Global Governance 2022

SECURING THE NET: GLOBAL GOVERNANCE IN THE DIGITAL DOMAIN

Puja Abbassi / Martin Kaul / Vivek Mohan / Yi Shen / Zev Winkelman

SEPTEMBER 2013

BERLIN
BEIJING
WASHINGTON DC

GG2022.NET

Supported by

Robert Bosch Stiftung

ERP

Partners

GPPi global public policy institute

Hertie School of Governance

BROOKINGS

Woodrow Wilson School of Public and International Affairs

Tsinghua University

Fudan University 1905

_ TABLE OF CONTENTS

GLOBAL GOVERNANCE 2022

GLOBAL PUBLIC POLICY INSTITUTE (GPPI)
REINHARDTSTR. 7
10117 BERLIN, GERMANY
GG2022.NET

PUBLISHED: SEPTEMBER 2013
EDITORS: JOHANNES GABRIEL,
OLIVER READ, JOEL SANDHU

_ ABOUT THE REPORT

This report was produced within the framework of the Global Governance 2022 program, organized by the Global Public Policy Institute in Berlin, in collaboration with partner institutions in the United States (The Brookings Institution and Princeton University), China (Tsinghua University and Fudan University), and Germany (Hertie School of Governance).

GG2022 brought together 24 young professionals from the US, China and Germany for three meetings, one each in Berlin (26-30 August 2012), Beijing (7-11 January 2013) and Washington, DC (5-9 May 2013). During these meetings, the GG2022 fellows jointly discussed challenges of global governance in the year 2022 and beyond, with a particular focus on three areas: cyber security, energy security, and development.

This report summarizes the work of the GG2022 working group on global cyber security governance. To explore possible futures in global cyber security governance, the working group used a scenario planning methodology with techniques developed extensively in the field of future studies. The diverse nationalities, backgrounds, and expertise of working group members contributed crucial assets for devising national strategies and solutions.

During the three sessions, the working group also met with leading academic experts and policymakers in the field of cyber security from all three countries. We are grateful to all these experts for their valuable input.

We would also like to thank the organizers and funders of the GG2022 program and everyone else who contributed to making the program possible, most especially Joel Sandhu and Johannes Gabriel. We are also grateful to Alex Fragstein for her design work and Oliver Read for editing.

Disclaimer: The views expressed in this report do not necessarily represent the views of, and should not be attributed to, any author in his individual capacity nor to their respective employers.

_ EXECUTIVE SUMMARY

Today's globalized and interconnected world is increasingly reliant on the Internet and cyberspace. These innovations have the potential to help maintain peace, increase prosperity, and increase access to information across the globe. Recent events, however, have evinced a trend of increasing threats and diminished security in cyberspace. The disclosures of massive cyber surveillance operations in North America, Asia, and Europe have raised additional concerns. The question of how global cyber security governance will evolve over the next decade is therefore of the utmost importance.

We argue that the range of possible outcomes for global cyber security governance is bounded at the extremes by two paths. At one end of the spectrum lies the death of the Internet as we know it. Though many stakeholders would label this future outcome dystopian, others might welcome it. At the other end of the spectrum is the potential for a utopian resolution to mistrust and conflict in cyberspace, which presumably satisfies all stakeholders. The actual path will likely fall somewhere in between. But these two poles can aid policymakers by conveying diverging directions that we might head and the implications of those scenarios.

Could the Internet actually die? The path to this outcome might be precipitated by an inability to address growing mistrust, the continued existence and exploitation of major cyber vulnerabilities, and mass fear created by new kinds of cyber attacks. Even in such a dystopian scenario, communication networks are likely to survive in some form. But we need look no further than the headlines about internet kill switches, sovereign control of information, and national firewalls to witness the fragmentation of the "open" foundation, both in terms of technology and governance, that has thus far prevented the extreme balkanization of the global Internet. When every country has its own search engine, social network, micro blog, and video sharing site, how many users will actually notice the lack or disappearance of international connections?

Will the international community ever reach a formal agreement regarding the rules of the road and enforcement mechanisms in cyberspace? Multilateral trust building, substantial advances in technology that mitigates cyber vulnerabilities, and inclusion of a more representative set of stakeholders would all make this outcome more likely. Unfortunately, recent developments do not provide a sense of tremendous optimism. And while distinctions between different types of espionage based on the purpose of collection is difficult enough, agreement on the rules of engagement in cyberspace would be even harder to resolve if actual conflict were to break out. Nevertheless, an appropriately empowered international body might be the only way to avoid the pitfalls of a disconnected world that is likely to emerge should the current rifts regarding cyber security grow so wide as to make any form of global governance impossible.

Ultimately our future is what we make of it. We therefore offer a lead strategy that identifies beneficial actions regardless of which future emerges and a set of four policy recommendations that aim to strike an optimal balance between the threats and opportunities presented by each scenario:

Lead Strategy

› Encourage domestic/bloc innovation
› Focus on technology that addresses cyber vulnerabilities
› Build confidence via incremental win-win cooperation
› Maintain the ability to act unilaterally

Policy Recommendations

› Enhance trust through existing governance structures
› Address long standing points of contention by internationalizing control over ICANN and curbing economic espionage
› Build capacity to reduce exposure to cyber vulnerabilities across the entire system of stakeholders
› Build a "trust cell" for cyber security governance that evolves from current structures and includes representation from NGOs and the private sector

These recommendations taken together present a robust set of actions that pave a path forward towards establishing an environment in which a more cooperative form of global cyber security governance could evolve.

_ SCENARIO 1: "CYBER DEATH" – THE END OF THE INTERNET AS WE KNOW IT

"If you look back, it almost seems as if there was a virus that targeted the very essence of cyberspace itself," sighs retired US General Keith Alexander. As he turns toward his fellow panelists, the former head of the Pentagon's Cyber Command adds, "in the end, cyberspace as we knew it simply couldn't survive." General Huichang, China's "cyber czar," and Thomas de Maizière, former German Minister of Defense and now special rapporteur to the UN Secretary General on Cyber Security, both nod in solemn agreement. All three panelists try to make sense of the Internet's demise over the last decade during a panel discussion at The Brookings Institution in the summer of 2022.

In hindsight, the death of the Internet as we knew it came as a succession of events that built upon each other and took place in three major stages:

› an "incubation period" during which steadily growing Sino-American tensions, an inter-state cyber incident as well as the continued militarization of cyberspace led to a gradual disconnection of various sectors of critical infrastructure from the Internet;

› an "outbreak phase," in which a "tsunami" of cyber crime led to a collapse of e-commerce and forced governments, overwhelmed by the volume of crime in cyberspace, to develop secure, parallel network architectures that conformed to national and regional boundaries;

› finally, the "passing of the 'old' Internet," initiated by Russia, China, and Germany following a global panic during a brief period of "cyber terror."

To paraphrase Winston Churchill, the years 2013 and 2014 marked the "end of the beginning" as the sequence of events led to the implementation of a new cyber architecture. A diplomatic row occurred in 2013 between the United States and the People's Republic of China. What began as a disagreement over industrial espionage and codes of conduct in cyberspace grew increasingly heated in 2014 when the US Congress passed legislation that blocked Chinese communication equipment providers Huawei and ZTE from the US market on the grounds of national security. Chinese Premier Li Keqiang retaliated by calling an emergency press conference and presenting a 466-page catalogue that described alleged cyber attacks on Chinese state-owned enterprises and security institutions stemming from IP addresses in the United States. The premier announced that all Cisco and Apple products were banned from the Chinese market.

These developments exacerbated the steadily growing tensions between the "G2," as the United States and the People's Republic of China were then referred to in the press, and led to the indefinite suspension of all formal and informal discussions, including all track II dialogues.

Things were about to get much worse. Two short weeks later, a "war of words" that had been brewing between China and Japan over the Diaoyu/Senkaku islands almost turned physical when fishing vessels from the two countries nearly collided in disputed waters. As diplomatic relations broke down, a sophisticated cyber attack aimed to paralyze the SCADA system of Tokyo's Yamanote subway line was detected and thwarted at the last minute. Three days later, a similar attempt to sabotage the control system of San Xia, China's biggest dam, was similarly detected and neutralized. While

the media ascribed the action to "patriotic hacktivists" rather than dedicated military cyber units, the culprits were never conclusively identified.

Thankfully cooler heads prevailed, and a military confrontation was avoided. Yet, the incident resonated throughout the defense departments of all the major powers, as a real-world example of the vulnerability of civilian critical infrastructures was brought to the forefront of the international conversation. Analysts and strategists in Berlin, Moscow, Tokyo, and Washington now had frightening evidence that the conventional logic of cross domain cyber deterrence – "if you shut down our power grid, maybe we will put a missile down one of your smokestacks," as put by a US military official in 2011 – was insufficient to prevent "rogue" cyber warriors from striking critical infrastructure facilities.

The incident was taken most seriously in China, where the San Xia intrusion was dubbed "Cyber 9/8"– a reference to the Chinese failure to prevent the Japanese invasion of Manchuria on August 9, 1932. Immediately after the incident, CNNIC, China's main institution for the management of the Internet, undertook a review of critical infrastructure practices, quickly disconnected industrial control systems from the Internet, and reorganized them around the Ministry of National Defense.

Such aggressive moves to bolster cyber defenses, as well as growing US-China tensions, led other states to follow suit. In capitals from Madrid to Seoul, disconnecting critical infrastructures from the Internet and organizing such systems on secure, governmentally controlled networks became an immediate priority.

As the imminent danger of military conflict receded in 2014, another long-feared development buffeted the Internet. Cyber crime, which had grown steadily over 2014 and 2015, erupted into what the news media described as a "tsunami" in 2016. Identity theft, coupled with state-sponsored or state-sanctioned industrial espionage, became so rampant that the world's largest insurers and reinsurers bowed out of the until-then booming cyber insurance market. In spinning off its cyber unit, AIG's CEO described the scope of its potential liabilities as "toxic." Stock markets worldwide took this news poorly, as investors dumped shares of companies reliant on e-commerce. The collapse of the insurance market led major financial institutions worldwide to revise their policies on liability. One by one, banks moved towards making it extremely difficult for customers to have fraudulent transactions voided when their accounts were compromised using valid credentials.

The collapse of e-commerce, which threw the global economy into a recession, was paired with a global run on banks. The lack of confidence in banks led to the withdrawal of private savings at record levels. This near-immediate global collapse of the financial system spurred governments to action. Major Internet companies, which over the past decade had increased their political influence to rank among the most influential players in the international system, were caught off guard by the speed of the collapse, and their lobbyists and representatives found themselves quickly ostracized in capitals around the world.

In emergency legislative sessions, law enforcement and intelligence agencies explained how the geopolitical tensions of the previous years had prevented them from effectively collaborating on a global scale, leaving an enforcement vacuum. Confronted with this reality, and facing immense political pressure, leaders across the globe came to a radical solution. At a G20 meeting in 2016, global leaders adopted a proposal put forth by a Sino-German-Russian troika that called for the creation of a second, parallel network air gapped from the current infrastructure. This new network was to be run on nationally controlled protocols that would be compatible with one another but could communicate only through trusted gateways, allowing for effective local law enforcement. While Internet freedom activists decried this development, public sentiment was firmly in support of government action by virtue of the cyber crime crisis.

Private firms, whose critical business functions had been crippled by the lack of security on the old Internet, were the first to transition to the new network. Though wary to depend on the government for critical parts of their operations, businesses were quick to realize the myriad benefits provided by this secure platform for e-commerce.

Citizens approached the transition more cautiously, having grown accustomed to providing their own security measures. Civil liberties organizations criticized the intrusive nature of the new network, which required continuous biometric authentication and afforded no expectation of privacy from law enforcement. When activity on the new network did cross international boundaries, it was subject to mandatory deep packet inspection on both sides of the connection. Common standards often ended at the handoff, as each state developed its own implementations of various networking protocols. Some governments allowed a wide variety of traffic in and out, while others restricted international traffic to the minimum amount necessary for essential functions of the state.

The "Second Net" offered a secure alternative in cyberspace, but it did not outright "kill" the old Internet. The old net was kept alive by concerned citizens, aided by NGOs and activists, many of whom relished the freedom and anonymity of cyberspace. Despite the impassioned support by a dedicated few, traffic on the old net slowed to a trickle by 2021 as more and more citizens became accustomed to the security-liberty trade-offs of the new net. While cyber crime continued to exist on the new network, it was drastically reduced back down to manageable levels. Effective domestic law enforcement agencies proved to be a credible deterrent.

In 2021, a talented 15-year old Malaysian hacktivist known as "X" was apprehended for attempting to access classified databases belonging to the US Department of Defense. His subsequent extradition and incarceration as an enemy combatant set the social media channels on the old network alight. Online protests erupted over the treatment of X and the revocation of fundamental civil liberties on the new net.

A message appeared on Twitter's old Internet platform purporting to be from a group known as @ ElectroMagneticPacket (EMP). EMP set an ultimatum for the hacktivist's release, threatening one "e-Execution" per day until X was set free. Despite the fanfare that this received in the activist community, governments initially ignored it.

Twelve hours later, EMP tweeted the name of their first victim – the head of the Malaysian intelligence agency that extradited X. Shortly thereafter, he died due to a malfunction in his pacemaker. EMP promised a second announcement within 12 hours, and panic spread across the globe. EMP followed through on its threat: Another official involved in X's extradition died in a gruesome auto accident when the navigation system in his car overrode his commands and directed his car over a bridge guard rail. EMP declared it would continue its retaliatory executions against countries associated with the hacker's capture until he would be freed.

Emergency meetings were convened in Washington, Berlin, London and other capitals around the world but the identity and origins of EMP remained unknown. On the third day, security audits at cyber armories in the US and China revealed major breaches that had occurred in the past year. Most importantly, several highly potent designs that targeted vulnerabilities in legacy systems on the old Internet had been exfiltrated. Investigations on both sides found that trails went cold, and it became clear that EMP was in possession of weapons that could wreak havoc on the old Internet at will.

Russia, China, and Germany came to an emergency accord, declaring in unison that they would completely disconnect from the old network. The United States and other countries followed within days. "And so," remarks Thomas de Maizière, "the Internet had gone completely dark. The old net never returned." Says General Huichang: "And it never will."

_ SCENARIO 2: "CYBER PARADISE"– THE ETERNAL NET

"It feels good," smiles Sergey Brin after his first week in office. "We all know that there are some challenges ahead of us. But we have also overcome quite a few. Could you have imagined 10 years ago that we would be sitting here today?" Hardly anyone would have foreseen Brin taking office in Singapore's Downtown Core as director of the International Cyber Security Agency (ICSA) in June 2022. Brin and his deputy director, Jian Shuo Wang, who successfully ran his own venture Baixing.com before being handpicked for the agency by China's outgoing president Xi Jinping, have worked in tandem to get the agency ready over the preceding 18 months and now oversee its operations.

Despite dire warnings, notably by former US Secretary of Defense Leon Panetta in the early 2010s, neither a "Cyber Pearl Harbor" nor a "Cyber 9/11" have occurred. Furthermore, organized cyber violence became increasingly unlikely due to three interrelated developments:

› bilateral and multilateral efforts between states that ultimately led to a General Agreement on Confidence Building in Cyberspace (GACBC);

› the diffusion and increased sophistication of cyber security systems/infrastructure, in particular advanced cryptographic and "electric fence" systems;

› and lastly, the creation of a regime centering around the International Cyber Security Treaty.

The GACBC emanated from a long line of discussions, meetings and conferences. Building on bilateral dialogues on both track I and track II levels, and the multilateral World Summit on the Information Society review meetings (WSIS+10), the United States and China sought to restore confidence and trust following a period of bickering over cyber espionage that originated in China in the spring of 2013. Traditional measures of confidence building were discussed and partly agreed upon. These included increased transparency on cyber doctrine, formal and informal exchanges between civilian and military officials, and sharing of information on cyber threats.

As the Internet was expanded further into all aspects of daily economic and social interactions, attention to the topic by politicians and the media continued to grow. Henceforth, a conference program was initiated that included not only the US and China but also the European Union, India, Russia, and Brazil. The discussions in this "cyber club" carried over to G20 meetings, as cyber security became a priority issue in national defense. However, advocacy groups and corporate actors soon bemoaned the increasing state-centrism in Internet governance. To appease these critics, European states advocated a multi-stakeholder model, and most governments joined in the promise not to restrict even more civil liberties in the name of cyber security. Resulting from this process, the G20 signed the GACBC in the winter 2015, with other states free to join. Within 18 months 104 states acceded.

Not everyone believed the GACBC was sufficient to constrain states that did not sign on, or sufficient to combat the rising number of cyber crime incidents. This motivated cyber security companies like Quest Software and Kaspersky Lab, and new entrants into the cyber security market like General Electric Cyber and Boeing's Digital Security Unit, to invest heavily in defensive cyber capabilities, for instance advanced cryptographic systems. Sophisticated encryption technologies and "electric fence" systems for digital loss prevention dramatically lowered the probability of successful intrusion and disruption of almost all networked

systems. Corporate actors, critical infrastructure providers, and military installations were hence less vulnerable to attack.

A "Cyber Cuban Missile Crisis" led governments to realize that an agreement on confidence building measures alone would prove incapable of securing cyberspace. In 2017, a highly complex virus nearly plunged Europe's air traffic into chaos. Security experts located and disabled the malware just hours before it would have "blown out" the air control system at Frankfurt Airport. It was widely believed that the virus was implanted in the laptop of an Austrian diplomat whose mission to Tehran was aborted at the last minute. The incident and subsequent popular protests sent shock waves not only through the Kanzleramt but also through the White House as well as the Russian and Chinese leadership circles. Decision-makers clearly recognized that offensive cyber malware might just be a digital Pandora's box. And a subsequent change in attitudes accelerated the formation of an International Cyber Security Treaty well beyond the capabilities of the GACBC.

With the US, EU, Russia, and China on board, the negotiations leading to the International Cyber Security Treaty in 2020 first centered around several non-aggression norms, which were quickly agreed to before being broadened in scope to armament control and a framework for offensive cyber capabilities. This first pillar was accompanied by intimate cooperation with regard to cyber crime, which relied extensively on the groundwork provided by prior successful European-American cooperation. It can be traced back to 2012 when the two partners spearheaded the Global Alliance against Child Sexual Abuse Online and set up the Dubai Committee on Cyber Crime Prevention and Enforcement in 2016, which tasked itself with further facilitating collaboration of law enforcement as members agreed to widely share information and intelligence on transnational cyber crime networks.

The treaty also represented the new power that multinational corporations (MNCs) exhibit in relation to the nation state. That the respective summit on the way to the treaty is commonly referred to as "G25" or "G20+5" illustrates the prominent role of five, particular MNCs in the field of cyber security/cyberspace among the group of leading countries. While governments stressed their final say on matters of cyber security, it was clear that sustainable security in cyberspace could not be achieved without the support of these MNCs. And yet, multinationals had to accept reluctantly a compromise that allowed individual states to adhere to the notion of information sovereignty curbing Internet freedom.

In a symbolic web conference, the treaty was ultimately signed by the heads of all 162 participating nations, foremost China, the United States, India, Russia and all 32 EU member states on January 4, 2020. It could be seen as the culmination of a decade long trend to successfully manage cyber security on a global scale, resulting in the establishment of the International Cyber Security Agency. The agency acts as hub for information sharing and inter-agency coordination on a global scale. US President Eric Schmidt, who relied on the slogan "conquering the future" to conquer the White House, proclaimed during the agency's opening ceremony: "Almost a decade ago, I referred to the Internet as the 'largest experiment involving anarchy in history.' I would now add that it is the most productive experiment the world has ever witnessed. We want to keep it that way by adding a watchdog that guarantees a necessary amount of order."

"Our job is almost done for us," smiles Sergey Brin, who resigned as US Secretary of State to head the new agency after President Schmidt's reelection in 2020. "Well, it is not that there is nothing for us to do," adds Wang, "but given the abysmal predictions 10 years ago, we are now living in something akin to a cyber paradise."

TIMELINES

> CYBER DEATH

- 2014 — Disconnection of national critical infrastructures from the net
- 2014 — Adoption of nationally controlled protocols
- 2016 — Cyber terror (e-executions)
- 2021 — US-China Energy Dialogue leads to BIT, which articulates tech transfer guidelines and energy innovation sharing regime
- 2022 — State disconnection from the “old” Internet

> CYBER PARADISE

- 2012 — General Agreement on Confidence Building in Cyberspace (GACBC) reached among major powers
- 2018 — G25 Summit as response to Cyber Cuban Missile Crisis
- 2020 — Ratification of International Cyber Security Treaty
- 2022 — International Cyber Security Agency (ICSA) becomes operational

_ STRATEGIC IMPLICATIONS

The preceding scenarios describe a range of options for the future of cyberspace and how the Internet could develop from the present day to the year 2022. The current trend is an increasing shift toward militarization of cyberspace and the nationalization of cyber infrastructures and governance.

This is mainly the result of both an inherently insecure platform and a lack of trust, and it may ultimately lead down a path to "cyber death" reminiscent of scenario 1. Nevertheless, both scenarios are possible futures.

In our analysis we therefore:

- analyze each scenario's main opportunities and threats;
- present a lead strategy, applicable and robust across both scenarios, which consists of the actions that should be taken no matter which direction global cyber security develops;
- outline policy recommendations that preserve an open and secure cyberspace.

Threats & Opportunities

> Death of the Internet

THREATS	OPPORTUNITIES
› Freedom of speech and privacy are curtailed.	› Domestic networks strengthen cultural and economic national identity.
› Nationalization in online world spills into the offline world.	› Risks of cross-border cyber crime and cyber war diminish significantly.
› International commerce and innovation are stifled.	› International institutions arise to mediate connections between networks.

Threats. In the "Death of the Internet" scenario, we see a monopolization of control in cyberspace by the state, leading to the end of the multi-stakeholder approach to cyber governance. Corporate and individual actors lose their voice. The threat to freedom of speech and privacy is increased by the assertion of control by governments. Nationalization in cyberspace brings further risks of spilling over into the offline world and reverting the globalization of the world to which we have grown accustomed. This in turn also poses a threat to international commerce and innovation.

Opportunities. However, as we see already in today's Chinese online economy, restricted international access can lead to strengthened domestic cultural and economic national identities. Instead of using globalized services (eg, Facebook, Twitter or YouTube) local alternatives are favored (Weibo or Youku). Another opportunity is the significant diminishing of cross-border cyber risks inherent to this scenario. Looking at the need for cross-border connections, international institutions like the International Telecommunication Union might arise that take on the task of mediating these risks.

› Cyber Paradise

THREATS	OPPORTUNITIES
› International discussions omit substantive privacy and freedom of speech provisions.	› Netizenship promotes global society.
› Continued use of existing insecure network means risks remain inherent.	› International innovation and commerce are strengthened.
› Strategic national interests conflict with cooperation in cyberspace.	› Confidence in international cooperation rises.

Threats. The international cyber security regime and treaty in this scenario were based on the fear of crime and terrorism on the Internet, risking the omission of substantive privacy and freedom of speech provisions. Further, the continued use of the current network, which never had security at the heart of its design, means that at least some risks might remain inherent. Another threat of this scenario is that the international cooperation that is agreed upon in the treaty might conflict with strategic national interests of states and may be difficult to enforce. Further, there might be an asymmetry in capabilities among actors to secure cyberspace. This also leads to the threat of a few powerful players dominating the cyber sphere.

Opportunities. Global "netizenship" promotes an even more global society than we already see emerging today. This can in turn be used to strengthen innovation and commerce internationally. Lastly, the confidence built through international cooperation in cyberspace might encourage trust in international cooperation in other fields of global governance.

Stakeholders' Perspectives

Current Internet structures are under pressure. We observe a growing trust gap between stakeholders on different levels. On the political level, the East-West divide – most notably between China/Russia and the United States – is increasing, as is the North-South cleavage between "data-donors" and "data-takers." We also see gaps between bigger and smaller companies, as well as between private and public actors. Further, activists and NGOs are growing more suspicious of both political and business entities. Moreover, there is a major demographic shift in Internet users from West and North to the East and South brewing. These cultures may see cyberspace and their role in it differently. In sum, stakeholders do not share a common, basic view of either cyberspace or the core concepts of cyber security.

Lead Strategy

The lead strategy presents a robust set of strategic actions that states can employ in either scenario to avoid threats being realized and to make use of opportunities. This implies that even though actors might find themselves in the worst case scenario, the lead strategy would still provide some benefits or at least bear no downsides.

Encourage domestic/bloc innovation. Innovation occupies a central position. Even in cyber paradise

most actors will likely seek to promote their domestic innovation capabilities to keep competitive advantages in some fields. In the case of a sudden death of the Internet, it is even more important for actors to encourage innovation as they are no longer able to rely on international cooperation. This strategy can be implemented not only inside the state but also inside blocs, where members share a general ideology, interest, or common understanding of cyberspace. This innovation is not meant to block out other countries or blocs, but rather, especially in the case of a future of a more open net, to be a measure for staying competitive and not being left behind.

Focus on technology that bolsters defense and resilience. Technological innovation should mainly target capabilities that bolster defense and resilience. Investing in defensive capabilities such as encryption technologies do not deter the threat per se. But decreasing vulnerabilities and limiting negative consequences of cyber attacks will enhance security without triggering a cyber arms race based on a perceived security dilemma. All stakeholders, especially the state, should not be encouraged to take advantage of the defensive capabilities for improving their offensive capabilities.

Promote confidence building by focusing on areas that promise absolute gains and win-win constellations. There is a lack of a consensus on core concepts, recommended policies, and modes of behavior in cyberspace. Confidence can nevertheless be formed via a step by step approach where cooperation starts in issue areas that promise absolute gains and win-win constellations, for example fighting child pornography and building mechanisms to exchange information on cyber vulnerabilities and incidents of cyber crime.

Maintain ability to act unilaterally. In both scenarios, total coherence is not possible as all actors still face the challenge of high uncertainty. Thus, even in a robust lead strategy the realistic approach for most actors, but especially for great powers, is to prepare for the worst, which means maintaining some abilities that allow them to act unilaterally, for example fallback systems that ensure the stability of the network in case central or global systems fail.

_ POLICY RECOMMENDATIONS

We have developed two illustrative sketches of extreme scenarios and attendant strategic implications that draw from understanding the consequences of "Cyber Death" as well as of "Cyber Paradise." We are keenly aware that hybrid scenarios may occur and, indeed, present a more likely outcome. A Cyber Cuban Missile Crisis, for instance, may not prevent the further fragmentation of the Internet.

Building upon the strategic implications of our two scenarios, we now present a set of policy recommendations for stakeholders – both state and non-state, reflecting the nature of the Internet – to adequately prepare for the coming decade in cyberspace governance. The following recommendations draw on the strategic implications as well as existing realities and lessons learned from past decision-making.

The basic premise of this report is that the Internet offers substantial economic and social benefits and that it is in the common interest to protect those benefits. Another premise is that there is no common global view or governance concept for cyber security. Thus, in drawing a linguistic analogy to the Schuman Declaration, the founding document of European integration, it is obvious that "an open and secure cyberspace will not be made at once or according to a single plan. It will be built through concrete achievements which create a de facto solidarity." We propose four fields of action that enable such achievements.

Effort 1: Enhancing Trust

Leverage existing governance structures, such as the Internet Governance Forum, and ensure democratic participation.

Establishing a bilateral US-Chinese working group on cyber security or multilateral fora such as the UN Group of Governmental Experts on Cyber are emblematic first steps in trust building. Yet some governmental fora and private collaborations have not fulfilled democratic expectations of legitimacy or participation. For example, the Global Network Initiative contains major cyber players with exceeding influence over billions of users without proper democratic legitimacy. However, the existence of such organizations and bodies provide venue for progress in enhancing cross-border trust and cooperation. They help to foster collective learning and understanding of concepts and behaviors.

The proceedings of the World Summit on the Information Society in 2005 already exposed international friction and mistrust on fundamental issues of Internet governance, eventually giving birth to the Internet Governance Forum. If properly structured and attended, the WSIS+10 process could transform the already existing Internet Governance Forum into a sui generis body that provides the multi-stakeholder system with an even more sophisticated architecture. However, multi-stakeholderism remains an empty phrase if stakeholders continue to only talk about each other, not with each other. Governments only pay lip service if their efforts do not comprehensively include cooperation and discussion with Internet exchange points, Internet service providers, content providers and NGOs as well as activists.

Effort 2: Internationalizing Power

Negotiations to internationalize control over ICANN and other major players including MNCs should be understood as concessions in exchange for international agreements on issues such as domestic crackdowns on international industrial espionage.

The Internet, its governance structure and major players therein are perceived by many around the world – China in particular – as dominated by the United States and, as such, used as a lever to threaten national sovereignty. Addressing those concerns may require further "internationalization" of the Internet ecosystem. This pertains foremost to the Internet Corporation for Assigned Names and Numbers (ICANN), which stands as a symbol for US dominance. Whether its influence as a "Internet phone book registrar" might be overestimated or not, the fact that ICANN operates a centralized control of IP-distribution and the Domain Name System under a memorandum of understanding with the United States Department of Commerce is still unacceptable to many stakeholders, several of whom expressed their objections at WCIT in 2012.

Although the United States does not exert the same level of control over ICANN as in the past, a further internationalization of the organization's structure following its current decisions to set up additional ICANN headquarters in Singapore and Istanbul would yield invaluable benefits for cooperation. Such changes would signal a credible commitment from the United States, but they will likely require reciprocation in the form of binding concessions from other stakeholders to crack down on piracy intrusions or to hamper industrial espionage.

Effort 3: Building Capacity

Investment must be made by all stakeholders towards deterring malicious cyber activity.

A chain is only as strong as its weakest link. The Internet, not having been designed with security in mind, is a series of weak links. "Security by design" offers significant benefits and has a deterrent effect upon smaller-scale cyber criminals. However, it is unlikely to deter the development of and research into offensive cyber capabilities at the state level.

Yet as a significant step all stakeholders need to reduce vulnerabilities by investing in security to a larger extent. They should be further incentivized by technology, policy, and norms. Capacity building makes individual companies and agencies more secure. However, current narratives on "deterrence by retaliation" versus "deterrence by denial" do not sufficiently address the challenges we face in cyberspace. We therefore want to stress the "economic self-deterrence" of the Internet by making individual threats even more valuable and therefore worthy of even greater protection. These steps to deter malicious activity represent progress towards the aspiration for safety and security online that remains balanced with ideals of openness and freedom.

Effort 4: Building Capacity

Leveraging the benefits of other efforts already underway, build a new forum out of existing structures where gains in trust, internationalization, and increased capacity can be locked in by a group that is sufficiently representative and mutually cooperative.

The aforementioned efforts should finally lead to the creation of a multi-stakeholder trust cell including G20, GNI and NGOs, hence "GNO25." We envision this trust cell emerging from current organizations (ICANN, ITU) while at the same time involving transnational non-profits and corporate

actors. We see such an architecture as both an effective and efficient means to deal with cyber security issues, as an international cyber security regime would create required lock-in effects, thus strengthening de facto solidarity. In other words, we have to show that cyber security is an open-sum game. The evolution of a GNO25 regime holds the promise to simultaneously limit cyber security challenges and to further stimulate an innovation ecosystem that facilitates and accelerates technological advancements. Moreover, trust built through increasing participation in Internet governance could be leveraged – at least at the state level – to discourage the use of offensive cyber capabilities.

Developing a cyber security regime that evolves out of existing Internet governance structures presents a Herculean task. However, this report argues that utilizing existing Internet governance structures instead of creating another international bureaucracy ex nihilo better preserves the innovative power of cyberspace. The creation of a cyber security trust cell from bodies such as the aforementioned ICANN, IGF, and others is both a desirable and realistic objective.

Taken together, these recommendations present a robust set of actions that pave a path forward towards establishing an environment in which a more cooperative form of global cyber security governance could evolve. Cyber security is undoubtedly a topic that has risen to prominence, but to suggest that negotiations on cyber will occur in a vacuum would be short sighted. The more our world becomes interdependent, the more strategic and pragmatic planning, together with institutional design, gain in importance for establishing international organizations to solve global problems. The rapid advancement of technology adds to the volatility of current global affairs and to the urgency of establishing effective cyber security governance. The magnitude of difficulty in establishing a cyber security regime may seem daunting. But one thing is certain: The status quo will not remain. By 2020 there will be two billion more users on the Internet, mainly from developing countries. Developing a form of global cyber security governance that can represent these and all future users is an opportunity with benefits that should outweigh the concerns.

_ ANALYTICAL BACKGROUND/METHODOLOGY

We derive the insights offered in this report not out of "thin air" but through a structured scenario approach. Scenario planning has become commonplace among business and government alike to strategically counter the challenges that increasingly complex, uncertain, and hence volatile environments present. We utilized the method in three major steps. First, we conducted an environment and factor analysis. Second, we utilized factor-system analysis and subsequently constructed two main scenarios using a cross-impact balance analysis. Third, we analyzed consequences and drew strategic implications as well as policy recommendations.

Environment & Factor Analysis

We tabulated the most salient technological, social, economic, and geopolitical developments that will likely influence international cyber security governance, ranging from trends in quantum computing to a potential Sino-Japanese conflict in the East China Sea. From the list of about 40 factors, we identified 15 factors that stand out in both their potential impact and their level of uncertainty, among them the occurrence of a large-scale cyber incident; the development of cyber weaponry and a potential change in the offense-defense balance; changes to the Internet's network structure ("balkanization"); and the development of international norms. We subsequently defined at least two possible outcomes for each crucial variable to complete our factor analysis.

Factor System Analysis & Scenario Construction

To observe cross-impact and interaction effects, we rated cross impacts between all crucial factor outcomes and created a matrix of rules on how these factors and their respective outcomes are interrelated. We utilized a specialized software (ScenarioWizard) to run a cross-impact balance analysis to separate the plausible and consistent sets of factor outcomes from the inconsistent ones and selected two abstract scenario frameworks. We provocatively named our scenarios "Cyber Death" and "Cyber Paradise." This does not mean that all factors radically differ in the two scenarios. (We envision in both scenarios, for example, that states will "bring themselves back in" and will resume a more pronounced role in cyber security governance.) But most factors do differ, so our scenarios represent the two ends of a continuum of possible futures. Having defined two plausible and selective future states of cyber security, we employed a driver-centered analysis to learn more about the forces that primarily influence developments. We then created corresponding histories for our pictures of the future by engaging in a collective writing process. We relied on intra-group discussions as well as exchanges with experts in the field, modeled several development paths for each scenario, and engaged in multiple rounds of editing, harmonizing, and re-editing. Recognizing that the future develops in a way that is hardly linear, we incorporated several changes in trajectories and turning points in each scenario.

Strategic Implications Framework

After they had been outlined and illustrated, the two scenarios "Cyber Death" and "Cyber Paradise" underwent extensive checks through expert reviews. We first accounted for positive and negative factors and consequences (opportunities and threats) that may shape cyber security as a global public good. Second, we derived strategic options to neutralize threats while utilizing opportunities for each scenario. Third, we determined the strategic fit between both strategy sets and developed a robust lead strategy, including all options that proved to be consistent for both scenarios. We then defined the key stakeholders in international cyber security governance and accounted for their perspectives and strategic interests in a subsequent decomposition process. By taking into account the broad range of – at times incompatible – interests among stakeholders and identifying strategic options shared among governments, international organizations, NGOs, and multinational firms, we were able to both refine our lead strategy and to derive concrete policy recommendations. This multi-stage process left us with a set of strategic recommendations intended to avoid worst-case outcomes and to pave the way for an effective and efficient governance architecture in the field of cyber security.

As outlined above, we used several techniques to make our scenarios robust, ranging from computerized uncertainty-impact and cross-impact analyses to qualitative content analysis and expert interviews. In doing so, we profited from:

› The interaction of group members with backgrounds in politics, consulting, law, public affairs, and academia. Scenario planning is a holistic approach and requires diversity to tap into several knowledge pools.

› The expertise of our invited panelists and discussants. They made us aware of points of contention that we overlooked or interaction effects that we had neglected and thus not only provided tacit knowledge but also ample feedback on our descriptors, scenarios, and recommendations.

› A rigorous review process that included internal supervision and the aforementioned external experts.

This structured scenario approach made it possible for our group to derive targeted and practical recommendations for courses of action in cyber security governance.

_ FELLOWS OF THE GLOBAL CYBER SECURITY GOVERNANCE WORKING GROUP

Puja Abbassi

is a PhD candidate at the University of Cologne, where he works on a project that focuses on IT-assisted security in food supply chains (funded by the German Federal Ministry of Education and Research). He is also a research associate at the Research Center for Global R&D Management (GLORAD). There, he covers the globalization of scientific journals. Puja's research interests include the influence of diversity and social capital on startup and venture capital success. Prior to starting his PhD, Puja worked as a visiting researcher for GLORAD at Peking University in China. He also worked on social network analysis projects as a research assistant at the Department of Information Systems and Information Management at the University of Cologne. His non-academic experience includes advising and working for start-ups and companies in the web, mobile and communication industry. Puja graduated from the University of Cologne with a degree in information systems and holds a certificate in Chinese studies from Beijing Language and Culture University.

Martin Kaul

is policy advisor to the speaker on climate policy of the Green Group in the Parliament of the Federal Republic of Germany in Berlin, where he works in the field of climate change as well as the German energy transition (Energiewende). Previously he has been head of office to the chairboard of the Green Group in the State Parliament of Berlin, where he was involved in finding political answers to pressing challenges – such as climate change or sustainable energy supply in the context of a metropolis. Martin has also worked for the head of the German Green Party on a number of international issues, such as climate change, energy security and international cooperation. In addition to being the author of political travel reports, Martin has published several articles on international topics, including his master's thesis, which focused on water-related conflicts and the merging of security and development. Martin holds a bachelor's in international relations from the Dresden University of Technology in Germany and St. Petersburg State University in Russia. He earned a master's in contemporary war and peace studies from the University of Sussex.

Joachim Knodt

Joachim Knodt joined the German Federal Foreign Office in 2011 and is currently working for the International Cyber Policy Coordination Staff. Before becoming a diplomat, he worked for the Google Policy Team in Berlin and was the assistant to the executive board at the Roland Berger Foundation. Prior to joining the foundation, he worked as a consultant for Roland Berger Strategy Consultants on different projects in the public and the private sector. For over two years, he supported the High Level Group of Independent Stakeholders on Administrative Burdens in Brussels, chaired by Edmund Stoiber. Joachim gained his first working experience as a Carlo-Schmid-Fellow working on public administration reform at the OSCE in Sarajevo, and as a student assistant at the European Parliament in Strasbourg. He was an election observer for the European Union and the OSCE in Georgia, Moldova and Guinea. Joachim received his academic training in France, Germany and Poland. During his

studies, he was awarded a scholarship by the Friedrich-Ebert-Foundation. He holds master's degrees in European studies from the College of Europe (Natolin, Poland) and in public administration from the University of Potsdam. In addition, Joachim is a certified foundation's manager from the European Business School in Oestrich-Winkel.

Vivek Mohan
is a fellow with the Project on Technology, Security, and Conflict in the Cyber Age at the Harvard Kennedy School's Belfer Center for Science and International Affairs. His writing and teaching focuses on privacy, surveillance, Internet governance and national security. Prior to joining the Belfer Center, Vivek was an attorney at Microsoft's Innovation & Policy Center in Washington, DC, where his work centered on telecommunications and cyber security policy. Vivek held a special appointment with the Internet Bureau of the New York State Office of the Attorney General, where he led several cyber fraud investigations. Vivek received his JD from Columbia Law School, where he served as an articles editor for the Columbia Science and Technology Law Review. Vivek received his bachelor's in economicsmagna cum laude from the University of California, Berkeley.

Yi Shen
is a lecturer in the Department of International Politics at Fudan University and heads up the university's newly established Center for Media Revolution and Governance. After receiving his PhD in 2005, he expanded his research to include cyber-related issues. Since 2009, Yi has conducted research on the interaction between information technology and diplomacy, with an emphasis on the latest developments in Iran, Tunisia, Egypt, China, Libya and other countries. Yi has written about 50 short commentary pieces for newspapers, including the Global Times and Wen Hui, and has published several academic papers analyzing America's cyberspace strategy. Yi holds a PhD from the Department of International Politics in the School of International Relations and Public Affairs at Fudan University.

Zev Winkelman
is an associate policy researcher at RAND Corporation in Washington, DC. His areas of research include international cooperation regarding cyber security, nuclear security and counterterrorism. These interests have provided Zev with opportunities to do research in Russia, Germany and Israel. In addition to experience with global security research, Zev has several years of experience in the global financial markets, working with risk management in currency trading operations and high frequency equities trading strategies. He received his master's in forensic computing and counterterrorism from the John Jay College of Criminal Justice, and both a BSE in computer engineering and a BGS in general studies from the University of Michigan. Zev recently received his PhD from the Goldman School of Public Policy at the University of California, Berkeley. His dissertation focuses on the use of structured analytic techniques to improve policy analysis, using debates on the balance between civil liberties and security as a case study.

WWW.GG2022.NET