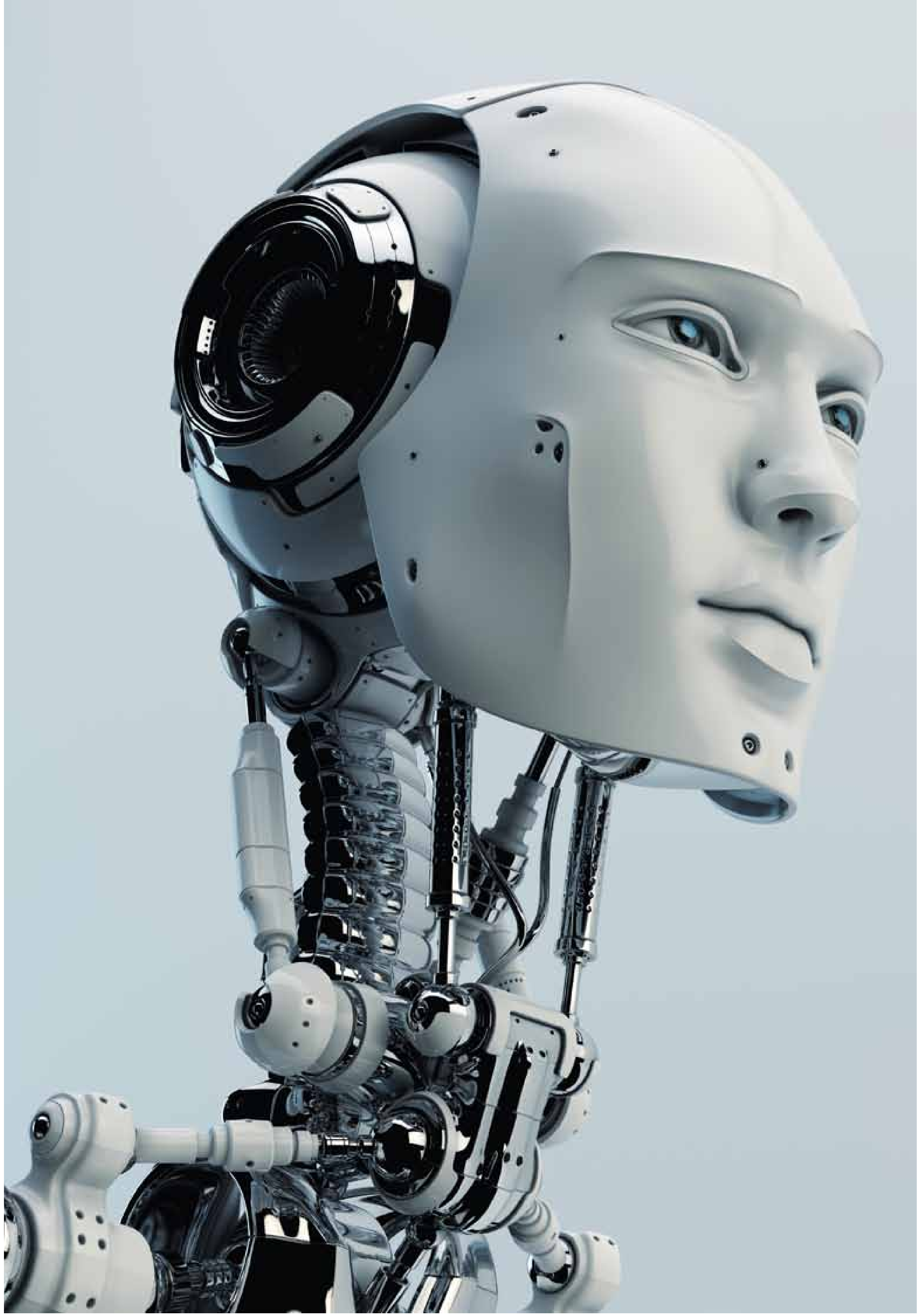
Deloitte.

European Cyber Defense

Part 2: Future of Cyber Security 2030

center
for the long view



Scenario Thinking

A glimpse into the future of the cyber security landscape in Europe

How the cyber security landscape will develop in the future is one of the most uncertain questions we face today. Exponential technological developments, changing regulations, and dynamic political environments lead to constant changes in the field of cyber security. New players enter the cyber security field, and the role of cyber security in political and military spheres is shifting. These are just some of the many powerful forces reshaping the cyber security landscape.

Decisions taken by different stakeholders in this uncertain environment will determine the future of public and private sectors, as well as that of civil society and citizens of states. Decision-makers today thus have the potential to set the scene for the future cyber security landscape.

Undeniably, capturing such complexity is difficult – especially if one resorts to conventional policy or strategy analysis. While it is impossible to predict the future, scenario analysis can cut through the complexity by telling plausible stories of the future, highlighting the risks and opportunities. Scenarios are narratives of alternative futures that serve as a foundation for strategic decision-making by private, public, or civil society stakeholders engaged in cyber security issues. It gives these decision-makers a chance to develop robust yet flexible strategies for potential future scenarios.

The cyber security landscape is undergoing rapid and accelerating changes. We have captured this in two distinct parts of this study. While the first part of the European Cyber Defense 2018 looked at the status quo of national cyber security strategies, this second part of the study focuses on the future: What will the cyber security landscape in Europe look like in 2030? What risks and opportunities result from it? To answer these questions, we have developed four possible scenarios.

In the **Golden Cage** scenario, the cyber security landscape in Europe is highly stable and secure. Threats are known and there is little disruption. Despite sharing the high costs of security, the industry is healthy. However, there is very little innovation, and a high vulnerability to unforeseen threats. Non-state actors outside the functioning order threaten cyber security. 'Golden Walls' have arisen around protected regions, such as the EU, and protectionism reigns. Society has become complacent, but threats are lurking in the shadows.

The **Protect Yourself** scenario describes a deeply insecure and technologically fragmented world characterized by a culture of mistrust and a high level of bureaucracy. The privatization of security and cyber self-regulation has generated small thematic islands of security. Innovative pressure to counteract the lack of effectiveness in cyber security is high, and diplomatic negotiations have increased significantly. However, new rules and regulations are not enforced, and cyber mercenaries are often the only protection against frequent cyber attacks.

In another scenario world, **Cyber Darwinism** has taken over. A laissez-faire Europe has become a digital jungle in which non-state or quasi-state actors have risen, and cyber federalism is the norm. While small heavily protected islands of (cyber) security exist, the outside world is highly insecure. The subsequent rise of two-class security has led to a high level of social injustice. Cyber security has become a clear competitive advantage iand business is migrating to areas with clear cyber regulation. Individualization has led to the end of globalization. Although multilateral and bilateral alliances continue, there is a high degree of rearmament. All in all, Europe consists of failed cyber states.

In the **Cyber Oligarchy** scenario, a small cyber elite controls cyber security. The highly innovative free market profits from little state influence and control. However, automation has caused high unemployment, while increases in cyber attacks and counterattacks have led to a high risk of (cyber) conflict. There is a strong need for deterrents, resulting in a Cyber Arms Race and many small hot wars. There is a large potential for new concepts of state, and the private sector takes an active interest in building a functioning state.

The cyber security landscape of today is changing rapidly and significantly. These four scenarios demonstrate how different the future could be. Each one has its own opportunities and risks – let´s see what they would mean for all of us.

Enjoy the ride

center
for the long view

Critical Uncertainties

Drivers shaping the future of the cyber security landscape

As part of the scenario analysis, we have developed a comprehensive list of political, military, technological, social, economic, and environmental drivers that have the potential to influence the cyber security landscape in Europe. This list is based on extensive research using natural language processing AI, expert interviews, and traditional research. A diverse expert panel from the public and private sectors and civil society then rated these drivers according to their impact on the cyber security landscape in Europe in 2030 and the uncertainty of their development. Following this, the most impactful and uncertain drivers were grouped into critical uncertainty clusters. Critical uncertainties are overarching key themes that have the potential to tip the development of the cyber security landscape in Europe in one direction or another.

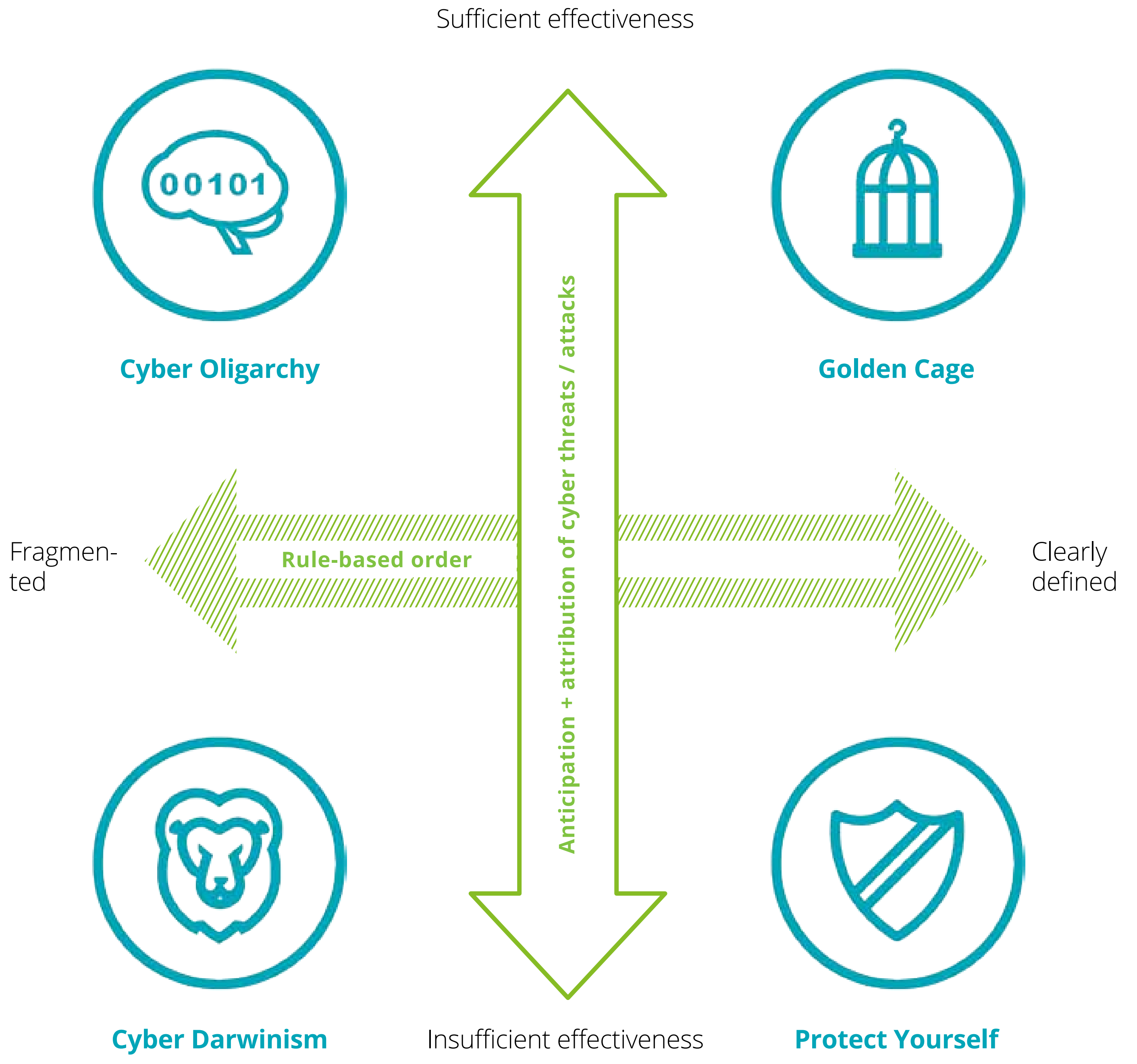
Our expert panel identified two critical uncertainties as key determinants of the future of cyber security in Europe. First, the existence and degree of a rule-based order. This delineates an order that is based on legal frameworks and standards at the local, national or international level, or any combination of these. Second, the possibility to anticipate cyber threats and attribute cyber attacks. Anticipating cyber threats involves the identification of and preparation for cyber attacks within the known range of attack mechanisms and methods. Attributing cyber attacks refers to the process of ascribing crimes to perpetrators by successfully tracking, identifying, and prosecuting cyber criminals.

The rule-based order can become either clearly defined and operational, or fragmented and based on the rule of the strongest. In the case of the former, Europe is characterized by the existence of operationally driven rules and regulations on cyber-related issues, bilateral and multilateral cooperation, and general human interaction in cyber space. By contrast, in the latter it is defined by a lack of generally accepted and enforced regulations, with cyber security being driven and controlled by a powerful minority. The underlying drivers of this critical uncertainty include international cyber cooperation, international unilateral cyber regulation, data protection and privacy regulation, the importance of the EU in cyber security, and the relationship between the EU and other players such as NATO, the UN, and individual states like Russia, China, or North Korea.

Anticipating cyber threats and attributing cyber attacks can be either sufficiently or insufficiently effective in future. On the one hand, this critical uncertainty could take the form of prevention, early detection, and resolution of cyber threats, with authorities being able to attribute attacks and efficiently persecute perpetrators. On the other, it could be characterized by high (cyber) insecurity due to inability to prevent or follow up on cyber threats. Drivers underlying these developments include the development of computing power, quantum computing, the level of cyber risk, the efficiency and accuracy of attribution, the effectiveness of law enforcement in countering cybercrime and ICT terrorism, threat intelligence, and malware and ransomware attacks.

The combination of both critical uncertainties leads to four visions of the future, illustrated in figure 1. All four of the resulting scenarios adhere to five criteria: They must be plausible, relevant, divergent, challenging, and balanced. Each of these four scenarios thus signifies a different story of the future, four alternative worlds that could exist in 2030.

Fig. 1 – Scenario matrix describing the future of the cyber security landscape in Europe



Four Possible Scenarios for the Future

The cyber security landscape in Europe in 2030

Golden Cage

Clearly defined and operational rule-based order and sufficient effectiveness of the possibility to anticipate cyber threats and attribute cyber attacks

In this scenario, Europe is highly secure and stable and faces very little disruption. Cyber threat levels are known, and security organizations report honestly on current threats and developments. While a strong cyber surveillance culture exists to ensure high levels of security, this is regulated clearly and transparently. Strong innovation in the early 2020s has led to a state of technological readiness for facing cyber threats. Frequent training and testing of cyber capabilities ensures constant vigilance regarding cyber threats. This is supplemented by civilian cyber drills, for example in schools and private firms. A Golden Wall has been erected around Europe, and protectionism defines European politics.

However, following the initial innovative push, now, in 2030, there is very little room for innovation, and the little innovative potential that remains is limited to the engineering sector. While the private sector is healthy, it shares in the heavy costs of the cyber security system. Society has become complacent and reliant on existing solutions. While states are on high alert and in a state of readiness when opponents and threats are present, they become drowsy when this is not the case. Consequently, while Europe is ready for known threats, it is highly vulnerable to unforeseen developments. Non-state actors operating outside of the existing order thus constitute the biggest threat to the European cyber security landscape.

Protect Yourself

Clearly defined and operational rule-based order and insufficient effectiveness in anticipating cyber threats and attributing cyber attacks

In this world, Europe is highly bureaucratic, extremely insecure, and technologically fragmented. While there are small thematic islands of security, for example around connected health care, cyber security outside these areas is lacking. As the public sector has failed to provide effective cyber security, security has been privatized, and cyber self-regulation and the use of cyber mercenaries is the norm. This has led to a new cyber security economy and competition between private and public security providers. The public sector is fighting hard to gain the respect of security spheres. There are extensive cyber reconnaissance troops and cyber task forces. However, increasing threat levels have led to the necessity of private-public partnerships. The resulting corset of security is suffocating society, and a culture of mistrust has taken over.

To counteract the lack of effectiveness in cyber security, there is huge innovative pressure in Europe, with both public and private sectors driving technological developments. The innovative potential lies in the private sector, but there is a focus on national cyber security innovation. Where necessary, states nationalize private firms in their search for efficient cyber protection. Economies of scale rule in this environment, and small and medium enterprises are suffering.

To keep up and increase the rule-based order, there has been a stark increase in negotiations and diplomacy. Cooperation and regulation has mushroomed on bilateral and multilateral levels, and new alliances continue to be formed. However, there is a lack of efficiency in enforcing these clearly defined and operational rules.

The cyber security landscape in 2030

Cyber Darwinism

Fragmented rule-based order driven by a rule of the strongest and insufficient effectiveness in anticipating cyber threats and attributing cyber attacks

In this alternative future, Europe has become a jungle that operates on a laissez-faire mentality. While small islands with a high level of (cyber) security exist within gated communities, the outside world is highly insecure. This has resulted in a two-class security system, which heavily discriminates against and excludes low security classes. A flood of highly inefficient cyber regulation on a regional, or at most national, level has led to Cyber Federalism: To compensate for the lack of effective national and international regulation, federal states and sub-regions have made their own cyber policies. The resulting regulatory chaos and existence of security hubs has given rise to regional cyber security havens, which profit from their security status and enjoy a high standard of living. Cyber warlords rule over individual territories, and non-state and quasi-state actors have gained power. Globalization has ended and individualization has taken over.

Cyber security has become a clear competitive advantage. Industries migrate to areas with high cyber regulation clarity, such as China. Alliances continue alongside existing bilateral and multilateral lines, but the lack of international regulation has resulted in the heavy rearmament of individual states and sub-regions. Overall, Europe consists of failed cyber states, ruled by the principle of the survival of the fittest.

Cyber Oligarchy

Fragmented rule-based order driven by a rule of the strongest and sufficient effectiveness in anticipating cyber threats and attributing cyber attacks

IIn this scenario, a small elite of cyber experts rules the cyber security landscape in Europe. The state is no longer in the driving seat of cyber security. Instead, there is private enforcement of cyber security according to the 'laws of the jungle'. Consequently, there is a high potential for new concepts of state, and the private sector takes an active interest in the presence of a functioning cyber security state, contributing both finances and knowledge to the public sector to (re)establish order. In this fragmented order ruled by the strongest, there is a strong need for deterrence, including nuclear. As a result, a Cyber Arms Race has ensued and tensions have been vented in many small hot conflicts. There has been an increase in cyber attacks, and the risk of (cyber) conflict, including the use of Internet Weapons of Mass Destruction (IWMDs), is high.

The lack of state influence and control has resulted in ample opportunities for the private sector. The free market profits from the large amount of room for innovation and creativity. Start-ups have thrived and generally aim not for independence, but hope to merge into one of the tech giants. Strong alliances have also formed between traditional industries, such as the automotive industry, and tech giants, with leading traditional firms operating underneath the umbrella of innovative tech empires. However, automation has caused high unemployment and social protests are frequent. Traditional bilateral and multilateral alliances remain and there is a high degree of clarity of players in the cyber security sphere.

Conclusions and outlook

The future of the cyber security landscape in Europe will have far-reaching implications for the private and public sectors and civil society

Contemplating these four scenarios, the most striking point is perhaps their timeframe. In the uniquely dynamic field of cyber security, thinking even a few years ahead often seems an unfathomable task, yet our scenarios give an outlook at what the cyber security landscape may look like beyond that, in 2030.

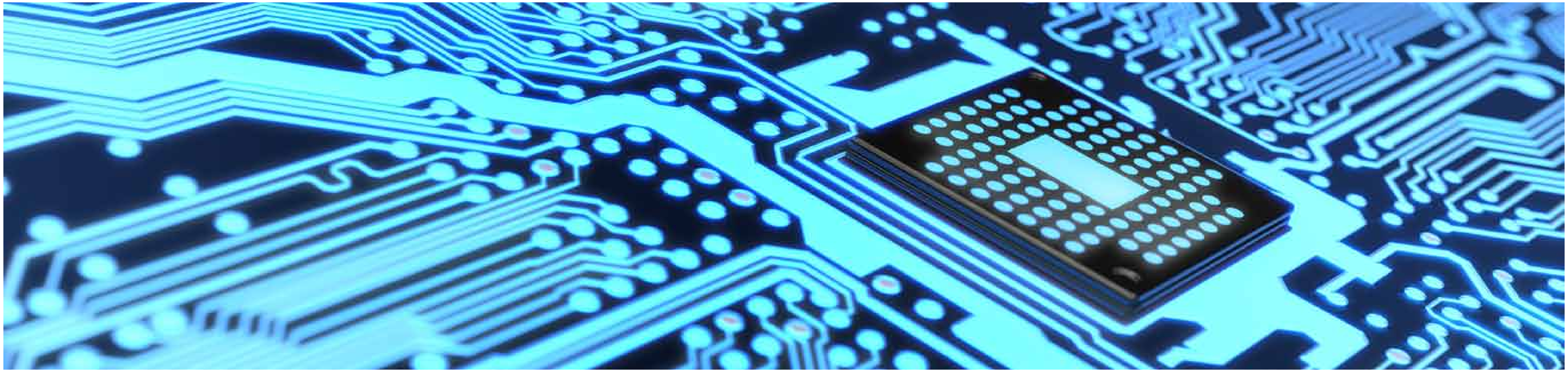
While the future of cyber security is extremely uncertain, it is highly necessary to consider its implications for the public and private sectors and civil society in Europe and beyond. Our four scenarios enable precisely that. We do not expect one scenario to happen completely and unequivocally as described here; rather, the future of the cyber security landscape will lie somewhere in between them. By thinking about and preparing for these four extreme scenarios, stakeholders can formulate robust but flexible strategies for any future in between these alternatives. Based on the insights into the status quo of national cyber security strategies in Europe, as outlined in the first part of the European Cyber Defence 2018, this is particularly crucial. With many cyber strategies dating back a number of years, and none looking forward into future threats, preparing for the future is particularly paramount.

While there are a myriad of common implications emerging from these scenarios, the biggest one is perhaps the overarching need for cooperation. Cooperation and coordination within and between states and regional and international organizations will be crucial. The private sector, including military and intelligence services, the public sector and civil society in each country will have to work together to prepare for future risks and make use of future opportunities. Equally, states will need to work in unison to drive cyber governance regionally and globally. Regional and international organizations and alliances, including in particular the EU, NATO and the UN, will have to cooperate with states and each other to enable cyber security on any level.

Many other general implications emerge across all four scenarios. The need for digital education and training, the necessity of engaging with questions around shifts toward hybrid or cyber warfare, including the potential offensive use of cyber weapons by states, and the need to protect critical infrastructure are just a few examples here. At the same time, each scenario brings with it a number of specific implications, both in terms of risks and opportunities.

Developing specific strategies for each of the four scenarios will enable decision-makers to respond flexibly to the dynamic cyber security environment within and outside Europe. By doing so, decision-makers can proactively drive transformation in the cyber security landscape and prepare for the risks that linger in the shadows along the way. As such, these stories of the future aim to stretch minds, challenge perceptions, and capture complexities that would otherwise be lost.

The four scenarios may be radically different, but they share one common theme: Foresight, vision, and close cooperation between decision-makers in the private and public sectors and civil society will be required to successfully navigate the ever-changing map of the cyber security landscape in Europe. Scenario analysis can serve as the compass to do so – and let you lead the way.



Methodology

A short introduction to scenario design and its methodology

This study on the future of the cyber security landscape in Europe is based on the seven-step scenario design methodology by the Center for the Long View (CLV), which applies the guiding scientific principles of objectivity, reliability, and validity. This study is the outcome of comprehensive research, expert interviews, and a scenario workshop involving selected political, military, economic, and social cyber security experts from the private and public sectors and civil society, as well as the Deloitte network and experienced scenario practitioners from the CLV.

Our scenario design methodology starts with the formulation of a focal question in order to determine the project's scope and strategic direction. The focal question for this study was the following: What will the cyber security landscape in Europe look like in 2030?

As scenarios are a way of understanding the dynamics that shape the future, the second step of our methodological approach is the identification of driving forces that have the potential to impact the outcome of the focal question. These drivers can be grouped into five categories, known as STEEP forces, which consist of social, technological, economic, environmental, and political factors.

In order to determine this study's long list of drivers, we primarily made use of interviews with selected Deloitte experts and our AI-based research tool, CLV Deep View. Deep View uses proprietary natural language processing algorithms to read millions of data sets with the aim of identifying patterns between key words, phrases, people, companies, or institutions. This allows us to gain a holistic understanding of highly complex issues and interrelationships, as well as to identify global trends. It also helps to avoid the bias of traditional approaches that often have a built-in tendency based on the character, mood, or personal preference of the scenario analysts.

In a third step, we prioritize and cluster the identified drivers into critical uncertainties. This is necessary as not all driving forces are uncertain. Some may be predictable and unlikely to vary significantly in the different scenarios. Thus, critical uncertainties must fulfill two criteria: Firstly, they must have a high impact on the outcome of the focal question. Secondly, they must be highly uncertain or volatile. Initially, all uncertainties appear unique, however, by analyzing the comprehensiveness and correlation of each critical uncertainty we can establish the building blocks for our scenario framework.

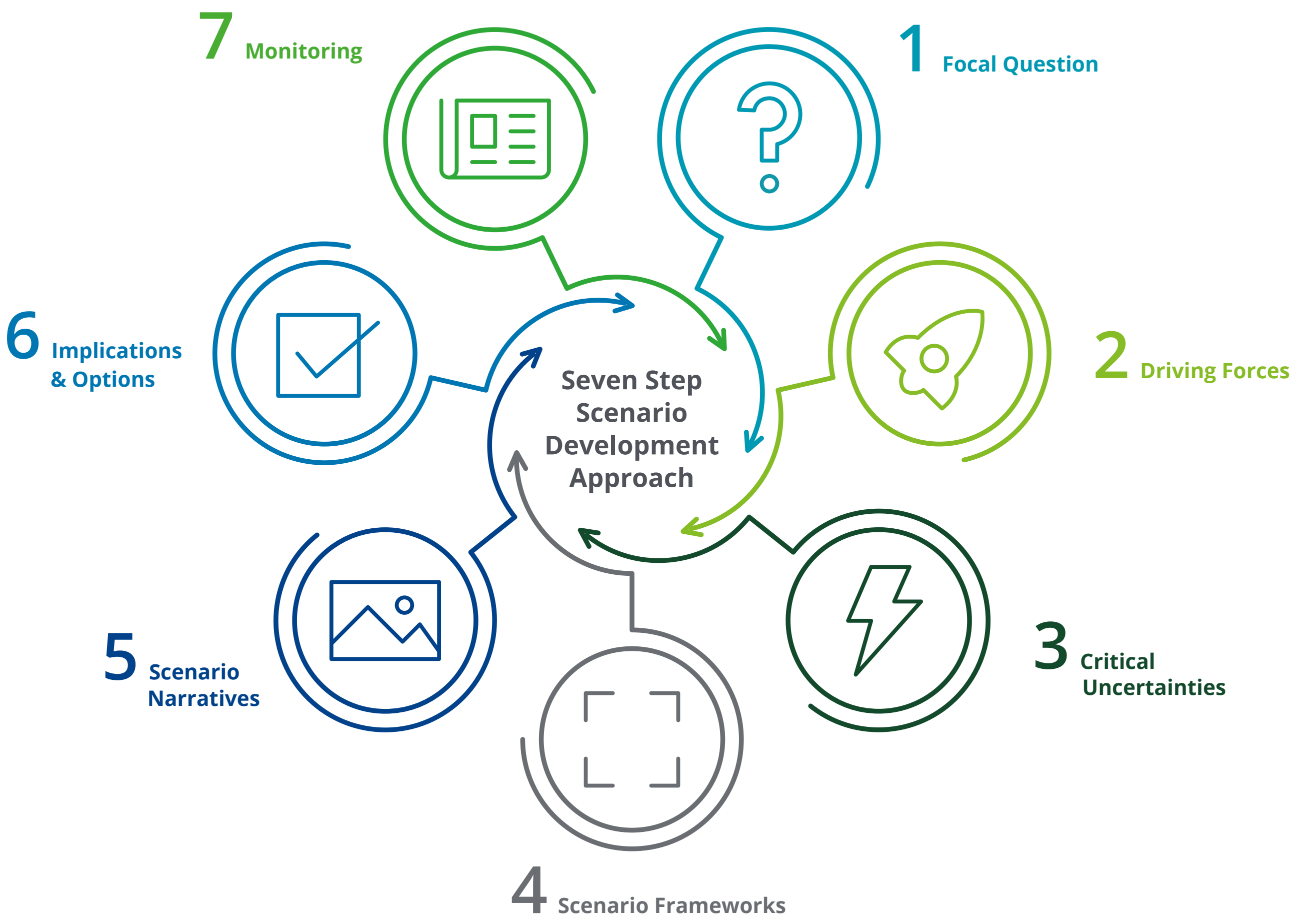
The scenario framework is developed in the fourth step of our scenario design approach. The critical uncertainties determined serve as the two axes that are combined into a matrix, resulting in four highly divergent but plausible scenarios. In our study, the two critical uncertainties are the nature of the rule-based order and the possibility to anticipate cyber threats and attribute cyber-attacks.

Having established the scenario matrix, we then develop the four scenario narratives in a fifth step. Scenario narratives define the framework conditions and atmosphere of each scenario within the context of a story. By using the previously identified drivers to reverse-engineer the milestones that would lead to each future, we can determine the key elements for each scenario.

Then, in a sixth step, we make use of these scenario narratives to derive resulting implications for the stakeholders involved, such as the private and public sectors and civil society.

In a seventh and final step, we define key indicators for each of the four scenarios to enable the monitoring of trend developments. The aim of this step is to observe which scenario is most likely to materialize at any given moment, and identify shifts from one scenario to another one.

Fig.2 – Seven step scenario development approach



Contacts

Katrin Rohmann
Public Sector Leader
Deloitte Risk Advisory
Tel: +49 (0)30 25468 127
krohmann@deloitte.de

Dr. Florian Klein
Head of the Center for The Long View
Monitor Deloitte
Tel: +49 (0)69 9713 7386
fklein@deloitte.de

Annina Lux
Center for the Long View
Deloitte Risk Advisory
Tel: +49 (0)30 25468 5131
anlux@deloitte.de

Special thanks to Knut Schönfelder and André Roosen for their contribution.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/de/UeberUns for a more detailed description of DTTL and its member firms.

Deloitte provides audit, risk advisory, tax, financial advisory and consulting services to public and private clients spanning multiple industries; legal advisory services in Germany are provided by Deloitte Legal. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 244,000 professionals are committed to making an impact that matters.

This communication contains general information only not suitable for addressing the particular circumstances of any individual case and is not intended to be used as a basis for commercial decisions or decisions of any other kind. None of Deloitte Consulting GmbH or Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

IIssue 11/2018