software deployment, while maintaining the highest standards of cybersecurity and digital trust.

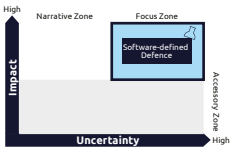
Stemple Categories



The military dimension has a high impact on software-defined defense, as it primarily aims to support the defense capabilities and mechanisms of the armed forces. Furthermore, technological factors influence SDD to a large extent, as the development, use and modernization of technology plays an important role in the continuous improvement and expansion of defence capabilities.

Relevance

Software-defined Defense could be a a key driver shaping the landscape of Digital Trust and Cybersecurity. As organizations increasingly rely on digital systems and networks, the automation and flexibility provided by SDD play a crucial role in enhancing cyber resilience and safeguarding digital trust. This is particularly pertinent for organizations tasked with protecting sensitive information and critical infrastructure from cyber threats, including government agencies, financial institutions, and critical infrastructure providers, such as the military. In the future, SDD could potentially revolutionize the way cybersecurity is approached, with the potential to further enhance digital trust through its scalable and centralized security controls. This could lead to a more proactive and adaptable cybersecurity framework, ultimately contributing to a more secure digital environment for various organizations, including those involved in national defense and security.



1984
The establishment of the first Computer Emergency Response Teams (CERTs) provides a foundation for software-defined strategies in cyber security response.

2022
he introduction of Artificial Intelligence for predicting and countering cyber attacks signified a shift towards more proactive software-defined defense strategies.

Exemplary Development

2016
SOAR platforms have become essential in streamlining and automating security operations, showcasing contemporary software-defined defense capabilities.

2035+
A highly innovative platform enables organizations worldwide to exchange information on security threats in real time and coordinate defence measures.

Figure 17: Driver Card for Software-defined Defence (SDD)

07

Afterword

Call to action

In an increasingly connected and technologized world, cybersecurity and digital trust in particular represent key challenges for the security of organizations in business, politics, and society. The digital transformation is closely linked to complex threat scenarios, ranging from targeted cyberattacks with infrastructure failures to manipulative information campaigns. At the same time, companies, authorities, and individuals depend on resilient and trustworthy digital systems to ensure economic stability and social progress.

This study on Digital Trust & Cyber(security) provides a methodological framework for the future-oriented analysis, identification, and evaluation of critical uncertainties in the digital space. By developing four future scenarios, social, technological, economic, ecological, political, and regulatory factors were identified that could have a significant impact on the digital security landscape in the coming years. Digital ethics is proving to be a key factor for sustainable security strategies, as technological advances without appropriate controls can give a false sense of security. This discrepancy between actual and perceived security poses significant risks, as it can lead to careless handling of security-relevant systems.

It is therefore crucial that both organizations and individuals take responsibility for strengthening digital resilience. This includes the use of advanced encryption technologies, the implementation of robust security architectures, and the continuous development of standards for digital trust mechanisms. The establishment of educational programs and training initiatives in the field of cybersecurity will play a key role in creating greater security awareness and enabling users to deal with the growing threats accordingly.

Ultimately, increasing networking offers not only risks, but also opportunities to optimize security-critical infrastructures. The consistent integration of security mechanisms into digital innovations can help to create a resilient and trustworthy digital environment. It is time to consider cybersecurity as a fundamental prerequisite for a functioning digital economy and society and to work together to build a secure, transparent, and technologically advanced future.

08. Authors

Felix Middendroff
Vice President | Head of Business Technology Germany, Capgemini Invent

felix.middendorf@capgemini.com

Annina Lux
Senior Manager | Business Technology Germany, Capgemini Invent

annina.lux@capgemini.com

Maximilian Lobbes
Manager | Business Technology Germany, Capgemini Invent

maximilian.lobbes@capgemini.com

Contributors:

Christian Schmidt-Brockhoff
Senior Director | Business Technology Germany, Capgemini Invent

christian.schmidt-brockhoff@capgemini.com

Marius Fischer
Senior Manager | Business Technology Germany, Capgemini Invent

marius.fischer@capgemini.com

Special thanks to:

Timo Graf von Koenigsmarck

Nora Preisker

Steffen Reidt

Tom Kussmann

Juri Denecke

Anna Schäfer

Daniella Domoskos

Colin Rode

About Capgemini Invent

As the digital innovation, design and transformation brand of the Capgemini Group, Capgemini Invent enables CxOs to envision and shape the future of their businesses. Located in over 30 studios and more than 60 offices around the world, it comprises a 12,500+ strong team of strategists, data scientists, product and experience designers, brand experts and technologists who develop new digital services, products, experiences and business models for sustainable growth.

Capgemini Invent is an integral part of Capgemini, a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Make it real | www.capgemini.com

Capgemini invent