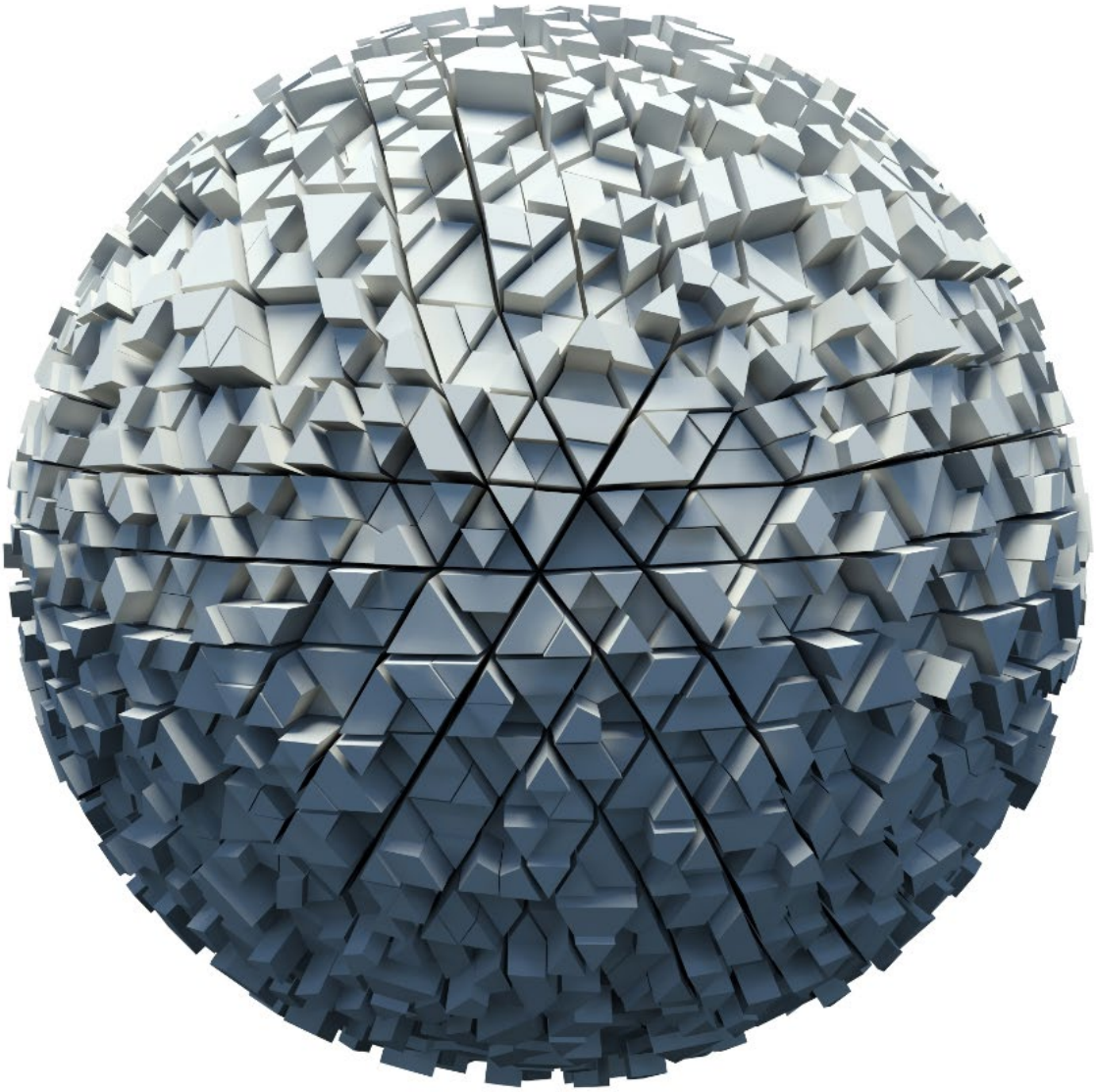
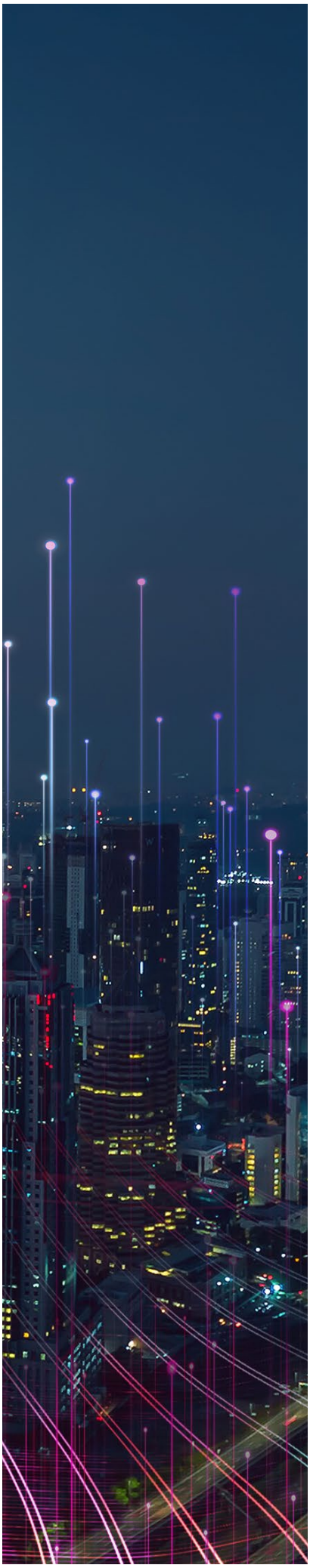
Deloitte.



Future of Cyber Risk 2035

A Glimpse into the Future of the Cyber Risk

center for the long view



Scenario Thinking

A Glimpse into the Future of Cyber Risk

Digital transformation is essential in today's world. While the COVID-19 pandemic has shown us yet again that there is still much to be done in this area, it also made another thing blatantly clear: In the future, digital transformation is inevitable. And the future starts now.

When it comes to digitalization, there are critical questions that we have to address: What kind of cyber risks will we face in the future? How will we manage them? And who will take on that responsibility? Among the many different forces shaping cyber risk, some are easy to identify, while others are lurking in the shadows.

In order to develop robust yet flexible strategies to manage cyber risk, we must address these questions and understand the complexity surrounding the topic of cyber risk. The decisions made by private, public and civil society stakeholders today are going to shape the world of tomorrow. That's why it isn't enough to have cyber risk-related strategies that only react to the most recent developments. We have to actively shape the social, technological, economic, military, political, legal and environmental developments in cyber risk, and we have to do it now. A first vital step is identifying existing, emerging and future drivers to better understand the relationships and interactions between forces at play. The developments around the global COVID-19 crisis have highlighted once again the necessity for proactive strategic future planning on Cyber and cyber risks. However, traditional methodologies are ill-equipped to be effective in this area.

It is, of course, impossible to predict the future. But we can use scenario planning to gain much deeper insight into potential future developments by capturing uncertainty and reducing complexity. The stories these scenarios tell us about potential future worlds allow stakeholders to develop strategies and make decisions that steer developments in a positive direction.

In response to the question of what cyber risks could look like in Europe in 2035, we developed four possible scenarios:

Scenario 1: Star Trek

Following lethal cyber attacks targeting the weaknesses of the digital scramble and heavily strained systems during the COVID-19 pandemic in the early 2020s, cyber risks are managed successfully economically, politically and socially through an increase of private and public cyber spending, one strong common cyber regulation and cooperation and a digitally literate society by 2035. While the government found its purpose in coordinating the cyber environment, the private cyber sector is flourishing, and the economy is growing in this secure environment. Stricter regulations have, however, curtailed cyber innovation, and for all of its advantages, the seamless integration of systems creates a single point of failure – vulnerability is still lurking just below the surface.

Scenario 2: Pandora's Box

In a politically and economically fragmented post COVID-19 cyber landscape, cyber risks are pervasive. In response to the governmental vacuum, the economy and society have self-organized. The lack of regulation was a watershed for innovation. Islands of specialized expertise emerged as a result, led by the few digitally literate experts. Small and large-scale cyber attacks are frequent and often impose major economic burdens. However, while the cost of security is strangling the economy and society, redundancies within the cyber landscape and continuous renewal through innovation ensure a basic level of security.

Scenario 3: Mad Max

Cyber Darwinism has conquered Europe. Massive A.I.-powered cyber attacks have put Europe in a constant state of cyber emergency as a direct result of the COVID-19 crisis, and cyber offenses are pervasive. Thanks to an urgent need to innovate in order to survive as well as major cyber spending in the public and private sphere, game-changing innovation and a vibrant start-up culture are driving the cyber market. The impact of cyber risks on physical security has resulted in the establishment of gated communities, and selfishness is dividing society. Mistrust of the public and private sector and within society lead to a large number of digital opt-outs and a long-term slow-down of digitalization.

Scenario 4: The White Queen

Because governments have proven unable to cope with cyber risks, especially those triggered by the rush to digitalize during the COVID-19 crisis, a conglomerate of tech giants has become the sole provider of security. In a highly secured environment, they have assumed responsibility for most governmental functions to fill the gap left by the public sector. To ensure compliance with security measures, social controls have been established by the dependent government. While large sections of the population are content with the stability, security and convenience of their new world, protests are on the rise against the government and the tech conglomerate, accusing those in power of creating "cyber cartels". With its seamless integration and as a single source of power, the cyber conglomerate remains vulnerable to attacks.

Cyber risks accompany the digital transformation that is changing our world. These four scenarios show how different the future of cyber risk could be.

Join us on a journey into these four alternative future worlds and what they mean for all of us.
Enjoy the ride, Risk Advisory

Drivers of the Future of Cyber Risk

Factors Impacting Tomorrow's World

A large number of factors with different origins have the potential to shape the future of cyber risk. These driving forces, or drivers, are variables that will or could influence how the future of cyber risk could look like in 2035. They vary in their impact, and their actual effect is often difficult to pinpoint due to the complex interlinkages and interactions between individual drivers.

To cut through this complexity, we used a methodology of comprehensive driver analysis that combines AI-based analysis with human expertise. Our analysts scan and analyze a vast knowledge landscape to create a holistic picture focused on social, technological, economic, military, political, legal and environmental drivers. Looking at the future of cyber risk, we created a shortlist of 100 of such drivers.

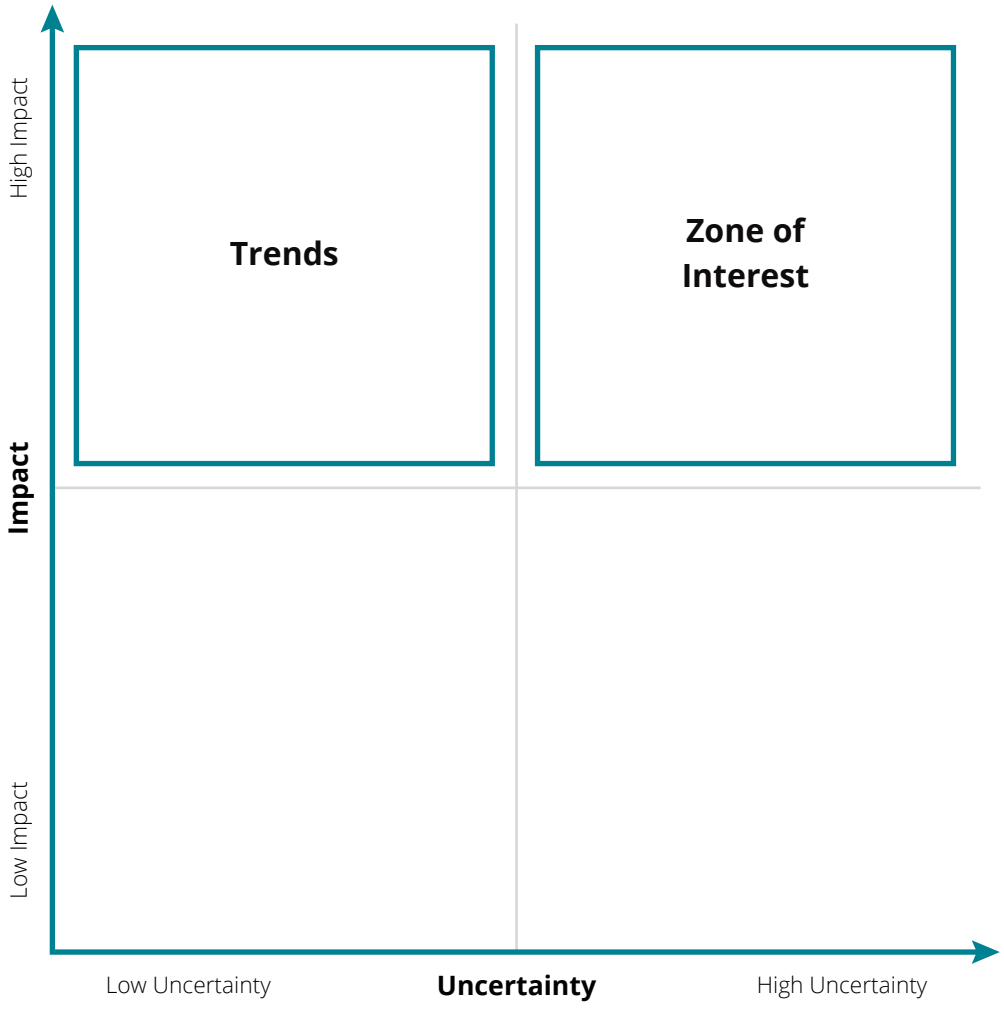
An interdisciplinary group of subject matter and industry experts rated each individual driving force on its likely future impact and uncertainty. This enabled us to focus in on two groups of drivers: highly impactful and very uncertain drivers form our "Zone of Interest" and highly impactful and very certain drivers are classified as "Trends" (Figure 1).

The Zone of Interest in this case contains 38 drivers, including such factors as the level of digital literacy, severity of cyber threats, availability of cyber talent, EU dependence on foreign technologies and perception of cyber risk as a threat to the environment. Another 32 drivers were identified as Trends. Examples here include the role of AI and machine learning, media attention on cyber security, political cyber espionage and C-suite involvement in cyber security strategy.

Even though each individual driver has its own unique impact, most of them are interconnected. The highly impactful and very uncertain drivers in our Zone of Interest can be grouped into clusters called "Critical Uncertainties", which form the basis for our scenario framework.

A large number of factors with different origins have the potential to shape the future of cyber risk.

Fig. 1 – Driver rating according to driver´s individual impact and uncertainty



Critical Uncertainties of the Future of Cyber Risk

The defining questions of the future

Critical Uncertainties are the "Million Dollar Questions" of the future. They have the potential to steer future development in one direction or another. For this reason, we have located our Critical Uncertainties along a spectrum between two extreme end-points. Our experts clustered the 38 drivers from the Zone of Interest into five Critical Uncertainties, two of which were then selected to define the two axes of our scenario framework for the future of cyber risk. The remaining three later function as important signposts for the narrative of each scenario. Our experts selected the following two Critical Uncertainties for this scenario set:

Critical Uncertainty: Level of Integration of Cyber Security into Technology – Patchwork versus Seamless Integration

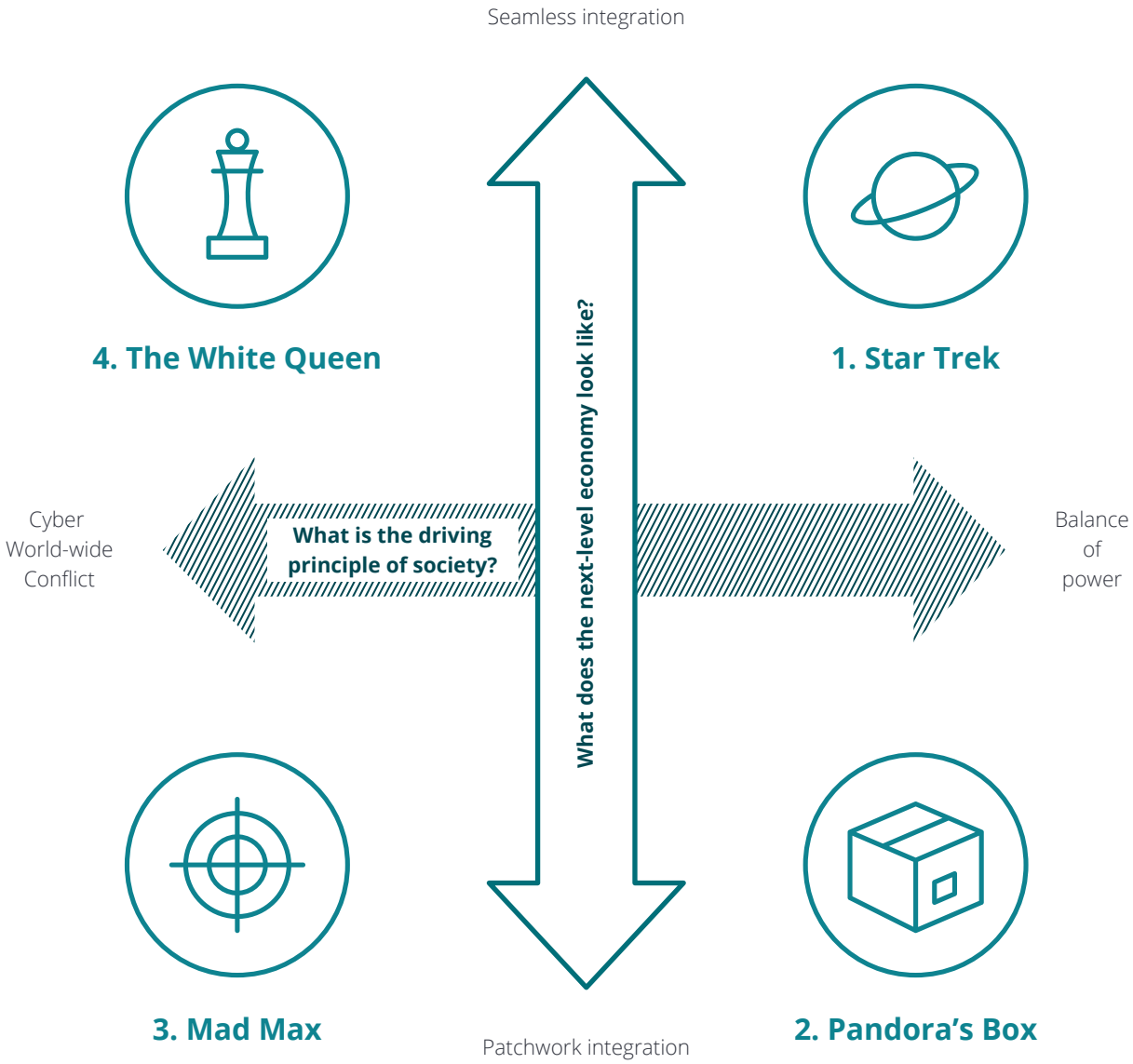
The first Critical Uncertainty selected by the expert panel is the question: "What is the level of integration of cyber security into technology?" It includes the following drivers from the Zone of Interest: security convergence of IT, OT and product safety, role of blockchain, role of quantum computing, conflict of physical and cyber security in private organizations, impact of net neutrality and secure protocols. The degree of integration of cyber security into technology shows how important security concerns and measures – including cyber vigilance and cyber resilience – are for the research, development, deployment and maintenance of technology products and services. Cyber security integration exists on a spectrum between patchwork solutions on the one side and seamless solutions on the other. In the former case, security concerns and measures are – if at all – only partially inbuilt into technology products and services. Cyber security plays a subordinate or negligible role. At the other end of the spectrum, security concerns and measures are completely and intrinsically inbuilt into technology products and services. Cyber security plays a natural and important role.

Critical Uncertainty: Nature of the "Cyber Battlefield" – Worldwide Cyber Conflict versus Balance of Cyber Power

The second selected Critical Uncertainty is the question: "What does the ´cyber battlefield´ look like?" The following drivers are included in this cluster: cyber security of critical infrastructure, influence of disinformation, dual use of cyber technology, development of computing power, EU dependence on foreign technologies, cyber warfare and the role of the government in cyber security. The nature of the "cyber battlefield" describes the status of cyber as an arena for economic, political, social and military activity. On the one extreme, the "cyber battlefield" can erupt into a worldwide cyber conflict. Cyber confrontations between major powers are frequent, creating tension and instability in the economic, political, social and military sphere and often resulting in conflict in these areas. On the other extreme, there is a balance of cyber power, defined by stability and harmony between economic, political, social and military powers regarding cyber issues. Interactions in or concerning the cyber space occur, but without triggering any long-term tension. Economic, political, social or military clashes are short-lived and minor.

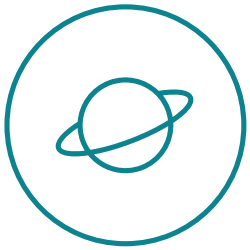
Combining both Critical Uncertainties in a two-by-two matrix creates a framework for our four alternative future scenarios (Figure 2). All four must meet five criteria: they must be plausible, challenging, balanced, relevant and divergent. Each world tells a different story about the future of cyber risk and gives a different answer to the question of what the future of cyber risk might look like in 2035. While we do not expect any one scenario to transpire exactly as described here, thinking about these alternative futures in their extreme forms allows stakeholders to take a flexible and proactive approach to navigating any developments in between these extremes.

Fig. 2 – Scenario Framework – Four possible scenarios on the future of Cyber Risk



The Future of Cyber Risk in Europe 2035

Four Possible Scenarios



Scenario 1: Star Trek

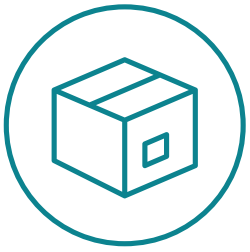
This world is characterized by a balance of power in cyber and a seamless integration of cyber security into technology.

In this scenario, we live in a stable, optimistic and forward-looking world. Europe is a highly technologized society, and cyber security has become a commodity. Massive A.I.-powered cyber attacks exploited vulnerabilities resulting from the digital scramble during the COVID-19 crisis, costing the lives of civilians even after SARS-CoV-2 was contained. This has raised public awareness for cyber issues and led to a sharp increase in cyber budgets and regulation in the early 2020s. The emergence of young cyber activist leaders has triggered large-scale protests advocating for the cyber security of all citizens and for the preparedness and readiness for future crises, such as developing digital tools for remote education. As smart cities, IoT, cloud systems and quantum computing become more widespread, security-as-a-service has become the norm. Consumers have come to expect operational excellence as standard, warranting strong cyber defenses.

By the mid 2020s, cyber spending is a key part of public budgets, including in healthcare, education as well as defense. A.I.-powered cyber defenses have been the focus of public cyber innovation. Successful cyber regulation has downgraded cyber risks and, as everyone is adhering to a uniform cyber standard, the economy and the society are running smoothly without cyber challenges. In this highly cyberized society, the second generation of digital natives is in power. Government has found its role in managing highly complex cyber regulation and ensuring compliance with the standards they have set. The cyber environment is highly coordinated, and the private sector, the public sector and civil society are all cooperating across borders to successfully contain cyber risks in the digital world. Europe has become the biggest exporter of cyber security, and the European Cyber Security Pass has become the established seal of quality for product security. People live largely digitalized lives, and cyberspace is a safe arena for social, political and economic exchange at the local, regional and global level.

However, while the high level of cyber security has enabled industry innovation to flourish, innovation in the cyber space is stalled due to the strong web of cyber regulation. While the costs of cyber security are generally manageable in most areas, developments in cyber are largely contained by strangling costs for entrepreneurs. Equally, seamless integration poses the risk of introducing a single point of failure, which means cyber risks are still lurking just below the surface. There is a lot of pressure to keep developing cyber security measures and products, and a danger to succumb to "no news is good news" attitude defining this world.

Scenario 2: The lack of governmental response in the early 2020s to the cyber challenges spotlighted during the COVID-19 pandemic has resulted in a fragmented cyber environment with thousands of standards and a lack of regulation.



Scenario 2: Pandora's Box

This world is characterized by a balance of power in cyber and a patchwork integration of cyber security into technology.

The dawn of a new decade has changed nothing in cyber. The lack of governmental response in the early 2020s to the cyber challenges spotlighted during the COVID-19 pandemic has resulted in a fragmented cyber environment with thousands of standards and a lack of regulation. When the government failed to keep pace with the rush to digitalization, the private sector took over and gave free rein to entrepreneurs, enabling innovation to flourish in this agile world. Small islands of specialized expertise have emerged across Europe, and SMEs have displaced technology giants as leaders in specialized technology. Millions of small innovations have swamped the market – but while they are helping to cope with challenges, they are not solving the quintessential problems in cyber and elsewhere. Technologies have become more and more complex, and the few highly skilled cyber natives have left the vast proportion of the digitally illiterate society behind, which is stuck in digital basics and unaware of security concerns.

In response to the governmental vacuum, the economy and society have self-organized, resulting in a chaotic alliance of the willing in cyber security. The public sector is completely dependent on the private sector for cyber security expertise and solutions. Through the messy constellation of regulation and activity in and pertaining to cyber, Europe has become impossible to defend digitally, particularly in the wake of the rush to digitalization during the COVID-19 crisis. Consequently, fragility and the social and political perception of cyber risks are high. Both small and large-scale cyber attacks are frequent and often impose a large social, political and economic cost. Economic cyber espionage on cyber security solutions has become the norm. This hostile security environment hinders cooperation and challenges globalization, leading to a multipolar (digital) world order. The only place where there is any meaningful collaboration is in the bare necessities – transferring technology from one remote expert island to another for the sake of security. While the cost of security is strangling the economy and society, redundancies within the cyber landscape and continuous renewal through innovation have led to a basic level of security – so far preventing a massive blackout attack.

Scenario 3: Mad Max

This world is characterized by a worldwide conflict in cyber and a patchwork integration of cyber security into technology.

By 2035, the cyber landscape in Europe has become utterly Darwinist, granting survival to only the strongest and instilling a "me first" attitude within the economy, politics and society. Focused, persistent cyber attacks on critical infrastructure and citizens following the COVID-19 rush to digitalization have caused massive political and social upheaval, leading to large investments in cyber. The irrevocable need to innovate in order to survive has led to a large amount of cyber innovation and a start-up dominated market, but severely curtailed product innovation. This has been intensified through globally coordinated A.I.-powered cyber attacks with high death tolls, such as large-scale power outages across Europe and beyond.

Since the end of the COVID-19 crisis, Europe has lived in a constant state of cyber emergency. All political and diplomatic endeavors to establish some form of cyber governance have failed; the cyber landscape is completely fragmented both politically and legally. The economy is suffering significantly, and without economic and political cyber alliances, it is impossible to cope with the stifling costs of cyber security. Much effort has been invested in the development of hybrid weapon systems, and military cyber offenses have become a socially and politically acceptable measure in cyber security. Cyber strikes by state and non-state actors have become a regular part of daily life, and mandatory cyber drills ensure the readiness of the population in case of cyber attacks.

Media attention on cyber is large, especially in light of the ever-increasing risks of IoT, A.I. and similar developments. The impact of cyber risks on physical security has resulted in the establishment of gated communities, and selfishness is further polarizing society. There is a high distrust towards the public and private sector and within society, leading to a large number of digital opt-outs and a slowing down of digitalization. Politically and socially, Europe has returned to a highly-digitalized stone age.

Scenario 4: The White Queen

This world is characterized by a worldwide conflict in cyber and seamless integration of cyber security into technology.

In the early 2020s, large-scale cyber attacks, especially with the uncontrolled digitalization rush resulting from the COVID-19 pandemic, have led to increasing fear and social instability. With the government having lost the citizens' trust due to its inability to respond to cyber threats, technology giants have used the high perception of cyber risk to increase their economic and political power by becoming the main provider of cyber security. This results in a dependency of the public sector and the society on the private enterprise cyber knowledge and capabilities. Technologies including A.I., Cloud Computing and emerging cyber security technologies are entirely controlled by this cyber tech group, making it the single source of protection.

Highly efficient in-house innovation among these few players has created a cyber conglomerate of technology stakeholders that sell protection to both the government and its citizens. The dependent government has put in place a coordinated and highly regulated cyber space, with strong cooperation on data exchange. To ensure compliance with security measures, social controls have been established by the government and are monitored by the cyber conglomerate. Cyber security has therefore emerged as a major strategic issue by the mid-2020s. More and more, the cyber conglomerate has taken on governmental tasks, including education and social welfare. Basic digital literacy has moved to the center of attention as the first level of cyber protection, making it a given in society.

While large parts of the population are content with the stability, security and convenience of their world, protests are on the rise. Activists are calling out the captive government and the rapidly increasing power of the conglomerate, accusing them of becoming a "cyber cartel". While the economic costs of cyber security are manageable, the social costs remain heavily contentious. Equally, with its seamless integration and as a single source of power, the cyber conglomerate remains vulnerable to attacks. The Cyber Resistance Activists are exploiting this fact more and more to weaken the social, political and economic system.

Conclusion

Our four alternative stories: The Future of Cyber Risk 2035

Star Trek, Pandora's Box, Mad Max and The White Queen represent only four alternative future worlds of what cyber risk could look like in 2035. Rather than predicting the exact outcome of the future, the four scenarios describe different frameworks and directions of possible future development. However, all four scenarios make clear that cyber risk will affect the economy, society and politics in various ways and that it is crucial for stakeholders and decision-makers to develop robust, yet flexible strategies and policies.

These four scenarios are not a solution, but rather a starting point for strategy development. They are the launching pad for our efforts to create a secure cyber future. In order to define and deal with the implications of each individual scenario, stakeholders need to cooperate and drive change. These radically different alternative futures make a number of things abundantly clear:

Cyber presents us with unique opportunities and with unique threats. To successfully navigate them both, we need to ensure proactive preparedness for, and an effective response and reaction to, cyber risks. The ability to remain in the game will be the key to success as cyber risks continue to evolve. Technology alone is not sufficient to rise to these challenges, but neither is individual action. Only through close stakeholder cooperation between the private and the public sector as well as civil society, continuous action and the combination of technology with human expertise and experience can we drive cyber.

The COVID-19 crisis has triggered a digitalization rush that opens up a myriad of opportunities. However, as we speed up digital transformation, we also need to speed up cyber security. In the end, it is up to all of us to shape our future. Let's make the first step today!

Methodology

The Center for the Long View Dynamic Strategy Approach

This report on the future of Cyber Risk 2035 is based on the seven-step scenario methodology of the Center for the Long View (CLV).

The CLV's dynamic strategy approach supports and enables stakeholders and decision-makers to build robust and future-proof strategies in a world characterized by uncertainty. The method combines prevalent scenario-planning methodologies with human intuition and innovative technology, following the seven distinct steps explained below. While we focused on steps one to five in this study, steps six and seven are essential to ensure the strategic validity of scenarios in the long run. Throughout the entire process of this project, we followed the guiding principles of scientific research, including objectivity, reliability and validity.

Step 1
Definition of the Focal Question

In order to set the focus of the study, the focal question is defined in a first step. Each individual component of the focal question's phrasing is analyzed in this process to ensure a common understanding the central topic of the project. Preliminary research and an initial analysis by the CLV's AI-based research tool, Deep View, support the process of defining the focal question. The goal of the initial research is a holistic and general identification of key topics that are relevant to the study. The focal question of this study was: "What could Cyber Risk in Europe look like in 2035?"

Step 2
Identification of Driving Forces

In a second step, future drivers and developments are identified and analyzed. Drivers are defined as those factors that can or will have an influence on the central topic in the future. The overarching goal of this second step is to create a list of the most relevant trends and driving forces affecting the key topic.

The CLV developed a threefold process of identifying key driving forces. Its main focus lies on the CLV Deep View analysis. Deep View is an AI-based trend-sensing tool that uses a proprietary natural-language processing software to conduct extensive analyses of articles, blogs, M&A transactions and patents. Deep View reads and understands the output of more than half a million sources within seconds, creating trend-based knowledge maps of interrelated current and developing topics. Complementary to the AI-based analysis, traditional desk research picks up the Deep View insights and focuses on prevalent trends in relevant key reports and publications. In addition, our analysts conduct interviews with internal and external experts to critically evaluate the validity of the Deep View and desk research results and gain further insights into what drives the future. Based on this threefold approach – Deep View, desk research and expert interviews – our team of analysts develops a detailed list of drivers that will, or could, affect the focal question. To ensure the driver list has a holistic character, we employ the STEMPLE framework, focusing on social, technological, economic, military, political, legal and environmental factors. Naturally, these seven categories are not mutually exclusive, and drivers can often be grouped into two or more categories. However, employing the framework ensures the driver list is well-rounded. A short-list of these drivers is then rated by an expert panel regarding their impact and uncertainty. Based on this expert rating, drivers are divided in four categories: those a low degree of uncertainty, which we refer to as Trends, those with a low impact and a low uncertainty, and those with a low impact and a high uncertainty. In the following steps, we then focus on the driving forces located in the Zone of Interest and the Trend section.

The method combines prevalent scenario-planning methodologies with human intuition and innovative technology, and follows seven distinct steps.

Step 3
Definition of Critical Uncertainties
Moderated by a CLV Scenario Team, a diverse selection of experts prioritizes and groups the highly impactful and highly uncertain drivers from the Zone of Interest into "Critical Uncertainties". Critical Uncertainties have the potential to shape the future in different, opposing ways. Two extreme endpoints of possible developments are defined for each Critical Uncertainty. While the focus in this step is clearly put on the Zone of Interest drivers, all drivers are used to develop the scenarios.

Step 4
Establishing the Scenario Framework
In a fourth step, two Critical Uncertainties are selected by the experts to form the two axes of our scenario matrix. As a result, four quadrants emerge around this framework, showing four possible alternative future worlds.

Step 5
Development of Scenario Narratives
Each of these four alternative futures is now storylined with a narrative. The remaining three Critical Uncertainties not used to form the axes as well as the Trend drivers serve as building blocks for the scenarios. Each narrative describes an alternative future and its trajectory of development between today and the time horizon defined in the focal question. All scenarios must fulfil five criteria: they need to be plausible, relevant, divergent, balanced and challenging. Crucially, we do not believe that individual scenarios will unfold in reality precisely the way it is described in the narratives. Instead, we see these four scenarios as extreme endpoints that allow a myriad of developments in between. As such, scenarios stretch our thinking and challenge the status quo.

Step 6
Determining the Implications
In a sixth step, we use the scenario narratives to derive consequences and potential courses of action or relevant stakeholders. Existing strategies are tested against each scenario and adjusted where necessary. At the same time, new strategic options are formulated. To ensure the long-run validity of these strategic options, consistent long-term monitoring of the scenarios is necessary.

Step 7
Monitoring the Scenarios
In order to monitor the developments described in the four scenarios, Deloitte has developed the AI-based modular tool Gnosis. Gnosis tracks developments and changes using indicators developed for each scenario and monitors them over time. To be able to track developments and changes with Gnosis, we develop indicators for each scenario and monitor them over time. By putting them into context with each other, any rapid and small alterations in our scenarios become evident, and the movement towards individual scenarios can be tracked. Explorative, AI-based research adds new drivers and allows for subsequent adjustments of the scenarios to new developments. This step is highly important to ensure that both the scenarios and the strategies remain up-to-date with current and future developments.

Contacts

Peter Wirnsperger
Leader Public Sector Germany
Risk Advisory
Tel: +49 40 32080 4675
pwirnsperger@deloitte.de

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

Florian Klein
Head of Center for the Long View
Monitor Deloitte
Tel: +49 69 9713 7386
fklein@deloitte.de

Deloitte.

Issue 06/2020