Monitor **Deloitte.**

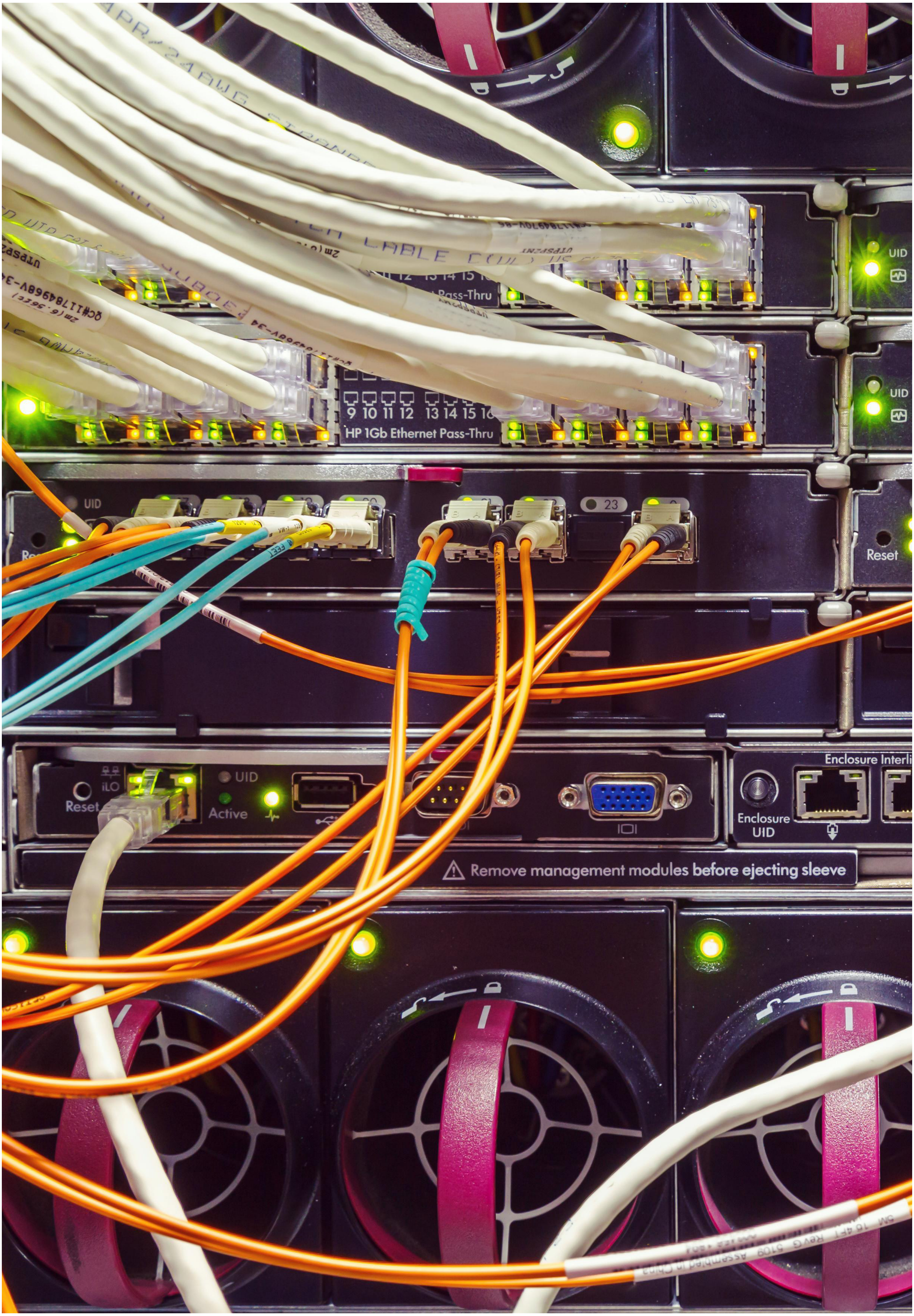
Glimpse into the future

Digital Conflicts in Geopolitics 2035

center
for the long view

Peace cannot be kept by force; it can only be achieved by understanding.

Albert Einstein


HP 1Gb Ethernet Pass-Thru
Pass-Thru
9 10 11 12 13 14 15 16
UID
Reset
23
iLO
Active
Enclosure Interli
Enclosure UID
Remove management modules before ejecting sleeve
CABLE
Assembled in China

Scenario Thinking

A glimpse into the future of digital conflicts in geopolitics

Geopolitical conflict is as old as humanity. It has been widely debated by academics, politicians and economists. However, in our rapidly transforming world, traditional debates can no longer adequately capture the complexities of geopolitical conflict in the digital sphere.

What could future digital conflicts in geopolitics look like in 2035? What role could the European Union (EU), China and non-governmental actors have in solving them? The answers to these questions depend on the many uncertainties that accompany the extension of classic geopolitical conflicts into the digital realm. How the private and public sectors, as well as civil society, in China and the EU respond to these complex questions will be vital in the future.

Scenario analysis can capture such complexities more effectively than traditional analytical methodologies. While it is impossible to predict the future, scenario planning can help to tell stories of the future, cutting through complexity and flagging opportunities and risks. This allows decision makers to develop robust, yet flexible strategies for the future.

Combining the scenario expertise of Deloitte's Centre for the Long View (CLV) with the academic expertise of the German Institute for International and Security Affairs (SWP) and the European University Viadrina, we developed four possible scenarios for the future of digital geopolitical conflict. While this glimpse will focus on the question of what digital conflict might look like, further publications by the SWP, in cooperation with the CLV, will take a closer look at the implications of these scenarios and potential solutions. The four scenarios demonstrate how different the future could be:

In the **Sophie's World** scenario, integrated social and technological systems have led to strong Sino-European political and economic cooperation. The risk of conflict has decreased significantly, and technological developments and mutual understanding have fostered a high level of resilience in both China and Europe.

The scenario **Collapse of the Digital Global Commons** describes a world of instability and danger. The integration of Chinese and European social and technological systems has led to an uncontrolled playing field for cybercriminals and terrorists, making digital ecosystems highly vulnerable. Both China and Europe respond with inward-looking governance, focusing on their own narrow interests instead of working together.

In **Cold War 4.0**, digital feudalism and protectionism have fostered highly polarized governance systems with digital Darwinism characterized by a 'me first' attitude in both China and Europe. Both operate in their own digital sphere and economic markets are isolated. Although diplomatic ties are still strong, other communication and exchange is almost non-existent because of frequent cyberwars and massive cyberattacks.

Unsplendid Digital Isolation describes a world of a Sino-European stalemate characterized by border walls, protectionism and isolationism. China and Europe have become highly resilient digital islands with no exchange between the two. Politically, dictatorships are on the rise, and technology is exploited to further narrow local interests only.

Before we travel into these four different future worlds we will examine the 'critical uncertainties' or factors that might influence them. Digital conflicts in geopolitics are characterized by rapid and significant change. Let´s journey into four different future worlds in 2035 and see what they would mean for us.

Enjoy the ride!

Your

center
for the long view

Critical Uncertainties

Drivers that will shape future digital conflicts in geopolitics

In today's complex world many forces have the potential to affect the development of digital geopolitical conflicts. 'Drivers' are what we call the factors that may influence the future. To identify and prioritize the large number of potential drivers, we used a combination of AI-based natural language processing algorithms, traditional research and expert interviews. The drivers range across all seven of the STEMPLE categories (social, technological, economic, military, political/legal and environmental factors) ensuring a holistic outlook on current and future complexities.

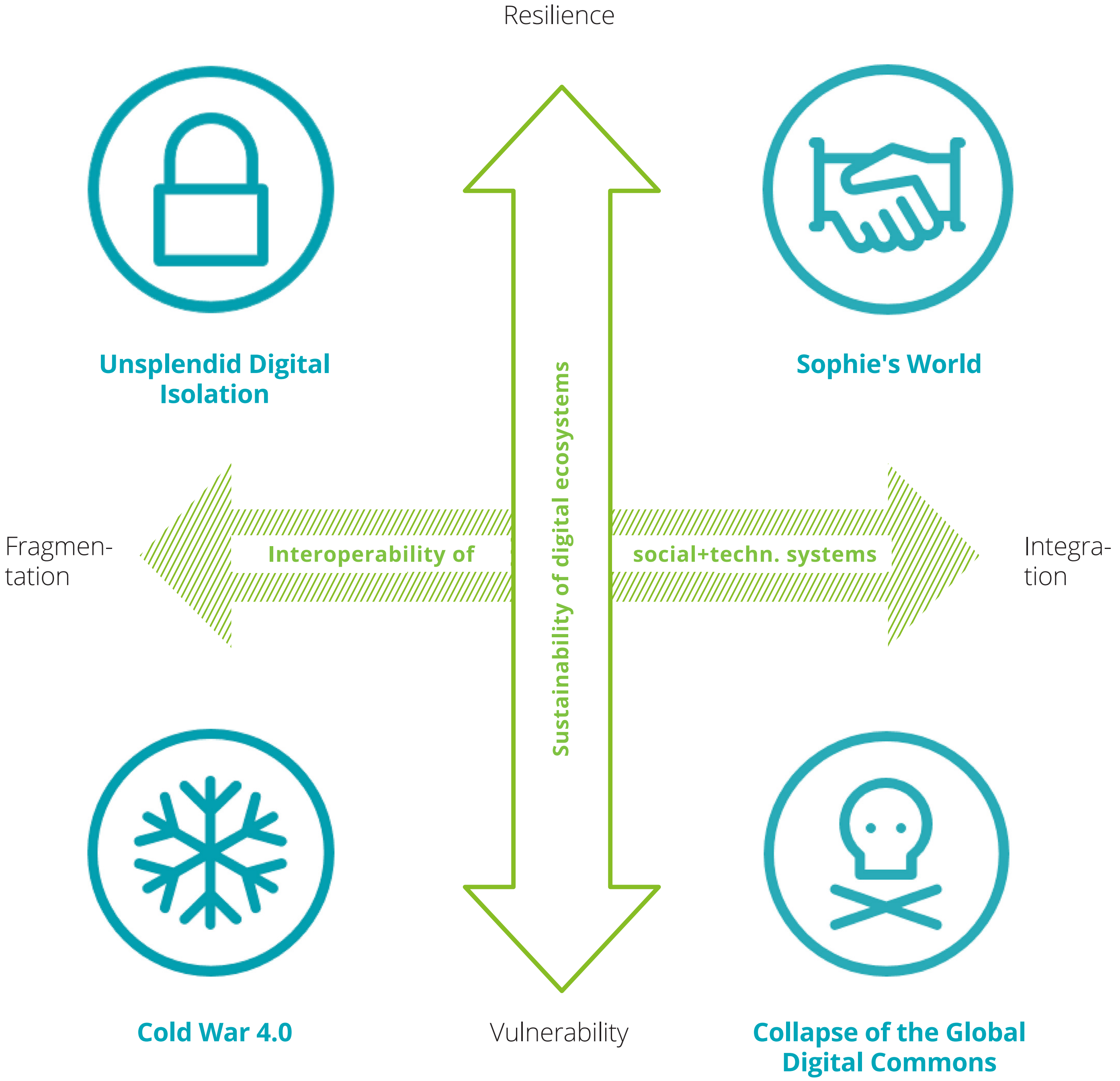
To build the basis for the scenario framework, an expert panel rated the drivers according to their potential impact and their uncertainty. Subsequently, the focus was put on the most impactful and most uncertain drivers, which were grouped into a series of 'critical uncertainties'. Critical uncertainties are clusters of interrelated drivers that capture decisive questions on future developments. In this process, our expert panel defined five critical uncertainties. After correlation testing, two out of these five critical uncertainties were identified as the axes pairs for our scenario matrix, forming four plausible but challenging scenario worlds.

The first critical uncertainty selected is the interoperability of Chinese and European social and technological systems. This delineates the compatibility of and relationship between social and technological standards in China and the EU. Chinese and European social and technological systems can either be integrated or fragmented. Integration means that the flow of people, information, capital, goods and services is encouraged and facilitated, and that societies can use a common market for social, political and economic exchange. Fragmentation means that the possibilities for social and technological cooperation and exchange between the EU and China are greatly reduced, and physical or digital transfers face severe barriers. The main drivers underlying this critical uncertainty range across all seven STEMPLE categories: Digital Divide, Artificial Intelligence, Skill gap in China and the EU, Interoperability of technological ecosystems, Data Protection and Privacy Regulations, Technology gap between the EU and China, and Industry 4.0.

The second axis is formed by the critical uncertainty ´sustainability of digital ecosystems´. This means the capability of long-term, development, production and maintenance of networks of digital platforms and related digital products. Digital ecosystems can either be resilient or vulnerable. Resilience is characterized by highly secure digital networks and products and the ability to effectively prevent, respond and react to cyber attacks. Vulnerability describes highly insecure digital networks or products and the inability to effectively prevent, respond and react to cyber attacks. Five major drivers shape this critical uncertainty: the cybersecurity of critical infrastructure, the level of cyber resilience, the attribution of cyber attacks, international cyber cooperation and the role of third party states in cybersecurity.

As a result, the four plausible but highly challenging visions of the future, illustrated on the right, were derived. These alternative futures give four answers to our focal question: What could digital conflicts in geopolitics look like in 2035?

Fig. 1 – Scenario matrix : The future of digital conflicts in geopolitics 2035



Four Possible Scenarios

The future of digital conflicts in geopolitics

Scenario 1: Sophie's World

Integration of Chinese and European social and technological systems and resilience of digital ecosystems

In this scenario, China and Europe cooperate in a peaceful world. The integration of Chinese and European social and technological systems has fostered a strong relationship and fruitful exchange. This has significantly reduced the risk of conflict and strengthened political, social and economic ties. In the competition-based economic system, both players were able to grow their capabilities within a defined set of standards. While there are no tensions on the use of these capabilities, the question of who controls these standards is contested. The Chinese and the European states have a strong hand in setting standards, but social and technological interconnectivity ensures close cooperation. A Sino-European Cybersecurity Council has been established to counter the existing cyber crime and cyber terrorism threats. However, despite these positive developments, tensions between China and Europe on the control of standards have the potential to grow and threaten relations between the two players.
Economic competition has led to permanent learning in both China and Europe. One result of this is a very high level of resilience of digital ecosystems. Both players are highly adaptable and able to cope with change well. Technology is generally employed for the common good, for example to increase social cohesion and is open to all. While there is agreement on social values between China and Europe, the instruments by which these values are promoted and enforced are contested.

Scenario 2: Collapse of the digital global commons

Integration of Chinese and European social and technological systems and vulnerability of digital ecosystems

In this alternative future, China and Europe find themselves in an unstable situation. Although diplomatic ties between both players are still intact, the strenuous balance of today´s Chinese-European relationship has been cemented over the years. The world is a dangerous place – despite the successes of integrating Sino-European social and technological systems, the open-border digital sphere has also given free reign to cyber criminals. The threat of non-state actors in this sphere is significant in both China and Europe.

This has led to a high vulnerability of digital ecosystems. Citizens' security and livelihoods thus depend on the states' success in protecting and growing the digitalized economic and social spheres. To do so innovation is needed, but access to technological developments is limited to the economically powerful and often used for narrow interests. Instability and the high level of cyber threat have led to low economic growth. Access to the open market is key for social and economic wellbeing. While big international companies can leverage the open digital playing field and profit despite the cost-intensity of the economy, all others fight for survival and employees are exploited for economic profit. While states have lost power, these big private players have gained influence.

Global governance thus remains a challenge – despite the high interoperability, individual territory-based governance systems have persisted. Although the interoperability of technological systems allows a Chinese-European exchange on different levels, social and cultural ideas have remained largely segregated.

Scenario 3: Cold War 4.0

Fragmentation of Chinese and European social and technological systems and vulnerability of digital ecosystems

In the Cold War 4.0 scenario, China and Europe operate in a highly polarized system governed by the survival of the fittest. Cyber war is frequent, and states govern with a 'me first' attitude. Digital feudalism and protectionism have carved the world into different socially and technologically fragmented spheres, all of which adhere to their own, oppositional social and political values. Ideologies and religion have flourished in this environment. With no direct border between China and Europe, divisions have manifested themselves in proxy wars across Asia and Africa. In and beyond these – partially hot- wars, technology is employed by states to further their own interests. Isolationism is also a feature of the economic markets. Separate blocks of digital economies have emerged, tightly controlled by states. Europe has lost the technology race, making it digitally vulnerable. However, with exponential technological developments and warlords and other non-state actors leading constant digital skirmishes, China also finds itself in a situation of high vulnerability. Massive cyber attacks have hit both players since the early 2020s.

This has led to the maintenance of communication and the establishment of a multilateral digital alliance between power players, including China and Europe. Despite the dire state of the world, the existence of such diplomatic ties holds promise, and stability could be reached through diplomatic means.

Scenario 4: Unsplendid digital isolation.

Fragmentation of Chinese and European social and technological systems and resilience of digital ecosystems

In this world, China and Europe find themselves in a stalemate rather than in sustainable stability. The world is characterized by border walls; protectionism and isolationism rule. Fueled by the fragmentation of social and technological systems, China and Europe have become strictly governed, highly resilient digital islands. Any exchange, whether digitally or in the analogue world, is almost impossible. Aggression dominates the tone on both sides as they stand on the verge of conflict.

Both China and Europe have cemented preconditions for dictatorships in the late 2020s, following an intense cyber war with disastrous consequences for both governments and civilians. The world has become highly polarized. This has resulted in the end of internet as we know it, and its substitution with heavily protected individual cyber spheres. Technology is widely used for narrow interests by both state and non-state actors. Governments actively control the information flow within their realms according to their clashing social and political values. Resilience has become a major government concern. To ensure this, China and Europe adhere to their own governance system, with no convergence on a uni- or multilateral level. Imperialism has returned, and both China and Europe compete to expand their influence and widen their respective islands, particularly in Africa and Asia.

The danger of instability is always lingering over both players´ heads, but there is also potential for growth; massive cyberattacks on both China and Europe have led to the understanding that change is necessary.

Conclusions and Outlook

The future of digital conflicts in geopolitics will have wide-ranging implications for public and private actors and civil society in both China and the EU.

The four scenarios each describe radically different worlds.
Yet, all four of them make one thing blatantly obvious: a close cooperation between China and Europe will be needed to deal with the different challenges that lie ahead.

This cooperation will hinge not only on governmental activity, but also on private sector action and the involvement of civil society. Close diplomatic cooperation will be vital, but not in itself sufficient to prevent and solve future digital geopolitical conflict. Instead, relationships need to be built on the political, social and economic level. This should not be limited to high-ranking officials of the private and public sectors or civil society organizations, but should trickle down into wider society.

Equally, to build positive relations successfully, traditional means will not suffice. In a digitalized world communication channels must be adapted to the new digital reality. This means supplementing traditional means and points of interaction with new ones, for example by supplementing traditional forms of diplomacy with digital diplomacy.

Both China and the EU need to be willing to understand political, social and economic specificities of the other, and aim at fostering a meaningful exchange on all levels. The civil society can be a powerful player here.

Naturally, the implications of the four scenarios go well beyond this. Implications should be analyzed and strategies formulated for each scenario. Common core policies applying to all four scenarios need to be devised. This in itself will require the engagement of a diverse set of stakeholders. Our scenario design process involved an interdisciplinary panel of public, private and civil society experts from both China and Europe. A similarly diverse group needs to be included in the formulation of strategic options. This in itself is a first step towards the

crucial coordination that is a key strategic necessity of all four scenarios.

These scenarios show a glimpse into four worlds that will be challenging to navigate. Whether this is the positive „Sophie´s World" or the three darker scenarios "Collapse of the Digital Global Commons", "Unsplendid Digital Isolation" or "Cold War 4.0", each scenario has its own individual friction stakeholders need to face as the drivers underlying critical uncertainties evolve.

The complex interaction of the different critical uncertainties and underlying drivers that we defined could paint a myriad of alternative futures. By capturing uncertainty using scenario design, we can take a glimpse into four different possible stories of the future. Of course, we do not expect one of these to unfold exactly as described – the future may lie somewhere in between. However, journeying into these four extreme worlds will help stakeholders to define robust but flexible strategies that enable them to cope with the uncertainties of today and tomorrow.

This is not a one-time task. To ensure the validity of strategic options, current and future developments must be carefully monitored. Although this project focused on the development of the four scenarios, monitoring drivers and related indicators will be key to adapt to changing winds in the journey across the scenario worlds. Only this will enable stakeholders not only to react to change, but to drive it proactively towards a positive future.

Let's make our journey into the future a positive one.

Methodology

Introduction to scenario design and methodology

This study on the future of digital conflicts in geopolitics is based on the seven-step scenario-design methodology of the Center for the Long View (CLV). It is the outcome of comprehensive research, expert interviews, and a scenario workshop involving selected experts from the private and public sectors and civil society from China and Germany, as well as the Deloitte network and experienced scenario practitioners from the CLV.

For this project, we focused on steps one to five, outlined below. The sixth step, the consideration of implications and the formulation of strategic options, will be considered in more detail in additional publications of the SWP. However, for the sake of completion, all seven steps of the CLV scenario methodology will be explained below.

This process begins 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: What could digital conflicts in geopolitics look like in 2035? As a follow-on step, we then look at the implications of that question: What role could the EU, China and non-governmental actors have in solving them?

As scenarios are a way of understanding the dynamics that shape the future, the second step of our methodological approach is the identification of drivers. Drivers are those factors that have the potential to significantly impact the focal question at hand. These drivers can be grouped into seven categories, called the STEMPLE forces: social, technological, economic, military, political/legal, and environmental factors.

In order to determine this study's longlist of drivers, we conducted detailed analyses with 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 inherent bias of traditional research methods. This longlist of drivers is then consolidated into a shortlist. For this project, this shortlist contained 104 driving forces across all seven STEMPLE categories.

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 predetermined and unlikely to develop in different ways across 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. These critical uncertainties then serve as the building blocks for the scenario framework.

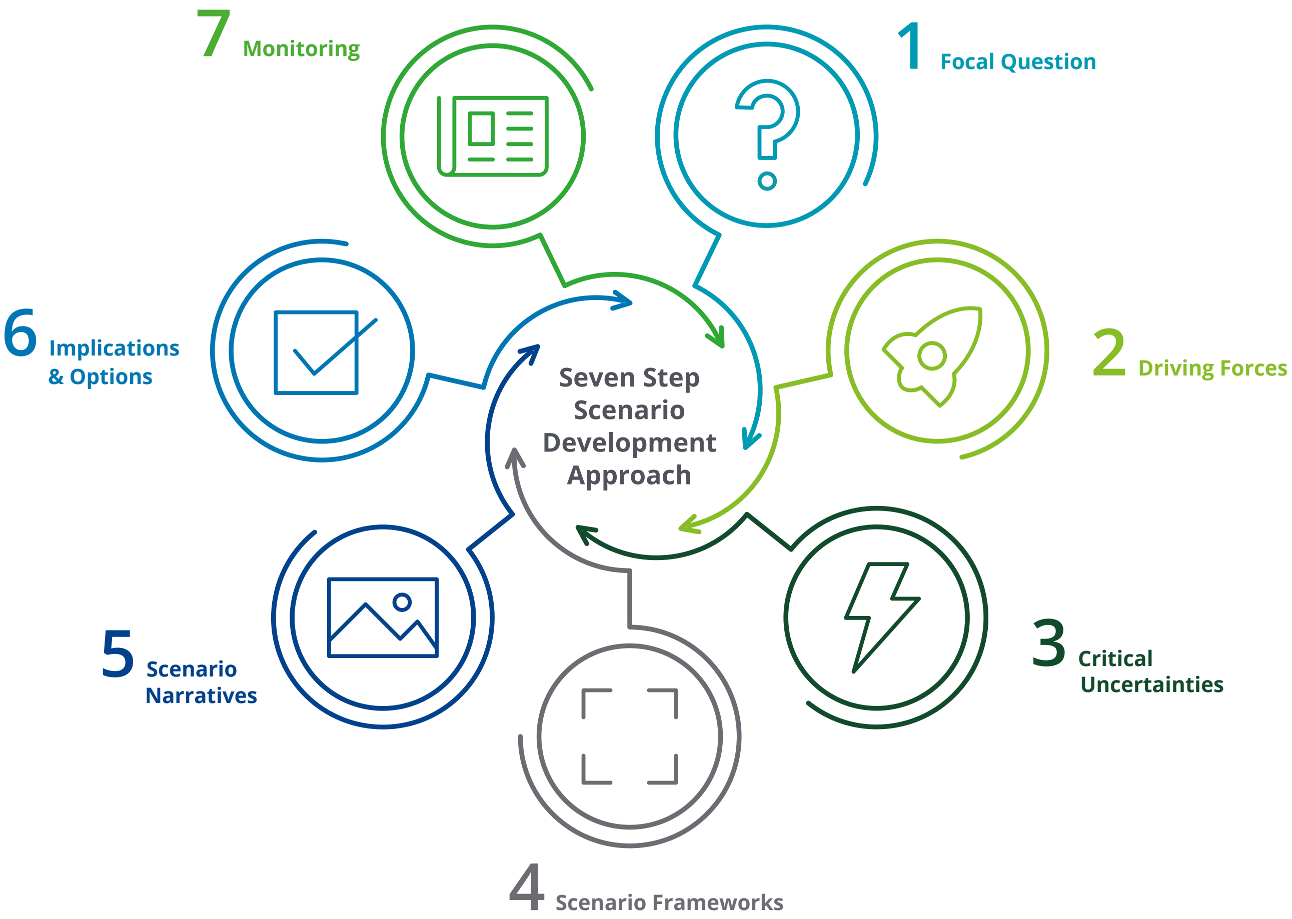
The scenario framework is developed in the fourth step of our scenario design approach. Following a correlation test, two critical uncertainties are selected by the expert group as the scenario matrix axes. The axes thereby form four highly divergent but plausible scenario worlds. In our study, these two critical uncertainties are 'the interoperability of Chinese and European social and technological systems' and 'the sustainability of digital ecosystems'.

Having established the scenario matrix, we then in a fifth step develop the four scenario narratives. 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 use these scenario narratives to consider the 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 relevant developments in order to establish which scenario the world is moving towards and to identify shifts from one scenario to another one.

Fig.2 – Seven step scenario approach of the CLV



Contacts

Florian Klein
Head of the Center for the Long View
Monitor Deloitte
Tel: +49 (0)69 97137 386
fklein@deloitte.de

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

With special thanks to Maximilian Lobbes for his contribution.

Monitor
Deloitte.

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.

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 approximately 286,000 professionals are committed to making an impact that matters.

Issue 03/2019