Global Governance Futures

ROBERT BOSCH FOUNDATION
MULTILATERAL DIALOGUES

Shared Responsibility: Towards More Inclusive Internet Governance

AASIM KHAN
JULIA POHLE
RUNHUI LIN
PARMINDER SANDHU
SETH OPPENHEIM
TAEJUN SHIN

MAY 2015

Supported by

Robert Bosch Stiftung

GGF Partners

GPPi GLOBAL PUBLIC POLICY INSTITUTE

The Tokyo Foundation 東京財団

BROOKINGS

Hertie School of Governance

Keio University

ashoka UNIVERSITY

WOODROW WILSON SCHOOL of Public & International Affairs

Acronyms

IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
iFTA	Internet Free Trade Agreement
IGF	Internet Governance Forum
IT	Information Technology
ITU	International Telecommunication Union

Cover photo: virtually light - hibernating

Table of Contents

About the Program

The Global Governance Futures program (GGF) brings together young professionals to look ahead 10 years and to recommend ways to address global challenges.

Building on the success of the first two rounds of the program (GGF 2020 and GGF 2022), GGF 2025 assembled 25 GGF fellows from Germany, China, Japan, India and the United States (five from each country). Over the course of 2014 and 2015, the fellows participated in four dialogue sessions: in Berlin (8-12 June 2014), Tokyo and Beijing (9-15 October 2014), New Delhi (18-22 January 2015) and Washington, DC (3-7 May 2015).

The GGF 2025 fellows – a diverse mix from the public, private and non-profit sectors, and selected from a highly competitive field of applicants – formed three working groups that focused on Internet governance, geoengineering governance and global arms control, respectively. Using instruments from the field of futures research, the working groups produced scenarios for their respective issue areas. These scenarios are potential histories, not predictions, of the future. Based on their findings, the fellows produced a range of publications – including this report – that present recommendations for steps to take on these issues towards a more desirable future.

The greatest asset of the program is the diversity of the fellows and the collective energy they develop when they discuss, debate and engage with each other during the four intense working sessions. This is why the fellows occupy the center stage of the program, setting GGF apart from many other young-leaders programs. The fellows play an active role in shaping the agenda of their working groups. The working process draws upon the GGF method and brings together the unique strengths, experiences and perspectives of each fellow in working towards a common goal. In addition, the fellows meet with leading policymakers and experts from each participating country. The GGF team works closely with the fellows to help them achieve their goals and, in the process, cultivates a community that will last well beyond the duration of the program, through a growing and active alumni network.

GGF is made possible by a broad array of dedicated supporters. The program was initiated by the Global Public Policy Institute (GPPi), along with the Robert Bosch Stiftung. The program consortium is composed of academic institutions, foundations and think tanks from across the five participating countries. The GGF partners are GPPi, the Hertie School of Governance, Tsinghua University, Fudan University, Ashoka University, the Centre for Policy Research, the Tokyo Foundation, Keio University, the Woodrow Wilson School of Public and International Affairs, and the Brookings Institution. The core responsibility for the design and implementation of the program lies with the GGF program team at GPPi. In addition, GGF relies on the advice and guidance of the GGF steering committee, made up of senior policymakers and academics. The program is generously supported by the Robert Bosch Stiftung.

The fellows of the Internet governance working group would like to thank the organizers of GGF 2025, the Robert Bosch Stiftung and everyone else who contributed to making the program possible – especially Thorsten Benner, Michelle Chang, Mirko Hohmann, Johannes Gabriel and Joel Sandhu. We are also grateful to Alex Fragstein for the design work, Oliver Read and Esther Yi for editing and colleagues at GPPi for commenting on this report.

Executive Summary

As a globally accessible information network, the Internet depends on key institutions and frameworks to manage the various technological, political, economic and social dimensions associated with its operation. With the aim of strengthening the Internet governance system, this report addresses the current difficulties associated with those institutions and frameworks by exploring two scenarios for how Internet governance might appear in 2025, a decade after the publication of this report. At one end of the analytical spectrum lies cooperation among stakeholders; at the other end, the collapse of the status quo. The report analyzes the opportunities and threats related to both scenarios in order to derive three major strategic policy implications to help shape the future of Internet governance.

The “Cyber Davos” scenario takes us to the year 2025, when policymakers from around the globe and CEOs of the world’s largest Internet companies gather for a meeting of the Xiamen Internet Forum, a new annual discussion venue on Internet governance, to celebrate the one-year anniversary of the Internet Free Trade Agreement (iFTA). This agreement traces its roots to 2015, when the United States gave up its role overseeing the Internet Corporation for Assigned Names and Numbers (ICANN). That event sparked a series of unexpected cross-border mergers and acquisitions between the US and China. Nearly a decade later, world leaders – drawing inspiration from the rapid liberalization of the global information and communications technology (ICT) sector and the exchange of human capital – signed the Internet Free Trade Agreement, despite opposition from civil society groups.

This picture of relative harmony stands in stark contrast to our second scenario, called “Google Shock,” in which trust in Internet companies collapses, resulting in significant economic damage to US and European information technology (IT) sectors. These events were triggered by the shocking revelation in 2015 that ties between American and European Internet companies and intelligence agencies were stronger than suspected. What followed was a substantial capital drain from American and European IT sectors, as well as the rise of Chinese Internet corporate giants. Meanwhile, deteriorating relations between NATO member states and Russia have led to a major conflict in cyberspace, causing loss of life and additional economic damage.

These scenarios present both threats and opportunities for policymakers. While “Cyber Davos” features a more secure and interdependent Internet governance system, the scenario also involves the threat of a governance system dominated by corporations, exacerbating economic and social inequalities globally. By contrast, the “Google Shock” scenario highlights the devastating consequences of growing insecurity in ICT systems and that insecurity’s devastating impact on economic growth. But the scenario also boasts a more balanced and equitable Internet economy, which comports with the realities of rising economies in the developing world.

Upon considering these two extreme scenarios, and the opportunities and threats that arise from them, we reach three major strategic policy recommendations. First, the global Internet corporate landscape should be diversified through increased competition and the facilitation of new business hubs. Additionally, we identify ways to engage with diverse voices on Internet governance issues and to enable the increased participation of the developing world. Finally, we emphasize that greater transparency and accountability could advance the credibility of existing institutional mechanisms, and we propose ways in which both multi-stakeholder and multilateral efforts could converge towards a more inclusive Internet governance ecosystem.

Disclaimer: The views expressed in this report do not necessarily represent the views of, and should not be attributed to, the authors' respective employers or any author in his or her individual capacity.

Introduction

The security and sustainability of the Internet are currently in jeopardy. The growing mistrust in Internet governance institutions, the undue strength of particular Internet companies, and disagreements on how to allocate web resources and maintain the security of the Internet's underlying architecture are all contributing to the fraying and fragmentation of the global network.

These tensions, however, are not new. Disagreements on the distribution and oversight of critical Internet resources, norms of behavior online and the rules of competition and commerce have been present since the Internet was first commercialized in the early 1990s. In the context of adopting Internet technical standards and assigning web addresses and numbers, the US liberalized that process in 1998 by creating the Internet Corporation for Assigned Names and Numbers. The debate about the internationalization of ICANN spilled out into the open at the World Summit on the Information Society, held in 2003 and 2005. Since then, global debates on Internet governance have been defined by tensions between two broad, competing visions of governance.

On the one hand, there is the classical intergovernmental approach, in which governments have the predominant, if not exclusive, right to policymaking, as is the case with decision-making in the United Nations. On the other hand, there is the multi-stakeholder model of governance, which challenges the exclusivity of governmental policymaking by favoring increased participation of the private sector and civil society.

Over the last two decades, governments and civil society groups have made a number of proposals to change the existing Internet governance regime. In most instances, these attempts have tried to shift Internet governance authority to a more centralized organization, or to create entirely new governance entities. Even an innovative forum like the NETmundial meeting, hosted by Brazil in April 2014, failed to address the fundamental dichotomy between a multi-stakeholder and an intergovernmental model of governance. The underlying tensions remain.

Our two scenarios seek to capture the causal links between the present and the future and to underscore the cost of inaction. Our first scenario, called "Cyber Davos," reveals a future in which Internet industry players gain even greater influence in Internet policy debates, leading to a new global consensus that is brokered by increasingly powerful corporations. In our alternate scenario, called "Google Shock," we present a darker vision of the future, in which state-to-state confrontations and falling revenues for major Internet firms bring the Internet system to the brink. For both scenarios, we identify respective opportunities and threats, and based on these, we develop strategic implications and recommendations for policymakers. The challenge for Internet governance lies in restoring the legitimacy of, and building trust in, the existing system and doing so in a manner that does not infringe upon the rights of the ordinary user.

List of Crucial Factors

CRUCIAL FACTORS	FACTOR OUTCOME IN THE "CYBER DAVOS" SCENARIO	FACTOR OUTCOME IN THE "GOOGLE SHOCK" SCENARIO
Major cyber confrontation	No cyber confrontation, but peaceful cooperation	A few countries involved in cyber attacks, resulting in economic damage and loss of life
China-US relationship	Improvement of relationship	High-level deterioration of relationship
Market-competitive structures	Consolidation of market structures	Diversification of market structures
US position on Internet Assigned Numbers Authority (IANA) transition	US support for the transfer of IANA function to the global stakeholder community	US opposition to the transfer of IANA function to the global stakeholder community
Cyber attack by non-state actor	No attack by non-state actors on critical infrastructures	Attack by a non-state actor, resulting in economic damage and/or minor loss of life
Google Shock (collapse of Internet giants)	No crash; IT market remains stable	Major Internet companies collapse, affecting the entire IT sector
Changing political alliances	Strengthening of current political alliances	Strengthening of current political alliances
Internet infrastructure	Agreement on preserving a single Internet infrastructure	Work on an expensive and exclusive network, independent from existing infrastructures
Influence of non-US Internet giants	US companies continue to dominate the global market	Non-US companies dominate the markets of their own or different regions
Internet vulnerability	Increase in network security	Increase in vulnerability of infrastructures, leading to partial Internet breakdown
Political power of corporations	A few Internet giants exercise extreme influence on all important Internet policies as a result of increased access to policymakers	Internet giants exercise little to no influence on Internet policies and processes
Domestic Internet policies of China, India, Brazil and European Union	Domestic policies are based on common principles and norms	Domestic policies are divergent and contradictory
Multiplication of Internet governance events, structures and groups	Agreement on and preservation of a single Internet ecosystem	Creation of an alternative to the Internet Governance Forum (IGF); separation of IANA functions from ICANN

Scenario 1: Cyber Davos

14 March 2025. The CEOs of the world's top Internet and technology companies have convened in Xiamen in China's Fujian province. The group is celebrating the anniversary of the Internet Free Trade Agreement, signed in 2024, a year after the creation of the Xiamen Internet Forum (popularly referred to as "Cyber Davos"). The Forum as well as the Internet Free Trade Agreement were made possible by the convergence of interests of world powers on global Internet governance issues.

The attendees of the Xiamen Internet Forum include the CEOs of major Internet companies, including Baigogo, a new joint venture that emerged out of Google's partial purchase of Baidu, the dominant Chinese search and advertising firm, a few years earlier. Also in attendance are the commerce and IT ministers of China, India, Russia, Brazil, Japan, the US and European countries, as well as representatives of various African and South American economies, all convening to celebrate the unprecedented integration of the world's leading Internet companies.

This private sector-led international effort goes back to 2015, when the US gave up its role overseeing the Internet Corporation for Assigned Names and Numbers, despite pervasive skepticism that this transition away from the US government would not occur by the September 2015 deadline. The event marked the start of a new era of cooperation between states, and of the reduction of tensions that emerged upon the 2013 Edward Snowden disclosures. Alibaba was the first major company to take advantage of the diffused tensions. Despite pundits predicting financial hardships due to political backlash, the Chinese Internet giant successfully purchased 34 percent of eBay's shares in 2017 to make inroads into the then-inaccessible US e-commerce market, which had been dominated by competitors such as eBay and Amazon. The stock prices of both Alibaba and eBay skyrocketed upon news of the transaction. Alibaba's newly expanded market access was followed by a number of mergers and acquisitions between US and Chinese Internet companies.

The purchase had the complementary effect of easing previously deep business tensions between American and Chinese firms. The successful alliance fueled a series of additional mergers and acquisitions across the globe – Tata Industries of India, for example, purchased a major share in DoCoMo of Japan. Furthermore, improved business prospects lured many companies into new business arrangements to access previously untapped African and South American markets – for instance, Deutsche Telekom took on major stakes in a variety of South American companies.

Meanwhile, Chinese firms, supported by their American investors, successfully lobbied the Chinese government to ease many of the "Great Firewall" restrictions. This, as well as the 2019 India-backed UN resolution establishing norms of cyber surveillance, helped alleviate civil society concerns regarding the use of data collection for national security purposes. Following two years of intense discussions, UN members began to align certain aspects of their domestic policies governing Internet issues – particularly on net neutrality, data encryption, privacy and network-security matters – with a view to signing a 2022 framework on global Internet governance. As part of this resolution, a UN committee tasked with governing cyber matters was created. Its mandate called for the official involvement of non-state technical advisors, including representatives of the International Telecommunication Union (ITU) and ICANN.

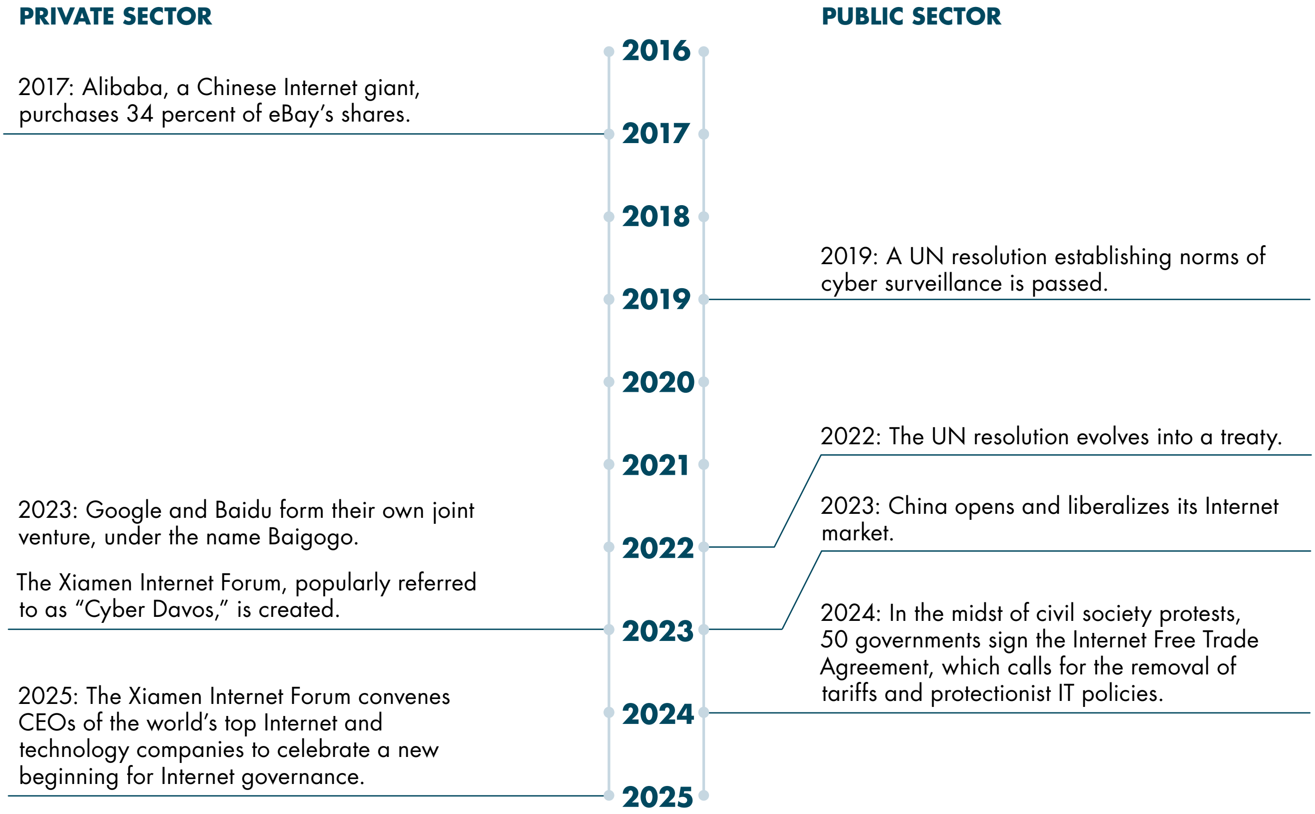
Taking a cue from the success of the Alibaba-eBay merger, as well as other global mergers, Google and Baidu agreed in 2023 to form their own joint venture, under the name Baigogo, to maintain their dominant positions in search, e-mail and messaging, and online advertising in a rapidly changing business environment. Such collaboration between Internet corporate giants in the US and in China turned out to be successful at fending off emerging competitors that were founded in the late 2010s. This led further to the opening and liberalizing of Chinese markets. In turn, Western countries opened up their markets to Chinese companies, such as Huawei and Tencent, which had previously been barred from the US partly for national security reasons.

Drawing inspiration from this rapid liberalization and the exchange of human capital, the US, Europe and the BRIC countries began regular joint talks in the Chinese resort town of Xiamen to explore the possibility of an Internet Free Trade Agreement. Two years of rigorous deliberations finally led to an agreement that codified the liberalization of Internet governance-related policies. In 2024, 50 governments signed iFTA.

Pursuant to iFTA, all signatories would allow full data flows in and out of their countries; foreign direct, as well as institutional, investment in Internet companies and IT firms; and the removal of tariffs and other protectionist policies on IT products and services.

However, iFTA was met with significant opposition from civil society representatives. They expressed concerns about what they perceived as capitulation to China's demands that certain restrictions on speech and provisions about the Great Firewall be left out of the agreement, and at the US's refusal to rein in Baigogo's increasingly invasive data-collection practices. Civil society representatives were also concerned by the possibility that the agreement, as drafted, might exacerbate the global income gap.

In response, China stated that those matters were irrelevant to a free trade agreement, and that it had already lowered restrictions significantly in recent years, allowing access to foreign search engines, cloud services and social media sites like Facebook and Twitter, which had previously been blocked. Similarly, the US responded to protesters by arguing that it had already established strong net-neutrality protections and new data-privacy laws, which had been welcomed by, among others, civil society groups.



PRIVATE SECTOR

2017: Alibaba, a Chinese Internet giant, purchases 34 percent of eBay's shares.

2023: Google and Baidu form their own joint venture, under the name Baigogo.

The Xiamen Internet Forum, popularly referred to as "Cyber Davos," is created.

2025: The Xiamen Internet Forum convenes CEOs of the world's top Internet and technology companies to celebrate a new beginning for Internet governance.

PUBLIC SECTOR

2019: A UN resolution establishing norms of cyber surveillance is passed.

2022: The UN resolution evolves into a treaty.

2023: China opens and liberalizes its Internet market.

2024: In the midst of civil society protests, 50 governments sign the Internet Free Trade Agreement, which calls for the removal of tariffs and protectionist IT policies.

Timeline of Scenario "Cyber Davos"

Opportunities and Threats

After identifying the critical factors that may influence the future of global Internet governance and completing a cross-impact balance analysis of those factors, we analyzed the opportunities and threats presented by the "Cyber Davos" scenario with the goal of developing policy recommendations.

OPPORTUNITIES The "Cyber Davos" scenario presents a number of opportunities for global Internet governance, most importantly those that pertain to increased stability and the diffusion of tensions in the Internet governance system. The successful completion of the ICANN transition and the end of the standoff between multi-stakeholderism and multilateralism, combined with the unprecedented mergers of many of the world's major Internet companies, could forge a new era of international comity on Internet governance issues. Geopolitically, these events could create a virtuous cycle: business agreements would create trust, trust would create more business, and this would culminate in major multilateral agreements on Internet governance, cyber security and international norms. For companies, these events could spur a rapid expansion of Internet commerce across borders and the opening of previously inaccessible markets to foreign competition. Governments, especially China's, could relax state-sanctioned censorship, and cyber security incidents might become less commonplace.

THREATS Certain features of this scenario are less desirable and may present a real threat to Internet governance issues. Through rapid mergers and acquisitions during the post-ICANN handover period, a select group of powerful Internet monopolies could emerge, wielding tremendous influence over both domestic politics and global Internet governance issues. Less powerful voices – such as civil society groups, as well as opposition political parties looking to challenge these companies – might be pushed out of the debate. Internet companies in the Global South might be hit the most, as the monopolies would seek to prevent competition.

OPPORTUNITIES	THREATS
More efficient decision-making processes in Internet governance institutions	Increased dominance of big business in global Internet governance
Increased stability of the international cyber system	Less economic innovation; creation of monopolies
Increased US-China cooperation on Internet governance	Marginalization of civil society groups in Internet governance policymaking
Opening of the Chinese “Great Firewall”	Exclusion of developing countries from Internet governance policymaking
Resolution of the multilateral/multi-stakeholder debate	Increase of income gap domestically, and between the Global North and South
Reduced censorship	Democratic institutions weakened by excessive lobbying

Scenario 2: Google Shock

14 March 2025. The US president has arrived in Silicon Valley to address the CEOs of major Internet corporations, promising to provide support for stronger legislation to address an ongoing crisis that the press has called Google Shock: the loss of trust in US Internet companies, and the significant economic damage sustained by US and European ICT sectors over the past several years. The president is expected to assure business leaders that the US will strongly defend their interests to help them regain a dominant market position by the end of the decade.

Financial analysts have wondered whether Google Shock could have been avoided if the US had bailed out Facebook when it declared bankruptcy earlier this year. But falling earnings of Internet companies like Google over the last seven quarters may have made this crisis inevitable. Citing parallels to the global financial crisis of nearly two decades ago, pundits claim that the failure of these companies has little to do with financial bubbles. Instead, the chief causes of the technology sector's meltdown, pundits say, are the companies' inability to provide quality service to customers outside of the US and Europe, the major cyber conflict between NATO member states and Russia, and the loss of investor confidence.

Frightened by forecasters' grim outlook for American companies, investors continue to keep their eyes on China and other major Internet economies, as the expectation remains that their companies will far more easily weather this crisis. Despite protests by some Chinese investors, Beijing has not responded to calls from the White House or American corporate leaders to join hands in addressing Google Shock. In fact, not a single CEO of any of the major Chinese Internet companies plans to attend the president's speech. Rather, the Chinese press highlighted Beijing's offer to host another World Internet Conference, a biennial event that has grown into one of the largest international forums on Internet development since it began in 2014 in China. Analysts have also noted that in a global marketplace with many and increasingly diverse technology companies, particularly those based in Asia, large US-based Internet firms have largely lost their ability to influence state-based Internet governance questions. But it remains to be seen how the effects of Google Shock will ultimately reshape the Internet governance landscape.

The chain reaction leading to the protracted recessions in the US and Europe and to the announcement of Google Shock was initiated by events that took place more than 10 years ago.

In 2015, two years after the Edward Snowden revelations, the trust of many citizens in the US and the EU was further shaken when it was revealed that numerous American and European Internet and telecommunications companies had much stronger ties to their intelligence agencies than previously reported. Because of the ensuing public protest, the US and EU governments started to rethink their policies on surveillance, cyber security, privacy and censorship. Investors and customers worldwide began to leave Facebook in droves, which left the company reeling, created a loss of market share that could be filled by Facebook clones in Asia, Europe and South America, and splintered social networking along national and regional lines. In one enduring image, the CEO of China's Weibo, who had taken the opportunity to strengthen ties with business leaders in developing nations, sported a hoodie emblazoned with the words "I am not Zuckerberg" during his appearance at the second World Internet Conference in 2016 in Wuzhen, China.

At the same time, relations between NATO member states and Russia over the armed conflict in Eastern Ukraine continued to deteriorate. On 17 July 2016, precisely two years after Malaysia Airlines Flight 17 was shot down over Ukraine, a cell of Ukrainian separatists carried out a series of cyber attacks that targeted the airline industry in Europe, exposing critical weaknesses in online systems used by carriers to safeguard passenger data and in the security of air-traffic control systems. After the election of a Republican president in November 2016, the US announced that it would vastly increase national spending on new, independent networks for military and national security purposes, as well as greater protections for critical infrastructure, industrial systems and research-and-development centers.

The year 2017 began as a productive one for Chinese Internet companies. Realizing the value of new markets and the need to resolve the "last mile" problem for the delivery of Internet services, Weibo and others entered lucrative agreements with governments in Africa, Asia and the Middle East in order to improve telecommunication infrastructure. In addition to the building of regional fiber-optic networks, these investments focused on improvement to mobile infrastructure, advancing both the availability and speed of Internet access for those markets that had been otherwise underdeveloped.

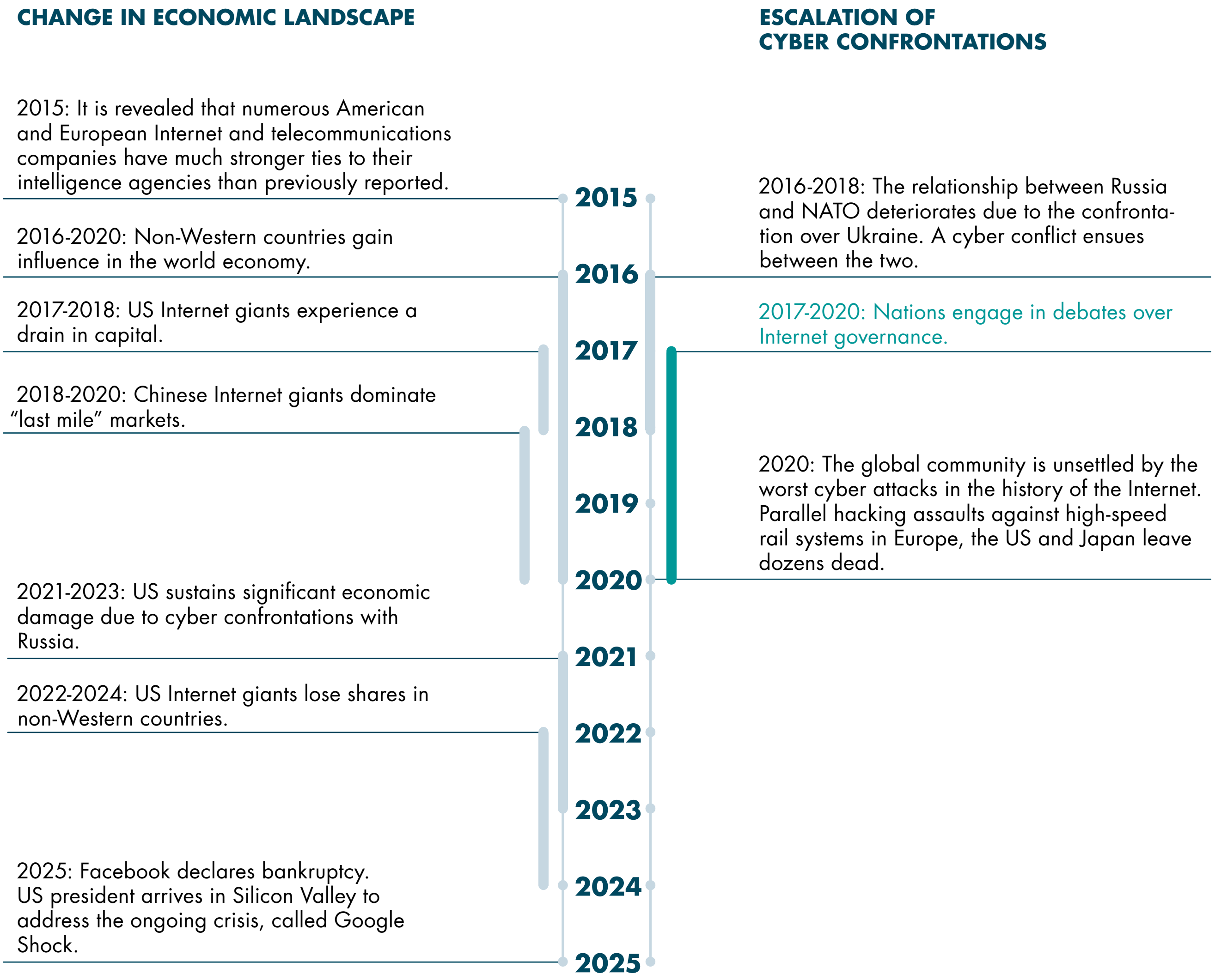
Meanwhile, the escalation of political tensions between the US and Russia brought about more cyber attacks, notwithstanding new infrastructure protections in the US. Among other strikes, American companies admitted to the theft of their trade secrets, and major European banks witnessed the loss of critical customer data. Internet access in Russia was crippled for several weeks after President Vladimir Putin's contested re-election in 2018; at that time, election observers at the Organization for Security and Co-operation in Europe found massive procedural irregularities linked to the recently introduced electronic voting system.

A week before the 2020 Summer Olympics in Tokyo, the global community was unsettled by the fiercest cyber attacks in the history of the Internet. Several parallel hacking assaults against high-speed rail systems in Europe, the US and Japan caused the malfunctioning of switches and other train controls, resulting in a series of crashes and derailments that left dozens dead and many more wounded. Russian authorities admitted to carrying out these attacks as retaliation against new sanctions levied by the US and the EU on Russia, in response to the country's continued aggression toward its neighbors.

Against this backdrop, debates over Internet governance continued. Using the end of the third round of the five-year mandate of the Internet Governance Forum (IGF) in 2021 as a pretense, Asian and Arab leaders again called for the creation of a new intergovernmental body to oversee Internet-related matters, this time joined by African governments, which had grown highly dependent on investments in their physical infrastructures by Chinese and Arab companies. Other governments, led by India and Brazil, continued to discuss alternative and more-radical solutions to the governance of critical Internet infrastructures, resulting in the creation of several new regional commissions and events that rendered global Internet governance forums increasingly fractious.

Between 2021 and 2023, the exchange of cyber attacks between the US and Russia reached a crescendo. Russia and its keyboard-for-hire hackers carried out major strikes against banks, industry and critical infrastructure in the West, causing the repeated inaccessibility of Internet root servers.

Despite important victories announced by US Cyber Command, the US sustained the worst of the damage. While Russia could rely on economic partnerships with its Asian and Arab neighbors, the conflict shook investor confidence in the US economy and led to a dramatic drop in the worth of US Internet companies in 2024. Some analysts estimated that the value of the US Internet industry had fallen to levels equal to those of 2010, an era in which the Internet had only a billion users. By 2025, Google shares were trading just above the levels at which they were valued almost a decade ago. Facebook, before it went into bankruptcy protection, was trading at less than a tenth of its total market value during its initial public offering in 2012, having lost virtually its entire market share abroad. Now, three months after Facebook declared bankruptcy, the US president arrives in Silicon Valley to announce his intention to support Internet companies reeling from Google Shock.



CHANGE IN ECONOMIC LANDSCAPE

2015: It is revealed that numerous American and European Internet and telecommunications companies have much stronger ties to their intelligence agencies than previously reported.

2016-2020: Non-Western countries gain influence in the world economy.

2017-2018: US Internet giants experience a drain in capital.

2018-2020: Chinese Internet giants dominate “last mile” markets.

2021-2023: US sustains significant economic damage due to cyber confrontations with Russia.

2022-2024: US Internet giants lose shares in non-Western countries.

2025: Facebook declares bankruptcy. US president arrives in Silicon Valley to address the ongoing crisis, called Google Shock.

ESCALATION OF CYBER CONFRONTATIONS

2016-2018: The relationship between Russia and NATO deteriorates due to the confrontation over Ukraine. A cyber conflict ensues between the two.

2017-2020: Nations engage in debates over Internet governance.

2020: The global community is unsettled by the worst cyber attacks in the history of the Internet. Parallel hacking assaults against high-speed rail systems in Europe, the US and Japan leave dozens dead.

Timeline of Scenario “Google Shock”

Opportunities and Threats

After identifying the critical factors that influence the future of global Internet governance and completing a cross-impact balance analysis of those factors, we analyzed the opportunities and threats presented by the "Google Shock" scenario with the goal of developing policy recommendations.

OPPORTUNITIES If realized, the "Google Shock" scenario could signify an increasingly multilateral approach towards Internet governance, with greater participation of non-Western states, particularly China, India and Brazil. From business and user perspectives, there could be opportunity for innovation, thereby limiting the potential for strong corporate interests to monopolize the IT marketplace. Additionally, due to more diversified participation in Internet governance policymaking, trust between major stakeholders could be established, helping to prevent future cyber conflicts.

THREATS Certain aspects of this scenario represent real threats to the future of Internet governance due to increased fragmentation. In particular, the deepening of tensions between states could lead to a greater escalation of cyber confrontations, whereas strengthened unilateral action regarding Internet infrastructure could cause a loss of the technical coordination needed to govern the network. In addition, the reduced influence of civil society and non-state actors in matters related to governance mechanisms could weaken user rights and raise the hurdles for meaningful participation of users in decision-making processes.

OPPORTUNITIES	THREATS
Less US dominance in global Internet governance	Potential escalation of cyber conflict
Increased participation of non-Western states in Internet governance debates	Loss of technical coordination needed to govern the global Internet
Reduced impact of corporate interests on Internet governance processes	Increased unilateral action on critical Internet infrastructure
Diversification of private-sector stakeholders	Fragmentation of the Internet governance regime
Resolution of the multilateral/multi-stakeholder standoff	Loss of influence of civil society and users on Internet governance issues
Increased commitment to resolving cyber conflicts	More regional monopolies of Internet companies

Policy Recommendations

This report presents two very different trajectories that global Internet governance might take. If either of the scenarios were to become reality, what can Internet governance stakeholders do to maximize the opportunities and to minimize the threats that arise? Upon considering this question, we reached a number of strategic policy recommendations that might shape the future of Internet governance. These recommendations are based on the premise that the goal of Internet governance is to maximize the Internet's potential for economic progress, sustainable development and social justice, as well as to minimize the risk of cyber conflicts and existing socioeconomic inequalities.

Internet Governance Institutions

RECOMMENDATION 1: Address the political and institutional challenge of combining a multi-stakeholder Internet governance system with intergovernmental processes.

Addressing the weaknesses of, and fundamental differences between, competing governance models might be the single most crucial step towards a more responsive and accountable Internet governance regime. Institutional reform should work towards a fair and balanced representation of various stakeholders in existing and future governance institutions.

EFFORT 1.1: In order to be more democratic and globally recognized, ongoing multi-stakeholder processes – like the Internet Corporation for Assigned Names and Numbers and the recent NETmundial Initiative – need to strengthen governmental involvement. These efforts should include official venues for open and frank intergovernmental exchange on contentious issues like security, espionage and human rights through regularly scheduled meetings, which should be the basis of forming Internet governance policy.

EFFORT 1.2: Multilateral organizations like the International Telecommunication Union need to openly address the limits of pure intergovernmental decision-making. They should grant official recognition to the private sector, civil society and user organizations, and institute transparent mechanisms through which these stakeholders can challenge and review the decisions taken at the intergovernmental level. This would encourage non-state stakeholders to engage more positively in multilateral debates and to increase the public legitimacy of multilateral processes.

EFFORT 1.3: The United Nations should renew the mandate of the Internet Governance Forum beyond 2015, reconfirming it as the Internet community's unique discussion forum, in which stakeholders can build a common understanding of policy problems related to Internet governance. The UN should strive for agreements on sustainable funding mechanisms that encourage more stability and transparency in the IGF's financial planning. The UN should create official procedures for transferring the recommendations and discussions of the IGF into UN resolutions, which could help countries to align their laws and policies on freedom of speech, net neutrality, privacy and cyber security.

Internet Business Landscape

RECOMMENDATION 2: Promote the diversity of the global Internet business landscape through increased competition and the facilitation of regional business hubs.

As market monopolization in the Internet economy puts democratic decision-making processes at risk and impedes innovation in the longer term, governments and international organizations need to undertake preventive and proactive measures to ensure competition and fair play.

EFFORT 2.1: Governments and regional organizations should encourage competition in domestic and regional markets and enhance antitrust regulations so that a single company cannot hold a dominant market share.

EFFORT 2.2: Governments should create incentives – like special economic and fair-trade zones and grants – for Internet companies and technology startups, particularly with the support of regional organizations. These initiatives could include the invitation of world talent by easing barriers for work-visa issuance, streamlining business-license authorizations and providing funding access and tax benefits.

EFFORT 2.3: International institutions should establish regulatory frameworks to encourage new and growing Internet businesses – such as those that focus on the use of big data and the "Internet of Things" – and to avoid the erosion of trust in Internet stability and access issues.

User Participation in Internet Governance

RECOMMENDATION 3: Develop mechanisms for empowering online user communities to increase the diversity of voices contributing to Internet governance policy.

Internet governance mechanisms too often fail to reflect the diversity of voices from the online user community. While some groups from highly developed countries have been more successful at speaking on behalf of their interests, developing countries often lack independent civil-society networks that could meaningfully engage with existing structures and compete with powerful business interests. In order to increase the legitimacy and accountability of existing governance mechanisms, there need to be efforts to empower users and increase participation of the world's marginalized regions.

EFFORT 3.1: Existing Internet governance institutions need to strengthen their formal strategies for bottom-up agenda setting and grassroots decision-making – for instance, through online voting systems with reliable follow-up procedures – in order to include a more diverse community of Internet users in debates on strategic governance and policy formulation.

EFFORT 3.2: In addition to these formal mechanisms for bottom-up decision-making, national governments and international governance bodies need to foster informal participation of a wider range of users through crowdsourcing campaigns and public consultation processes. Internet governance events should establish efficient remote-participation opportunities that allow for meaningful interaction.

EFFORT 3.3: To empower users from less developed countries, governments, international organizations and Internet companies should create sustainable structures for capacity building, training and fellowships, which should be adapted to local needs and conditions. Existing initiatives could be expanded, and permanent mechanisms for funding – such as revenues from new top-level domain allocations – could foster a long-term commitment to a more diverse and balanced representation in the Internet governance regime.

Fellows of the Internet Governance Working Group

JONAH FORCE HILL researches and works on a variety of Internet policy and cyber security issues, including privacy, global data flows and Internet governance. Previously, he was an analyst at Monitor 360, a strategy consultancy based in San Francisco, where he advised corporate and public-sector clients on technology policy. He has served as a teaching fellow for the course "International Cybersecurity: Public and Private Sector Challenges" at Harvard University and as a consultant and researcher for the White House's National Security Council. Jonah speaks regularly at international conferences and summits, and his writings have appeared in numerous publications, including Lawfare, The Atlantic, and Georgetown Journal of International Affairs. He holds an MPP in international affairs from Harvard's Kennedy School of Government, a master's in theological studies from Harvard Divinity School and a bachelor's in religious studies from UCLA.

AASIM KHAN is a PhD candidate and recipient of the first Mazumdar studentship at the India Institute, King's College London. His thesis focuses on political ideas and institutions shaping the expansion of Internet and related social media in India. His research interests include politics of institutional reforms and citizenship, law and governance in contemporary South Asia. Before moving to London in 2010, he worked with Oxfam GB and prior to that, with the Indian news network CNN-IBN. During these years, Aasim reported extensively on politics in India and also gained field experience in several other countries of the subcontinent, including Afghanistan, Pakistan, Bangladesh and Nepal. His commentary has appeared in Economic and Political Weekly, Himal South Asia and The Book Review. Aasim holds a master's in global media and communications from the School of Oriental and African Studies in London.

RUNHUI LIN is a professor at the Business School of Nankai University. For more than 10 years, his work and research has focused on network structures, governance mechanism and innovation performance of enterprises and organizations. He has published in China and abroad in the areas of corporate governance, network governance and IT governance. From 2004 to 2005, he was a Harvard-Yenching Institute visiting scholar at Harvard University. Since 2006, he has been serving as the director of the Network Governance Center at the China Academy of Corporate Governance. Runhui is also the deputy director of the Office for International Academic Exchanges at Nankai University, where he has gained much experience in promoting collaboration between institutions of higher education and international mobility for university students. Runhui earned a PhD in management science and engineering. He received his master's in project management from Tianjin University.

SETH OPPENHEIM is an attorney-advisor with the US Department of Justice, with expertise in international and national security law and policy. From 2008 to 2012, he was an attorney at the US Department of Defense, where he served as agency counsel in national security litigation, including in a matter before the US Supreme Court. Seth has been a Foreign Service Officer, a Robert Bosch Foundation Fellow in the Legal Advisor's Office of the German Federal Foreign Office and a Fulbright Scholar to Austria and to UNESCO in Paris. He has worked in the Office of the Prosecutor of both the International Criminal Court and the International Criminal Tribunal for the former Yugoslavia, where he assisted in the prosecution of former Yugoslav President Slobodan Milošević. Seth is a graduate of the University of Michigan Law School and the University of Michigan, where he earned both a master's and a bachelor's in political science. He also received a master's in Advanced International Studies from the Diplomatic Academy of Vienna and the University of Vienna, where he was a Fulbright Scholar.

JULIA POHLE is a research fellow at the WZB Berlin Social Science Center, where she investigates the mechanisms and dynamics of the emerging Internet policy field. She is also an associated researcher at the SMIT research center of Vrije Universiteit Brussel, where she is currently finishing her PhD about UNESCO's policy discourse on the information society. Prior to her work in academia, Julia was a consultant for UNESCO for several years. Her research, teaching and writing focus on the history of and actors in communication geopolitics, Internet policy and the role of institutions in Internet governance. Julia is a member of the steering committee of the Global Internet Governance Academic Network (GigaNet) and is actively involved in the Internet governance community. She studied cultural studies, computer science and philosophy in Bremen, Bologna, Berlin and Paris and has received numerous fellowships, including from the Carlo Schmid Program and from the Research Foundation – Flanders.

PARMINDER PAL SINGH SANDHU is presently the joint secretary at the Department of Food of the Government of Punjab, where he is steering the Unique ID project as nodal officer for the State of Punjab. In addition, he leads the various reform initiatives in the public distribution of food grains in his state. Prior to this, Parminder worked as a city manager as well as an administrator in various districts, where he has been recognized for his contribution to the grassroots implementation of various e-governance and service-delivery programs. His academic interests include issues related to public institutions, governance, democracy, bureaucracy and leadership development. A poet at heart, Parminder is an engineer by training and holds a master's in public policy from Harvard's Kennedy School of Government.

TAEJUN SHIN is currently the managing partner at his own private equity company, Gojo & Company. Taejun started his career at Morgan Stanley, where he created financial models and risk management tools, which later became global templates for Morgan Stanley Real Estate Fund. After four years at Morgan Stanley, he joined Unison Capital, the largest private equity firm based in Japan, where he managed several investment projects. While working in the finance industry, Taejun founded Living in Peace, the first microfinance investment fund in Japanese history. The fund is achieving above-market performance. He also created a crowdfunding donation platform for orphanages in Japan to improve living conditions for children. Taejun graduated from Waseda University's Graduate School of Finance with a master's in finance. Taejun has authored seven books about finance, innovation and child poverty, one of which has been published in Taiwan, South Korea and China. He has also completed long-distance triathlon competitions and a 1,648-kilometer ultra-marathon.

Annex: Scenario-Planning Methodology

METHODOLOGY Scenario planning has become a common tool for businesses and governments to strategically counter the challenges presented by complex, uncertain and hence volatile environments. We utilized the scenario-planning method in three key steps. First, we identified factors that could influence the future of global Internet governance and singled out those factors we found to be the most critical. Second, we constructed two scenarios using a cross-impact balance analysis of the factors identified. Third, we assessed opportunities and threats derived from the two scenarios and developed recommendations for how to avoid the worst outcomes of the scenarios and to encourage the best.

CRITICAL-FACTOR ANALYSIS In the first step of the scenario-planning approach, we tabulated the most salient technological, social, economic and geopolitical developments that will likely influence the future of Internet governance, ranging from trends in online social networking to a potential conflict between major cyber powers. From a list of about 40 factors, we identified 15 crucial factors that stood out for both their potential impacts and their levels of uncertainty – including the mergers of large Internet companies, the improvement of the US-China relationship, the balkanization of the Internet's network structure and the continued development of international norms. We then defined at least two possible outcomes for each factor.

FACTOR-SYSTEM ANALYSIS AND SCENARIO CONSTRUCTION To observe cross-impact and interaction effects, we rated cross-impacts between all crucial factor outcomes and created a matrix of rules for how these factors and their respective outcomes are interrelated. We utilized specialized software to run a cross-impact balance analysis that separates plausible and consistent sets of factor outcomes from inconsistent ones, and we selected two abstract scenario frameworks. We provocatively named our scenarios "Cyber Davos" and "Google Shock." This does not mean that all factors radically differ between the two scenarios. But most factors do differ, so our scenarios represent two ends of a continuum of possible futures.

Having defined two plausible and selective future states of Internet governance, we created corresponding histories for our pictures of the future by engaging in a collective writing process. We relied on intra-group discussions and exchanges with experts in the field, modeled several development paths for each scenario and engaged in multiple rounds of editing. Recognizing that the future does not develop in a linear way, we incorporated several changes in trajectories and turning points into each scenario.

REVIEW OF ANALYSIS AND RECOMMENDATIONS After they were outlined and illustrated, the two scenarios, "Cyber Davos" and "Google Shock," underwent several rounds of review.

As outlined above, we used a set of different techniques to make our scenarios robust, ranging from computerized uncertainty-impact and cross-impact analyses, to qualitative content analysis and interviews with experts. In doing so, we profited from:

- The interaction between group members with backgrounds in academia, consulting, law, politics and public affairs, as scenario planning is a holistic approach and requires diversity to tap into different knowledge pools;
- The expertise of our invited panelists and discussants, who made us aware of points of contention that we had overlooked and interactions we had neglected, and also provided valuable feedback on our descriptions, scenarios and recommendations; and
- A rigorous review process that included internal supervision and review by the aforementioned external experts.

We accounted for positive and negative factors and consequences that may shape Internet governance. We then derived recommendations. Having identified potential opportunities and threats, we generated strategic options concerning the future of Internet governance that neutralize threats and utilize opportunities for each scenario. Finally, we developed concrete policy recommendations for a diverse set of strategic actors, including international organizations, members of the business community and representatives of civil society.

www.ggfutures.net