TOWARDS A GLOBAL FRAMEWORK FOR CYBER PEACE AND DIGITAL COOPERATION: AN AGENDA FOR THE 2020s

edited by
Wolfgang Kleinwächter, Matthias C. Kettemann and Max Senges with Katharina Mosene

Prefaces by
António Guterres, UN Secretary-General, and the "Father of the Internet", Vint Cerf

Internet Governance Forum Berlin

25–29 November 2019

IGF BERLIN 2019

TABLE OF CONTENTS

PARLIAMENT

PRIVATE SECTOR

CIVIL SOCIETY

ACADEMIC COMMUNITY

TECHNICAL COMMUNITY

PART 2: ISSUES

CYBERSECURITY

DIGITAL ECONOMY

HUMAN RIGHTS

ANNEX

WELCOME MESSAGE

Thomas Jarzombek, Commissioner for the Digital Industry and Start-ups and Federal Government Coordinator of German Aerospace Policy

The 14th UN Internet Governance Forum in Berlin 2019

Dear reader,

Germany is proud and honoured to host the Internet Governance Forum (IGF) this year. Together with the IGF's Multistakeholder Advisory Group appointed by the Secretary-General of the United Nations, we have given this year's IGF the title "One World. One Net. One Vision." The intention is to stress the aspects the international Internet community share in common and to develop globally accepted solutions to today's and tomorrow's challenges. What solutions exist for functioning competition between large and small/medium-sized enterprises in the platform economy? How can we protect ourselves against attacks on the integrity of the Internet and its content whilst upholding data privacy and freedom of opinion? How can we succeed in maintaining and developing the global nature of the Internet with its emphasis on human rights – keeping it interoperable and freely accessible? What role does the Global South have in all of these developments, and how can we work together to increase its participation? These are just a few of the questions being discussed at this year's IGF in the three major thematic fields of "data governance", "safety and security" and "inclusion".

I believe it is important not to allow our busy day-to-day lives to prevent us from looking ahead and thinking about what shape the Internet should take in the coming years and decades, and how the governance structures need to be designed. I therefore welcome the process on the future of digital cooperation launched by the Secretary-General of the United Nations, the first outcome of which was the report published by the panel in June. Germany supports the findings of the report and will particularly work to ensure that the idea of an "IGF plus", improved and adapted to meet the new challenges, is pursued further. We will play an active role in this process.

This compendium also looks to the future, and the editors have succeeded in gathering a broad spectrum of views and opinions on all the issues of relevance to the future of Internet governance in the 21st century. It thus serves as an excellent vademecum for the participants at this year's IGF which can continue to be used in future as a source of inspiration and ideas for the crucial debate on Internet governance in the coming years and decades. For this reason, the Federal Ministry for Economic Affairs and Energy quickly decided to support the volume with a substantial sum.

Thomas Jarzombek

PREFACES

António Guterres is Secretary-General of the United Nations

Internet governance must lead to policies that improve lives

From its earliest days, the internet has involved academic researchers, government entities, private companies and networks of engaged individuals. Today's internet is vastly different in scale, but the diversity of actors remains the same; it is a place where people from across the world can come together to collaborate in seizing the benefits of transformative information and communication capacities.

It is in this spirit of multi-stakeholder collaboration that the Internet Governance Forum emerged from the 2005 meeting of the United Nations World Summit of the Information Society. Supported by an intergovernmental body and overseen by an advisory group, the IGF provides a platform for rich discussion among private sector representatives, government ministers, technology leaders and civil society groups.

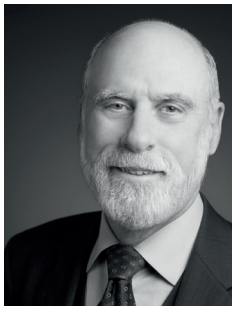
Internet governance must lead to policies that improve lives. We cannot leave our fate in the digital era to the invisible hand of the market force. At the same time, classical approaches to regulation do not easily apply to a new generation of technologies. Non-traditional, multilateral and multi-stakeholder cooperation will be crucial.

Policy-setting and cooperation among actors in the digital space have not kept pace with the impact and implications of new technologies. Digital advances touch the economy, human rights, national security and much else, yet discussions can often be siloed.

In June of this year, the High-level Panel on Digital Cooperation that I convened put forward wide-ranging recommendations that point the way towards a shared digital future of safety and opportunity for all. One of the Panel's recommendations calls for an enhanced IGF.

The thoughtful work contained in this book underscores the need for a holistic approach to internet governance, and for an effective and inclusive multilateralism that advances the well-being of all. I look forward to working with all partners towards securing a more prosperous and peaceful digital future.

AN AGENDA FOR THE NEXT DECADE



Vinton G. Cerf, widely considered one of "the fathers of the Internet", is VP and Chief Internet Evangelist at Google. He helped found ICANN and was Chairman of its Board from 2000 to 2007. The recipient of many honorary degrees he has been awarded, inter alia, the National Medal of Technology, the Turing Award and the Presidential Medal of Freedom.

The third decade of the 21st Century is imminent and we find ourselves contemplating an extraordinary range of opportunities and challenges. The Internet has reached an estimated 50% of the world's population and this percentage is expected to increase with the rapid spread of 4G and 5G mobile and switching technologies. Vastly higher access speeds are anticipated in both wired and wireless modes. Undersea cables are being laid at a furious pace. Extremely ambitious plans are already unfolding for literally tens of thousands of low and very low Earth orbiting satellites that may make Internet access almost inescapable even at the poles of the planet! Added to that is an expected avalanche of programmable and networked devices sometimes called the Internet of Things.

Meanwhile, it seems as if new applications of machine learning arrive daily, lending credibility and utility to speech recognition and understanding. Even though the exchanges are relatively simple, they result in answers to questions, control of household and office devices, translations among languages and natural sounding speech generation. Moreover, the same general purpose machine learning tools result in successful image analysis applied to medical diagnosis and scene analysis, facial recognition and support for autonomous vehicles.

As one of the early developers of what is called the Internet, I have watched it evolve from an experiment sponsored by the US Defense Department to a globe girdling system driven by a wide range of private and public sector actors using a range of business models. Moreover, the advent of the World Wide Web application unquestionably triggered a tidal wave of new developments leading to massive generation and sharing of information, ease of discovery through search engines and new businesses bolstered by the arrival of smartphones and their "apps" in 2007. This vast, rich, and fertile infrastructure has given rise to millions of applications, hundreds of thousands of new businesses, billions of users, and GDP growth not seen since the late 19th and mid-20th Centuries.

As this technology has become readily available to the general public, private sector and governments, there has been a concomitant rise in abuse ranging from fraud, the spread of misinformation and disinformation, social turmoil, identity theft, use of digital technology to commit old and new crimes, harmful behaviors, security risks, loss of privacy and a laundry list of other ills. We should not be surprised at this. Any new, disruptive technology brings with it the potential for emergent behaviors and phenomena exhibiting beneficial and harmful characteristics. Human nature and its strengths and weaknesses give rise to both sides of a tidal wave of change. On the positive side, the Internet and World Wide Web have unleashed constructive uses that would have been unthinkable even twenty years ago. Massive amounts of information can be searched in milliseconds. Games and movies and other entertainments are discoverable and accessible on demand. Goods and services can be ordered and delivered in real time in some cases and overnight or within a few days in other cases.

These benefits and deficits manifest wherever the Internet is accessible and because the Internet is essentially insensitive to crossing of jurisdictional boundaries, the phenomena are apparent on a transnational basis. It is precisely for this reason that activities such as the Internet Governance Forum have been created. The global forum has spawned national and regional forums in aid of discussions with more local focus. A wide range of issues have been catalogued in these meetings and have spawned a range of institutional and documentary responses, some of which are referenced in the appendices to this book.

Since the first meeting of the Internet Governance Forum in 2006, the attendees have worked hard to articulate the benefits and risks of widespread Internet use. As the 2020s approach, it is apparent that the multi-stakeholder discussion that has informed the IGF must advance from discussion to a more action-oriented agenda. Having identified problems and issues, the IGF needs to enable and empower its secretariat to monitor and report on progress toward solutions and resolutions. While the IGF is not likely the correct forum for problem solving, it can become an instrument to highlight successful initiatives and draw attention to areas still in need of attention.

What might an agenda for problem solving include? In the absence of enforceable treaties to deal with harmful behaviors undertaken through Internet enabled applications, one might begin to formulate norms for digital behavior that might someday become the basis for treaties. The Global Commission on the Stability of Cyberspace has taken that approach and documented a number of recommendations. The Secretary-General of the United Nations established a high level panel on digital cooperation which has delivered its final report that has triggered an initiative to engage in dialogue aimed at establishing constructive and cooperative multi-stakeholder efforts towards solutions. Better inter-jurisdictional cooperation among law enforcement agencies and the identification and apprehension of criminals using the Internet can increase safety and security of the general public and institutions of all kinds.

I am concerned that the demonstrated benefits of an open, accessible and fully connected Internet will be eroded by government actions intended to protect against abuse but which may have the ancillary side-effect of fragmenting the Internet, eroding human rights and stifling innovation. The Internet Governance Forum and other organizations with a stake in the continued utility of the Internet must stand against this erosion of the Internet‘s nature and promise by helping all stakeholders to understand the potential impacts of hasty or ill-considered actions to counter abuse. We have arrived at a time when the adoption of principles must now be augmented with implementable norms and ultimately enforceable international treaties that strike the requisite balance between freedoms and human rights and harmful behaviors that create unacceptable social and economic deficits.

The technical and academic community has a major role to play in all of this. Software and hardware design practices are needed that increase the security, safety and utility of the Internet and its applications. Guidance for user education and operational practices are needed to make effective some of the technical solutions such as strong, two-factor authentication, cryptographic protection of confidentiality, software update practices and responses to the brittleness of machine learning tools and applications. While open source software and hardware design have been powerful mechanisms for propagating best practices, the safety and security of these open source offerings can be questioned. When everyone is theoretically in charge of vetting for quality and bug discovery, no one is in charge. Consequently, widespread use of open source in products and services may well propagate unexpected and exploitable vulnerabilities and even deliberate malware into the ecosystem. A regime of accountability for quality assurance is sorely needed as our daily lives become dependent and interdependent on an increasingly complex and potentially fragile infrastructure. Incentives such as “bug bounties” can help. Hoarding of “zero day” exploits for purposes of offensive use should not be permitted to become the norm.

An agenda that contributes to the safety, security, reliability and usability of the Internet and its applications should be the order of the day for all stakeholders and the IGF can be one means to deliver that message widely and effectively.

Source

[1] https://cyberstability.org.

[2] https://www.un.org/en/digital-cooperation-panel.

INTRODUCTION AND ACKNOWLEDGEMENTS

Wolfgang Kleinwächter, Matthias C. Kettemann and Max Senges

The title is the message: We live in the age of „digital interdependence“, says the Final Report of the UN High Level Panel on Digital Cooperation (HLP.DC). Since the days of the UN World Summit on the Information Society (2002 – 2005) the world has changed. Two decades ago, we discussed the Internet revolution. This was seen more as a technical issue with some political implications. Today, digitalization has penetrated all areas of life and there is less and less difference anymore between offline and online. Cyberspace is everywhere.

The UN High Level Panel has opened our eyes, rocked our minds and invited us to discuss the future of the world at the eve of the third decade in the 21st century. The 2020s will be crucial to build a people centered information society. In 2025, there will be the second WSIS Review Conference (WSIS +20). 2030 marks the target year of the sustainable development goals (SDGs).

In our eyes there are three issues for #NextGenerationInternetGovernance, which are in the center of the discussion:

1. How to organize a holistic approach to Internet Governance, taking into acocunt the interdependence of stakeholders and the interdependence of sectors.
2. How to combine multilateralism and multistakeholderism in global Internet policy making.
3. How to enhance global mechanisms to frame the future development of digital cooperation.

In the Internet there is no single solution, no „silver bullet“. With this publication we want to show a broad variety of different approaches and opinions. This could help to broaden our minds, to deepen our understanding and to contribute to the way forward.

When WSIS established in its Tunis Agenda (2005) the Internet Governance Forum (IGF), the basic idea was to create a discussion space for all the new cyber and digital issues to enable decisions makers to find sustainable solutions in the various international, regional and national institutions, which have a mandate to take such decisions.

The idea has worked. The IGF is a success, even if there is plenty of room for improvement. The 14th IGF in Berlin (November 2019) will be another opportunity to look deeper into the still widely unknown territory of cyberspace.

The editors of this book were guided by the two basic ideas of the UN report: the Multistakeholder and the multidisciplinary approach. We have structured the report in two parts: On the one hand we have invited representatives from various stakeholder groups – government, parliament, business, civil society, technical and academic community – to comment on the report. On the other hand, we have asked experts from the three big „baskets“ of the Internet Governance Ecosystem – cybersecurity, digital economy and human rights – to reflect about the report. And we added our own proposition, how cyberpeace and digital cooperation can be enhanced in the 2020s.

In it, we develop the contours of a new normative order of the digital with good rules for a better Internet: Relying on the formative power of norms within our digital ecosystem, we develop a multitiered approach to a #NextGenerationInternetGovernance. Technology, we argue, influences our behavior, but the focus on code and standards as ‘telling us what to do’ can be reoriented through our value-based normative approach. Rather than letting actors within the Internet Governance realm instrumentalize security or let profits dictate policy, our approach holds the promise of sustainable digitalization and digital sustainability. Based on a forward-looking reading of the UN Secretary-General’s High-level Panel on Digital Cooperation we call for a #NextGenerationInternetGovernance to emerge over the next decade. It should be comprised of four loosely coupled, interdependent and mutually reinforcing governance frameworks - on peace, economy, rights, and AI - to be bootstrapped at and facilitated by the IGF. We propose to make Internet governance work for all through four interlinked policies: an **#OnlinePeaceFramework** (Digital Peace Plan), a **#DigitalMarshallPlan** (Digital Sustainability Agenda promoting inclusive economic growth and sustainability through internationally coordinated technology policy frameworks), **#OnlineRights4all** (A Digital Human Rights Agenda), and **#ResponsibleAIStewardship** (framework for future-proofing the research, development and deployment of AI based on a human being-oriented conception of technology and established Internet governance norms).

All contributions are extremely valuable perspectives on the IGF and Internet Governance. To get just a first taste of the many crucial contributions to the

future of Internet governance this book has to offer, consider (among many others) these selected arguments:

Vint Cerf, one of the fathers of the internet and Internet Governance, opens the discussion asking for new solutions that don't require regulation or treaties but instead rely on practice guided by transnational norms as discussed e.g. in the Commission for Stability in Cyberspace. In line with this book's editorial he also lists several areas where the IGF could be significantly improved; namely (1) identification of problems; (2) reporting on progress of solutions and (3) recommendations for venues to tackle problems and possibly creation of new ones.

ITU Secretary General, Houlin Zaho, elaborates on the historic and current leading role of the ITU as a multilateral, multistakeholder and consensus based institution, that drives UN efforts in ICT for SDGs and a just information society.

Amadeep Singh, one of the Chairs of the UN High Level Panel, discusses the opportunities that new technologies like the internet and AI create for us to make a new start at international governance with. He recommends to root governance development deeply within networks of practice (e.g. health or finance) in order to make them more meaningful for communities of practice and enable smart learning loops, moonshots and leapfrogging.

Guy Berger, one of the originators of UNESCO's work on Internet Universality and the ROAM (Human **R**ights, **O**penness, **A**ccess and **M**ultistakeholder) principles, elaborates on how these tools can be used by UNESCO and its member states to evolve next generation internet governance.

Marietje Schaake, a former Member of the European Parliament and now Stanford Cyber Policy Center's international policy director, calls for a "serious reality check". We've talked the talk: between "Magna Carta, Social Compact, New Deal or Geneva Convention Online" there will soon be "no more big words unused". Multi-stakeholder gatherings, she argues, should focus less on new processes, statements, and more on results and enforcement. The time has come "to move beyond words: The IGF is the perfect moment for a reality check and some tough love."

German parliamentarian and Chair of the Digital Agenda Committee, Jimmy Schulz, urges and organizes a deeper integration of parliamentarians into internet governance and the IGF in particular. He calls for us to find courage and to team up in a movement for digital Enlightenment aimed at liberating people from their "self-imposed immaturity".

Anriette Esterhuysen from the Association for Progressive Computing (APC), one of the longest true civil society stakeholders with deep expertise in ICT4D and Human Rights, stresses in her piece that states should live up to their responsibilities and use all stakeholders to guide them. Multistakeholder Governance only complements this traditional approach.Several areas of good practice and challenges are discussed and thee IGF is identified as the best mechanism to evolve and tackle next generation internet governance.

Anette Mühlberg from the German Trade Union ver.di refers to the consequences of global digitalization for the future of work. Artificial intelligence will affect the way we work and live and she refers to the receommendations of the ILO Global Commission on the Future of Work and the G20/OECD principles, which should guide the development and deployment of Artificial Intelligence.

Thomas Schneider, former ICANN GAC Chair as well as WSIS, IGF and EURODIG veteran, puts forward learnings from Switzerland's history that apply to the IGF and Internet Governance. Increased differentiation and interdependence in the global information society requires a strong United Nations that fosters peace and cooperation. The recommendations by the High Level Panel can be combined and refined to set the right incentives to enable hard but productive decisions that balance competition, solidarity and voluntary compromise.

Carlos Afonso, one of the architects behind one of the most successful practical implementations of Multistakeholder Internet Governance at the national level in Brazil, shares his well grounded views on how multistakeholder and multilateral initiatives need to build on each other. While he sees improving the IGF as the way forward, the concrete measures of improvement need to be worked out further.

Lynn St. Amour is the current Chair of the IGF's central Multistakeholder Advisory Groups. She urges all stakeholders to focus on improving the IGFs impact and support, together as well as on actionable outcomes by soliciting and addressing the interests and needs of stakeholder (practice) communities.

Robin Mansell, one of the top academic thought leaders in media governance at the London School of Economics, asks a very difficult and important question that is at the center of developing a next generation cyber governance: which services are offered by public institutions and which by private companies.

Jonathan Zittrain from Harvard‘s Berkman Klein Center reviews the evolution of governance of the digital space from the early era focused on user rights to the current focus on avoiding user harm and ensuring „public health“ (online). Asking stakeholders to synthesize both perspectives, he is looking for us to develop the ideas and institutions of #NextGenerationInternetGovernance to be legitimate because of the inclusive an deliberative and, where possible, federated arrangements that resolve challenges in a dynamic equilibrium of interests.

Wolfgang Ischinger, Chair of the Munich Security Conference, which is one of the pioneering world leader fora for deliberation about international (cyber) security, makes the key point that multistakeholder governance is the only viable approach, but that trust between actors needs a shared understanding of the problem space both on the expert technical level as well as on the strategic political level. He also highlights the various innovative Cybersecurity initiatives that were started in the last years.

Christoph Steck from Telefónica builds on the company‘s New Digital Deal report published not long ago. His pitch is to engage in more agile, transparent, transnational cooperation to implement the New Digital Deal for more human-centric digitization envisioned by his company.

And finally Bill Drake, who has been an eminent analyst and advisor since WSIS and throughout the IGF‘s history, summarizes and weighs in on the viability of the main aspects of the IGF Plus proposal. He especially stresses the need for the IGF as information clearing house.

In conclusion, we would like to thank Katharina Mosene for her fantastic editorial support. We also would like to thank the German Ministry for Economic Affairs, and in particular Rudolf Gridl und Heiko Wildner, for their support. We also wish to thank Google for making this book possible.

PROLOG

The following statements were given at the presentation of the UN High Level Panel on Digital Cooperation and transcribed from the video recordings.

Statement at the launch of the Final Report, New York, June 10, 2019

Melinda Gates, Co-Chair of the UN High Level Panel on Digital Cooperation

"The future is being created literally every day and it's changing. It's changing so fast, we can't predict where digital is going to take us 30 years from now."

"[In the panel] we talked about the incredible opportunities that technology gives us in the future to create the world that we want: a more just and humane world. And we also talked about some of the downsides and we started to ask: What needs to be done to create the future we want? ..."

"The Internet should be for everybody but today it's not; women are 40% less likely around the world to have access to the Internet and so we have to look at special programming for women."

"We need to be investing in human capital and infrastructure. But infrastructure today is not just roads and water and electricity, those things are absolutely important, we still need to push those; but it also means access to information ..."

"Our exciting panel [enquired how to make]]human-centered design fit the digital future, how do you make it inclusive, so that it really changes everybody's life so that we can imagine a future in 2030, where all people are digitally connected. I keep going back to an example of a woman. So many women who are marginalized and pushed to the edges of society, who are out in remote places, when they have access to a digital phone, they can reach for help, they will tell you saving a dollar a day or two dollars a day, they have power in their family ... ."

"There are concerns for good reason. We all have a right to our privacy and to our data but there are challenges and misuse. But what you're seeing is that the tech sector comes together, [like in] artificial intelligence. They are working together to say what are the standards we want to use for AI, what's the transparency we want to have for AI and they're starting to self-govern. ... We need smart regulation around that."

Source
https://www.youtube.com/watch?v=UcB_aIq1OwA

Statement at the launch of the Final Report, New York, June 10, 2019

Jack Ma, Co-Chair of the UN High Level Panel on Digital Cooperation

"It is a great honor to get involved because this digital age ... will be with us the next 30 to 50 years. We had a great panel and people from different backgrounds. ... I think it's important that we should not worry about the future. Nobody is an expert of the future, we should learn, we should embrace it and we should change our mentality to embrace this revolution and have confidence in ourselves. There are problems, but we can solve the problems when we work together and face this challenge. It's the cooperation between governments, small businesses and technology companies and even universities, that changes the way of thinking."

"I think the most important element of this digital period is inclusiveness. It helps women, helps small businesses, helps developing countries. ... For my site we have over 10 million small businesses selling on our site .... Nobody really cares about whether you're a woman or a man, whether you are well educated or not, as long as your product is good. Woman can do much better jobs on the Internet because this is not an arena of competition of muscles, it's a competition of the heart, brain and wisdoms. Today small businesses can compete everywhere with anybody. In the digital age small is beautiful and small is powerful."

"It's just the beginning. ... globalization is not inclusive enough."

"On privacy, not only government should [be concerned]. Business should be worried as well. If the private sector thinks about jobs, about inclusiveness, about the security and privacy, your company will be sustainable, will be welcome in this century. Otherwise you'll be out. If you do not pay attention to privacy, you do not pay attention to data security, if you do not pay attention to human rights, if you do not pay attention to the interest of the society you will disappear also very quickly. I think in the digital age big companies means big responsibility – the bigger you are the bigger responsibility you have."

"I think this report is just a beginning. ... [Today] we teach our kids to memorize, to calculate faster, to learn facts. But the next generation needs an enabling education system. The young people have to understand the digital age. Let´s adjust our educational system".

"There is a difference between information technology and digital technology. IT makes your stronger, but DT is empowering others. If you want to be successful in the digital age, you have to empower others. ... Every technology company should do good things."

Source
https://www.youtube.com/watch?v=UcB_aIq1OwA

From digital independence to digital interdependence

Jovan Kurbalja

At a time when everything is digital and every aspect of our society, including how we communicate, socialise, make decisions, work and ultimately live is influenced by technology, the notion of digital interdependence becomes all the more relevant.

It is in this spirit that the UN Secretary-General established the High-Level Panel on Digital Cooperation (Panel) in July 2018. The Panel was tasked to "address the social, ethical, legal, and economic impact of digital technologies in order to maximise their benefits and minimise their harm." Under the co-chairmanship of Melinda Gates and Jack Ma, 20 members of the Panel engaged in intensive consultations with governments, the tech industry, and local communities worldwide.

In June 2019, the Panel issued its Report titled 'The Age of Digital Interdependence' with the following five set of recommendations.

Firstly, the Panel recommends that 'by 2030, every adult should have affordable access to digital networks, as well as to digitally-enabled financial and health service'. It is with this recommendation that the Panel attempts to fill in the gap in the 2030 Agenda that failed to dedicate a specific sustainable development goal (SDG) to digital technology. In truth, digital technology is only briefly mentioned in SDG 9 (Industry, Innovation and Infrastructure), target c, which in essence calls for increased access to ICTs and affordable access to the Internet in least developed countries by 2020.

This recommendation that could also be regarded informally as the 'digital SDG' allows the Panel to set the stage for a holistic mainstreaming of digital technology in the 2030 Agenda. As a practical first step, the Panel proposes the creation of a digital public goods sharing platform, and endorses digital inclusion and equality of women and other traditionally marginalised groups. The Panel also calls on the stakeholders to agree on a set of metrics for digital inclusiveness.

The second recommendation focuses on the development of human as well as institutional capacities of governments, civil society, and the private sector. The Panel proposes the establishment of regional and global digital help desks as practical mechanisms for fostering, coordinating, and implementing capacity development activities.

The third set of recommendations addresses the issue of human rights and human agency in the digital age. The Panel proposes an agencies-wide review of how existing international human rights accords and standards apply to new and emerging digital technologies. It recommends that this evaluation is conducted with the inclusive participation of civil society, governments, the private sector and the wider public. Furthermore, it goes on to underline that "life and death decisions should not be delegated to machines". In this set of recommendations, it also encourages multistakeholder digital cooperation on the design of standards and principles for future AI developments. To this end, the Panel highlights a few guiding principles and approaches, namely, explainability of AI code, human accountability in AI, as well as respect of transparency and non-bias in use of AI system. The Panel also calls for action in order to address human rights violations on social media platforms, in particular those concerning children.

The fourth recommendation on trust, security and stability calls for the establishment of a Global Commitment on Digital Trust and Security which should complement the existing digital-related processes such as the UN Governmental Group of Experts (UN GGE), the UN Open Ended Working Group (OWEG), and regional cybersecurity initiatives.

The fifth and the final set of recommendations is dedicated to digital governance which was one of the main underlying reasons for the establishment of the Panel's mandate. The Panel frames digital governance in the context of shared values, principles, understandings, and objectives that should be outlined in a "Global Commitment for Digital Cooperation". The Panel proposes the UN's 75th anniversary in 2020 as an adequate date for the adoption of the Global Commitment. Moreover, the Panel introduces the following three models as the basis for the discussion of governance mechanisms: Distributed Co-Governance Architecture (COGOV), the Internet Governance Forum Plus (IGF+), and the Digital Commons Architecture. Lastly, the Panel underlines that the digital governance processes should be strengthened by the appointment of the UN SG's Technology Envoy, an option that the UN Secretary General said he will explore in his Strategy on New Technologies.

Discussions on these and other functions and models for digital cooperation will most likely dominate in the post-Panel dynamics. In fact, the Panel's report along with its recommendations only marks an important step on the long journey ahead.

Answering digital policy calls – Proposals from the UN High-Level Panel on Digital Cooperation

In June 2019, the UN Secretary General's High-Level Panel on Digital Cooperation presented a set of recommendations on sustainable development, human rights, cybersecurity and other aspects of digital cooperation in its report titled 'The Age of Digital Interdependence'. In particular, the Panel sought to address the growing number of calls from citizens, companies, and governments worldwide for strengthening of digital governance. The two most recent ones, which are even calls by title, are the Christchurch Call[4] issued by New Zealand and France to eliminate violent terrorist and extremist content online, and the Paris Call[5], issued by over 100 governments and companies to strengthen trust and security in cyberspace. In order to address the issue of digital governance, the Panel built on more than a 1000 mechanisms ranging from standardisation instruments used by, among others, the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU) to guidelines and self-regulation tools used by the tech industry and their associations. It also reviewed legislation, treaties, and other legally binding mechanisms employed by governments and international organisations.

The Panel employed the 'form follows function' approach in order to ground governance proposals in digital reality, policy sensitivities and practical needs of actors and communities worldwide. It conducted its deliberation through a number of steps including: spotting gaps in the existing governance mechanisms, outlining the values that governance should support, identifying the core governance functions, and, lastly, landing all of them in three models for digital governance and cooperation.

Gaps

The Panel identified, among others, the following main gaps in the current digital governance:

- A relatively low place on many national, regional and global political agendas of digital technology and digital cooperation issues.
- Weak level of inclusion, in particular, of small and developing countries, indigenous communities, women, young and elderly, and those with disabilities in digital cooperation arrangements.
- Overlap, high complexity and ineffectiveness of mechanisms covering digital policy issues.
- A relative lack of reflection of the cross-cutting nature of digital technology in traditional policy work.

- Lack of reliable data, metrics and evidence on which to base practical policy interventions.

Key Principles

The Panel listed the following main principles and characteristics which should respond to digital governance gaps: consensus-orientedness, polycentricity, customisation, subsidiarity, accessibility, inclusiveness, agility, clarity, accountability, resilience, openness, innovation, tech-neutrality, and equitability in outcomes.

Key Functions

Once it identified the gaps and key principles, the Panel listed the core ten functions that digital governance architecture should perform: leadership, deliberation, inclusivity, provision of evidence and data, norms and policy making, implementation, coordination, partnership, support and capacity development, conflict and crisis management.

Governance Models

Lastly, the Panel proposed the following three governance models which should address the above described gaps, support values and principles, and perform core governance functions:

- Internet Governance Forum Plus (IGF+)
- Distributed Co-Governance Architecture (COGOV)
- Digital Commons Architecture (DCA)

At a time when there is no appetite for new multilateral mandates, one of the main strengths of the IGF Plus proposal is that it could build on the existing mandate provided by Article 72 of the 2005 Tunis Agenda for the Information Society.

In addition, the IGF Plus uses an evolutionary approach by:

- building on the achievements of the existing IGF process: gender balance (difficult to achieve in the digital field), innovative working methods, and a well-developed network of national/regional IGFs; and
- addressing major weaknesses of the IGF such as a lack of actionable outcomes, lack of dedicated discussion tracks for governments and other stakeholders, and limited participation of actors from small and developing countries.

The IGF Plus would consist of: Cooperation Accelerator, Policy Incubator, Observatory, Help Desk, and Advisory Group.

The **Cooperation Accelerator** would connect as many dots in the digital policy space as possible by bringing forth a multidisciplinary approach and by including diverse perspectives from across the policy spectrum. It would improve and accelerate the cooperation between different events and processes covering the same issues such as AI, cybersecurity or data. With better coordination, organisers of parallel processes could become, at the least, aware of each others' activities, and at best, specialise in specific coverage of certain aspects including ethics, security, standards, and data, to name a few, of complex matters such as AI.

The **Policy Incubator** would provide the right environment to develop, monitor, and adjust policies and norms in an expedient manner. For instance, after receiving requests for action such as the Christchurch Call or the Paris Call, the Policy Incubator would identify whether existing regulations could be applied or adjusted to take prompt action. In many cases, the existing rules would suffice. However, should there be a gap the Policy Incubator would develop new solutions in an evidence-based and transparent manner that could be used by governments, tech companies, and international organisations as an input for their policy and regulatory activities. The Policy Incubator would not itself adopt legally binding rules.

Lastly, an Observatory and Help Desk would be established to improve and increase coordination and information-sharing, and to provide more efficient capacity development in the digital policy realm. The highly decentralised structure of the IGF Plus would be co-ordinated by an **Advisory Group** gathering leaders from the tech industry, governments, academia, and civil society. To ensure legitimacy and success, it would be desirable that the Advisory Group is chaired by, or in close involvement with, the UN Secretary-General.

The main weakness of the IGF Plus proposal is its name. Digital policy has moved beyond the core Internet issues towards policies on data and artificial intelligence. Since 'digital' is a common denominator for all of them, the most appropriate name for the IGF Plus would be the Digital Cooperation Forum or even the Digital Cooperation Council.

Whereas the IGF Plus proposal is the most mature and closest to the digital reality, the COGOV and DCA proposals also provide useful building blocks for governance in the digital policy space.

The COGOV would foster new cooperation networks which would help find innovative solutions that governments and other stakeholders could

immediately utilise. The DCA would establish dedicated tracks to support sophisticated and efficient communication on individual issues between all relevant actors, with particular attention given to the promotion and realisation of SDGs. In all three proposals, there is a definitive aim to streamline deliberations in order to deliver prompt and evidence-based policy actions.

History has shown us time and time again that the only way to make real progress on global issues is through global cooperation. After decades of experiments and academic discussion on digital governance, it is now time for consolidation and action. The next stop on this journey is the 14th IGF in Berlin , where the Panel's recommendations will be discussed and the digital governance architecture should start emerging.

Source

[4] *https://dig.watch/newsletter/may2019.*
[5] *https://www.diplomacy.edu/blog/table-paris-call-trust-and-security-cyberspace.*
[6] *https://dig.watch/events/14th-internet-governance-forum.*

Implementing Sustainable Digital Cooperation: Towards a #NextGenerationInternetGovernance for the 2020s

Matthias C. Kettemann, Wolfgang Kleinwächter, Max Senges

Based on a forward-looking reading of the UN Secretary-General's High-level Panel on Digital Cooperation we call for a #NextGenerationInternetGovernance to emerge over the next decade. The "New Deal" on Internet Governance in the 2020s should be comprised of four loosely coupled, interdependent and mutually reinforcing governance frameworks – on peace, economy, rights, and AI – to be bootstrapped at and facilitated by the Internet Governance Forum (IGF). In all, this paper aims to kick-start critical deliberation on responsible stewardship of the internet's public goods and innovation, or in political terms principled and inspiring Internet governance for the future (#IGforTheFuture). In short: To make Internet governance work for all we need.

- an **#OnlinePeaceFramework** (Digital Peace Plan),
- a **#DigitalMarshallPlan** (Digital Sustainability Agenda promoting inclusive economic growth and sustainability through internationally coordinated technology policy frameworks),
- **#OnlineRights4all** (A Digital Human Rights Agenda), and
- **#ResponsibleAIStewardship** (framework for future-proofing the research, development and deployment of AI based on a human being-oriented conception of technology and established Internet governance norms).

Setting the scene

The UN Secretary-General's High-level Panel on Digital Cooperation has recently submitted its report on the relevance of internet governance policies that are informed by interdependence and oriented towards ensuring an inclusive digital society and economy for all. In this editorial we reflect on the proposals, potentials and challenges covered in the report and complement the panel's approach with draft normative elements for a next generation internet governance regime. Our proposals are meant to stimulate the debate and inform new normative approaches to evolve the public value that can be harvested from internetworked technology. While the normative path is yet uncharted, we assess that the ideal place to start the journey towards a

global future-proof and resilient internet governance regime is the Internet Governance Forum (IGF), beginning with this year's multistakeholder gathering in Berlin in November. The IGF is ideally suited to host these strategic global deliberations as well as to evolve and bootstrap the practices and institutions that must unfold over the next decade.

Solving the Internet governance puzzle

The year 2020 is almost here. **The importance of the Internet's integrity** – its security, stability, robustness, resilience and functionality – has been recognized, in documents from states, international organizations, corporations and civil society, and lately by the UN Secretary-General's High-level Panel on Digital Cooperation, **as paramount to national and international practice communities from finance, to transnational communications infrastructure, national defense and national and international energy networks to name only a few examples of the nexus of infrastructure internet applications.** But as the political field of Internet Governance – the multitude of private and public, national, regional and international policy arrangements impacting the use and development of the Internet – has matured, we also see information and communication technologies increasingly misused to contribute to global insecurity, rather than to ensure stability, security, safety and integrity; to violate human rights, rather than to secure them, and to entrench existing economic power relationships, rather than to promote a more equal world by empowering small and developing nations.

The age of digital interdependence

Most recently, the Report of the UN Secretary-General's High-level Panel on Digital Cooperation, The Age of Digital Interdependence (June 2019), has **called, inter alia, for a "Declaration of Digital Interdependence" and a "Global Commitment for Digital Cooperation".**

With the goal of achieving an "inclusive digital economy and society" the Panel has developed a number of recommendations for a next generation internet governance to emerge by 2030. Namely to ensure that

- "every adult should have affordable access to digital networks, as well as digitally-enabled financial and health services, as a means to make a substantial contribution to achieving the SDGs"; that
- "a platform for sharing digital public goods, engaging talent and pooling data sets, in a manner that respects privacy, in areas related to attaining the SDGs" is created; that
- "specific policies to support full digital inclusion and digital equality for women and traditionally marginalised groups" are adopted and "a set of metrics for digital inclusiveness" agreed upon.

With a view to increasing "human and institutional capacity" the Panel recommends the establishment of regional and global digital help desks to help governments, civil society and the private sector understand digital issues and develop capacity to steer cooperation related to social and economic impacts of digital technologies.

In terms of increasing human agency, the Panel confirms that "human rights apply fully in the digital world" and urge the UN Secretary-General to "institute an agencies-wide review of how existing international human rights accords and standards apply to new and emerging digital technologies." Internet platforms are asked to work with governments, international and local civil society organizations and human rights experts around the world "to fully understand and respond to concerns about existing or potential human rights violations" in the "face of growing threats to human rights and safety, including those of children".

With regard to algorithmic decision-making the Panel calls on automated decision-making systems to be "designed in ways that enable their decisions to be explained and humans to be accountable for their use": **"Audits and certification schemes should monitor compliance of artificial intelligence (AI) systems with engineering and ethical standards, which should be developed using multi-stakeholder and multilateral approaches."**

In order to increase trust and security, the **Panel recommends the development of a "Global Commitment on Digital Trust and Security".** Purposeful digital cooperation arrangements are needed, the Panel continues, "[i]f we are to deliver on the promise of digital technologies for the SDGs". Having identified gaps in existing governance arrangements, the Panel then proposes three digital cooperation architectures "intended to ignite focused, agile and open multi-stakeholder consultations in order to quickly develop updated digital governance mechanisms". In order to "update digital governance," the Panel suggests that the **UN Secretary-General "facilitate[s] an agile and open consultation process to develop updated mechanisms for global digital cooperation".** The first step - the initial goal - would be marking the UN's 75th anniversary in 2020 with a "Global Commitment for Digital Cooperation," which can serve to enshrine "shared values, principles, understandings and objectives for an improved global digital cooperation architecture".

Parsing the Panel's report further we continue to find common ground: Indeed, everyone should have the means to be online and able to benefit from the advantages of the digital age. Human rights, security and trust in cyberspace should be strengthened, and appropriate mechanisms for global digital cooperation created. The universal values that are referred to, including respect, humanity, transparency, sustainability and harmony, are both interesting and sensible. A "Declaration of Digital Interdependence" is needed, however, to clearly define those values – building and consolidating the many values, principles, and initiatives – in a UN-sanctioned declaration that complements the Human Rights canon.

Additionally, we need to elaborate and refine the architecture and rules of core cyberspace infrastructure as well as transpose and extend the governance regimes of other practice communities to embrace the emergent properties of digitization (i.e. coming online). Of course we should build on our existing regime(s), but the conflation into one global digital space has brought the complexity of economic, security and user-interests into one giant agora. The challenge to implement effective governance in unprecedented fast-evolving technology capabilities that spread at a global scale and are part of the dynamics behind the catastrophic global warming makes our joint venture truly urgent and epic in dimension.

Between binding international customary law and treaties, principles of international law, regional integration law, national law, transnational normative arrangements, internet governance principles, open standards, and best practices, the notion of "rules" has become so broad online that no one can claim to fully understand the rules. A comprehensive ecosystem of loosely coupled[7] smart regulation with transborder compatibility is indeed essential. **We assess that one of the ingenious design decisions made by the fathers of the internet, to establish architecture and practice that allows for internet traffic to flow without written contracts between network operators, is a main cause for the unprecedented innovation and economic engine[8].** The Panel makes clear that the time of traditional international treaties, negotiated behind closed doors, is over. Multilateralism will continue to be important, but multilateralism needs to be understood as encompassing other "sides" and as complemented or informed by multi-stakeholder approaches: this is "innovative multilateralism".

Source

[7] David Weinberger, Small Pieces Loosely Joined: A Unified Theory of the Web (2003).
[8] Andrw Sulivan, The Internet is made with carrots, not sticks | TechCrunch (2016)
[9] Kent Walker, How we're supporting smart regulation and policy innovation in 2019, (2019)

But what makes rules smart? We argue that the rules need to be set up to evolve and adapt to the progress of innovation. Thus smart rules and smart ways to recognize and implement rules must implicitly question and confirm their validity and legitimacy in light of technological innovation, as well as new challenges of ensuring security, enabling development and respecting, protecting and implementing rights[9].

The governance fields the Panel addresses – security, development, rights, AI - correspond to the next generation Internet governance elements we present in this paper. The contributions in this editorial shed light on how these rules can be developed and implemented fairly. The approach we put forward aims to marry core elements of the options laid out by the panel into one holistic governance model with core (internet) infrastructure governance complemented by sectoral governance solutions driven by relevant stakeholders in a practice community (e.g. health, mobility), all loosely coupled through joint deliberation, framing and monitoring at the governance clearing house IGF.

What's at stake in Internet governance?

Ensuring peace and security, development and human rights in times of digitality therefore always means: governing the Internet with a view to its impact on these key goals of the international information society. How can we realize the Internet's potential as a tool for international security, for development and for exercising human rights? How can we evolve sustainable digital governance and governance of digital sustainability? While we focus on connection and connectedness here, we note that there are also non-networked infrastructures upon which we increasingly depend. Protection of safety, security and privacy in the use of these devices is as important as Internet safety and security. We see the two debates as necessarily connected.

Our approach recognizes that current international law and Internet governance do not yet reflect the urgency we need to feel when providing rules and practices that lead to sustainable ecologies and a just, equitable society. The goal of our approach is simple: ensuring security, enabling sustainable digital development, and respecting, protecting and enforcing rights in the digital world.

Ensuring the integrity of the Internet as a public good through responsible stewardship by relevant stakeholders leading to multipronged Internet governance approaches is the backbone of our proposal for the #nextGenerationInternetGovernance in the 2020s. We are, of course, not alone with our finding. Complementary sectoral approaches to introducing

common commitments, norms and principles, targeted at a more nuanced Internet governance approach, have been pursued by companies, including Siemens (Charter of Trust) and Microsoft (Tech Accord), and by institutions, including the W3C (Contract for the Web), as well as states (and other stakeholders), e.g. through the Paris Call or Christchurch Call. The Paris Call, especially, was a rallying point for many international actors, including states, to realize the need for a commitment to safeguarding the core of the Internet through norms. Building on these approaches and valuing the normative acculturation they engender, we aim to provide a comprehensive framework of loosely coupled solutions that interact normatively, and are mutually reinforcing and interdependent.

Towards a solution

While we acknowledge the importance of recognizing digital interdependence and find much value in the commitments made in the framework of previous normative approaches, we would like to go a step further in deliberating #NextGenerationInternetGovernance in the 2020s.

#NextGenerationInternetGovernance ought to be based on a commitment by all stakeholders – particularly states and businesses – to take on shared but specific stewardship to provide open and resilient Internet services to all and to protect the rule of law and human rights. Rather than using regulation as a means of asserting national or commercial dominance, stakeholders need to commit firmly to common goals: to ensure that the Internet can be a tool to realize cybersecurity, human rights and entrepreneurship in fair (digital) markets, based on (by now) decades of commitments by all stakeholders to a human rights-based and development-oriented information society.

We conceive of this #NextGenerationInternetGovernance to be comprised of four interlinked parts:

1. a Digital Peace Plan – or #OnlinePeaceFramework – including norms for good behaviour of state and non-state actors in cyberspace and confidence-building measures to counter (neo)nationalist policies that endanger the stability and functionality of the global Internet and its infrastructure, and encompass (1) human rights-based approaches to national security (including military aspects and confidence-building measures), (2) the fight against cybercrime and (3) technical security and network resilience;
2. a Digital Sustainability Agenda – or #DigitalMarshallPlan – to promote human rights-sensitive (digital) economies based on market-driven innovation with data flowing freely in trusted environments, in which sustainable economic growth and decent work are ensured, where the next billion Internet users are brought online; and generally, to drive forward the realization of the UN Sustainable Development Goals;
3. a Digital Human Rights Agenda – or #RightsOnline4All – providing norms and policies to respect, protect and implement human rights on the Internet, based on existing norms, targeted at all relevant stakeholders, in their respective roles; and
4. a Framework for Future-Proofing AI Norms – or #ResponsibleAIStewardship – including guidelines on increasing accountability for the use of AI.

#NextGenerationInternetGovernance is holistic in that it applies to all 'layers' of Internet governance, from the social layer to the content and services layer, from the infrastructure to the logical layer. Importantly, the #NextGenerationInternetGovernance is not an effort to create new rules for an international terra nullius. It builds on previous work on shared responsibility, responsible stewardship, for internet-related global commons and a substantial number of normatively relevant documents, both binding and not, that evidence – especially in their aggregate – a strong commitment by states and other stakeholders to cyberpeace, sustainable digital development, human rights and a rights-based accountable use of AIs.

#OnlinePeaceFramework – A New Deal on Security

A comprehensive global framework coupled with multistakeholder-based commitments is necessary to ensure a peaceful and sustainable development of the Internet in the 2020s. Most importantly, there is a need to protect the public core of the Internet. Any attack against its basic functionality fundamentally impacts our global society.

The **#OnlinePeaceFramework** cannot be a single document but rather a series of joint analysis, deliberation, practice and institutionalization. It should start with an analysis of cybersecurity-related problems, thereby mapping technical aspects, institutional mandates, stakeholder roles and initiatives. Some aspects will need international treaties, such as the trade in cyberweapons, some may require only informal ad hoc arrangements, such as working groups to fight certain viruses. The Digital Peace Plan should have three main parts, dealing with (1) national security (including military aspects and confidence-building measures), (2) cybercrime and (3) technical security and network resilience, respectively. The issues in the three sub-areas could be negotiated by different groups and platforms but should be loosely coupled via liaisons and interactive communication channels.

#DigitalMarshallPlan – A Digital Sustainability Agenda for Business, Trade, Work and Sustainable Growth

A Digital Sustainability Agenda should be adopted and deployed to increase the productive forces within the global private sector as a whole and technology companies in particular. The Agenda could be implemented through a Digital Marshall Plan which can generate infectious positive momentum, incentivize the evolution of open business standards and practices, dynamize trade relations regarding the Internet and improve development opportunities for all in an Internet based on data flowing freely in trusted environments (G20/OECD, Osaka).

Sustainable digital growth is conditioned by and profits from the availability of decent work (ILO Resolution, June 2019) which is, in itself, a condition for realizing our shared humanity productively in the information technology age.

The UN 2030 Agenda for Sustainable Development identified the building of resilient infrastructure, the promotion of inclusive and sustainable industrialization and the fostering of innovation as key goals of sustainable development. The challenge we are now facing is the reconciliation of the impact of digitalization with the objectives of sustainable development. The goal of the Digital Sustainability Agenda would be the democratization of the means of digital production through the revitalization of a transnational socio-economic data ecosystem. **The fundamental infrastructure building blocks for each layer ought to be open standards-based and therefore evolved transparently through all interested stakeholders. This will allow for the provision of digital commons (tools and content) to all mankind while a level playing field provides competitive opportunities for innovation to all.**

Part of the Plan would be approaches to ensure that **all humans have a right to a digital identity** (SDG **16.9** "By 2030, provide legal identity for all, including birth registration") allowing them to take part in business transactions, access online educational programs (upskilling) and participate through eGovernment. Next to various authorities issuing national and international identities, responsible business facilitators that are also the providers of practical services like transaction signatories and storage are needed.

We would benefit from a **globally distributed registry for digital content** (incl. software), **which allows all rightsholders to have their value creation assessed, verified and subsequently enforced internationally.** At the same time, fair use provisions for non-commercial, e.g. artistic, private and educational purposes need to be refined and enforced. The best effort principle should be maintained in order to allow all users equal opportunity to benefit from and provide services and content on the digital ecosystem.

An open standard payment protocol can provide the basis to have financial institutions focus on new value creation and facilitating trade rather than charging for administrative and transaction services. In order to ensure the right to privacy, there needs to be an anonymous payment mechanism.

Part of the proposed Agenda would also be to **start a trans-national multi-lingual development of a shared semantic ontology or a digital Rosetta Stone:** the joint international development of a semantic model of the world is one of the greatest challenges and opportunities of modern mankind. Once achieved, it will make it feasible that all digital tools (from home electronics and appliances, to factory equipment to transportation systems) interoperate, thereby eliminating economic lock-in and related costs.

#OnlineRights4All – The Digital Human Rights Agenda

The Digital Human Rights Agenda is based on the commitment to existing norms and their technology-sensitive development. The dual nature of the Internet – as a space to use for the promotion of human rights and a space in which abuses can take place – has been convincingly established. Therefore, achieving public policy goals lying in the international common interest, like the protection of human rights online, is key to a sustainable online order.

Online rules encompass international legal rules, national legal rules and transnational normative arrangements. We have to enquire into the standards and practices used by judicial and quasi-judicial bodies, acting on behalf or within private companies, and enquire whether they enshrine legal recourse in tandem with the importance of the decisions they take. Protocols need to be developed in a human rights-sensitive way. Human rights-related protocol considerations include nudging and human rights protection optimization strategies.

Businesses must participate in norm-setting processes in good faith, including through self-regulation. While the potential benefits of self-regulation should be recognized in international negotiations, self-regulatory processes must support and enhance states' existing rights protection infrastructure, not weaken or replace it.

#ResponsibleAIStewardship – Establish best practices for governing Emerging Technologies

Over 30 declarations on algorithmic accountability and related reports on the ethics of AI have been published in the last years. Instead of submitting the 31st, we ought to establish liability frameworks that define responsibilities and make developers and practitioners commit to codes that center on human dignity and ensuring human decision-making sovereignty when implementing automatic decision-making (support) systems.

What do states, what does civil society want from AI? How can we achieve this without risking violation of individual and collective self-determination? We believe that we need to establish a normative framework with clear guidelines for the deployment of Artificial Intelligence in society, especially the societal implications of AI use. Automated decision-making systems must be designed with sensitivity to human rights and human development in mind. Humans must be kept in the loop so that systems can be monitored for errors and accountability. Any automatic decision must be clearly identified as such, traceable back to the logic underlying the decision.

In a 2018 paper on regulating automated decision-making[10], Google highlighted five policy areas regarding automation where research was needed. Our Framework echoes this call and proposes discourse platforms to allow consultation on them. It may be helpful to establish some global standards as "due diligence" best practice processes in relation to developing and applying AI.

Further approaches that ought to be implemented within the Framework include standards for explainability of AI; a fairness appraisal (to balance competing goals and definitions of fairness in AI use); safety considerations for workflows; access to training data for research purposes; and determining Human-AI collaboration, especially the relevant weaknesses and strengths and how they can be managed in light of a liability regime .

A new normative order of the digital: good rules for a better Internet

We understand our proposals as having orientative value in the coming discussion processes to establish new forms, forums and formats for digital cooperation. We offer more granular suggestions that fit well with proposals, as by the German Advisory Council for Global Change, for the development of a UN Framework Convention on Digital Sustainability and Sustainable Digitalization.

We are convinced of the formative power of norms within our digital ecosystem. The new deal for #NextGenerationInternetGovernance relies on its inherent normativity to shape technicity. Technology influences our behavior, but the focus on code and standards as 'telling us what to do' can be reoriented through our value-based normative approach. Rather than letting actors within the Internet Governance realm instrumentalize security or let profits dictate policy, our approach holds the promise of sustainable digitalization and digital sustainability.

Fast-forwarding Internet governance: #IGforTheFuture, where Forum follows Function

Up to now we have reviewed and contextualized the High Level Panel report and described normative building blocks with which to lay the foundations for sustainability and for progressive digital societies of today and tomorrow. The Panel on Digital Cooperation pointed out that the UN can add value to the normative framing of digital transformation by acting, inter alia, as a convener and a space for debating values and norms. The IGF can act as a clearing house and central deliberation space, where practices, norms and standards are discussed and where organizers of multi-stakeholder initiatives on specific issues assess progress and where the capacity of all stakeholders in mapping and measuring normative progress through best-practice models can be increased.

This continues to be true. However, we believe that the IGF Berlin 2019 can signal a turning point in the framing of Internet governance by reinventing itself to truly become a forum for #NextGenerationInternetGovernance.

One stratification of internet governance that we believe can work well is to distinguish between perspectives of organizations and aspects of challenges by dividing the online space into

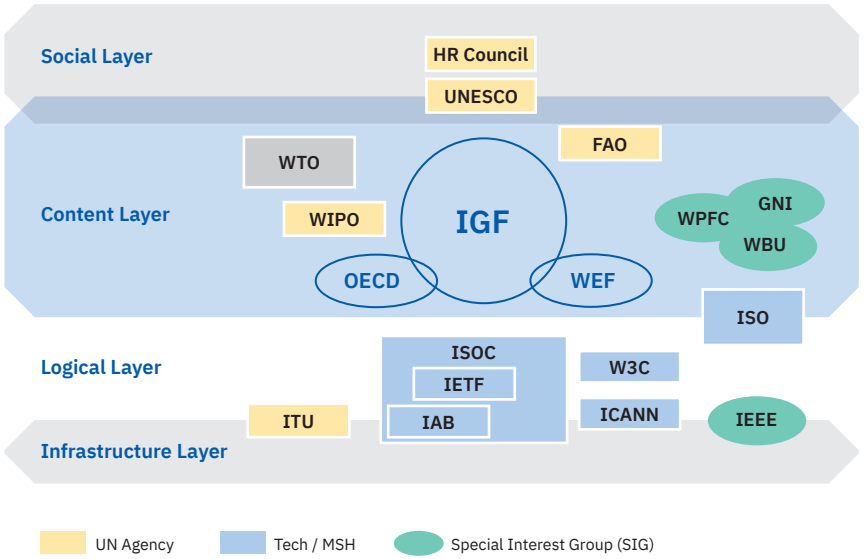
1. the physical layer – technology that allows for the connectivity and computation,
2. the logical layer – the logical and protocol suits that enable the decentralized management of the network traffic ,
3. the content layer, which includes all the information and applications of the world wide web, but also industrial internet services etc. and lastly
4. the social layer, which includes all the inter-cultural and inter-personal actions (see illustration below).

Source

[10] Amodei et al., Concrete Problems in AI Safety, https://arxiv.org/pdf/1606.06565.pdf.

[11] Perspectives on Issues in AI Governance - Google AI (2019).

Internet governance ecosystem

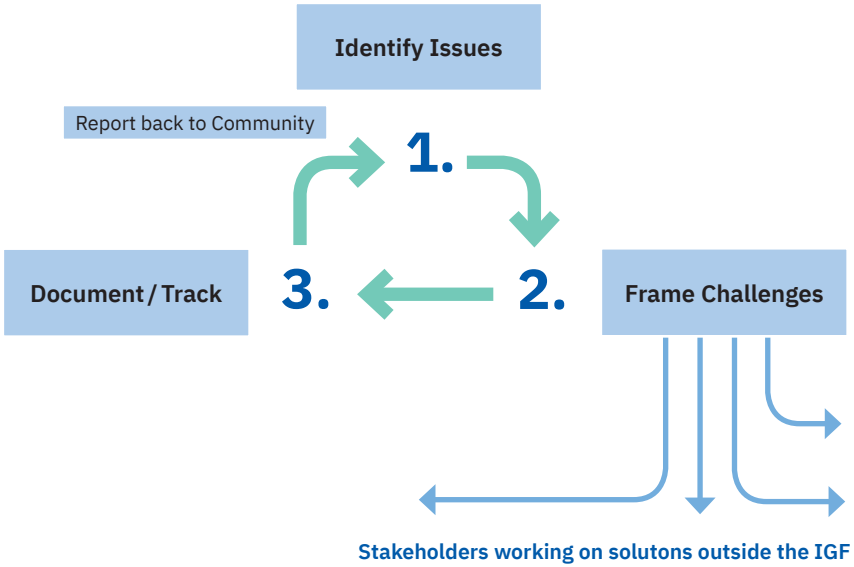


Additionally Cerf, Ryan, Senges and Whitt have pointed out in the 2014 paper "Ensuring that Forum Follows Function"[12] , the chief and most notable role of the IGF is that of the aforementioned "global clearinghouse and deliberation space tasked with (1) identifying emergent internet governance challenges, (2) framing them so that experts from all relevant institutions can cooperate in developing and implementing innovative solutions, and (3) assuring that the progress and discourse are archived and available for analysis." The core functions of the IGF are depicted below.

Source

[12] *https://global.asc.upenn.edu/app/uploads/2014/08/BeyondNETmundial_FINAL.pdf, pp. 31*

Three core functions of the IGF



We posit that this approach of forum following function is still key to ensuring a successful #IGforTheFuture. The good news here is that our approach calls for no new organization or mandate, but rather for the IGF to act as a global unifier and simplifier of Internet governance-related policy activities, a central reservoir for policy streams. What should its role be in the future?

(1) Identify issues: The IGF, supported by a strong MAG and strengthened Secretariat, should continue to identify emerging issues and introduce them to the global stakeholder community. For that, the process of selecting topics and workshops should be as accountable and open as possible.

(2) Then the **framing of the issues** should take place. As Cerf et al. (2014) write, experts attending the IGF analyze existing issues and

"stratif[y them] into modular challenges which are maximally independent when it comes to the (1) core technical functions, (2) the content and services realm as well as matters of human rights."

Then, IGF participants identify the ideal institution to work on the issue:

“Each institution can decide in what constellation of collaborators it wants to address which problem. The setup hence (i) allows for competing or parallel approaches and (ii) positions the IGF as facilitator rather than responsible for finding solutions to the various persistent challenges and constantly emerging issues.”

Then, these ideas are transferred to the optimal institutional form (ad hoc or permanent) to deal with them, respectively. A quickly materializing threat might need a multistakeholder coalition. A suspected cyberattack might call for NATO leadership. Pervasive human rights abuse via the Internet in a country might call for the regional human rights organization to act in consonance with NGOs. The need for a new standard would be dealt with e.g. by IETF’s standard-setting apparatus. A larger question of a new ethical framework for AI (and where needed legal framework) can be first addressed by global academia that pulls together other stakeholders and delivers a report about options and trade-offs. This approach would ensure responsive regulatory approaches (smart regulation).

(3) Finally, solutions are **tracked** and **‘legitimized’** through open review, debate and monitoring. This should happen both at IGF workshops that should show more continuity from one year to the next and in the various actor constellations that should nevertheless not only ‘do justice’ but be seen to do good. This makes their work transparent and immunizes them against critique as to their secrecy. The IGF can present a year’s worth of solutions, identify best practice models and offer critique of normative approaches that didn’t solve the problem they set out to. This ‘reporting back’ to the community is an essential part of ensuring policy continuity and feeds into the first function, the identification of pressing issues.

We stand with Cerf et al.’s 2014 conclusions and also believe that

“the IGF has the mandate and potential to serve these core functions and thereby stay a neutral non-decision-making platform dedicated to bringing all relevant institutions and experts together and facilitating the coordination of partners so that they can address the challenges relevant to them. These core functions do not exclude the other important functions the IGF serves - like capacity building or promoting universal access - as outlined by its mandate.”

#IGforTheFuture and the future of the IGF

The IGF 2019 in Berlin, with a view to the 2020 anniversary of the founding of the United Nations, **is an optimal starting point for discussions on #NextGenerationInternetGovernance on cybersecurity, human rights, economic progress, and future-proofing laws and society in light of the challenges presented by developments such as the Internet of Things and AI.** The answers need to be as convincing as the challenges are great: realizing a rights-based, sustainable next generation internet governance regime through adaptive and tailored governance approaches with the complex goal of ensuring loose coupling but not centralization or strict dovetailing of mandates.

One of the founding ideas and ideals behind the Internet was to enable communication across long distances, to bring the world together. As normative actors, we need to take the Internet seriously - in managing adverse effects and in enhancing positive ones. As the 2020s approach, it is high time to reach across the stakeholder aisle, to make different normative ‚cultures‘ cohere, to build trust, and to create a truly transnational network of actors to ensure that the network of networks can fulfill its promise to the world and its people.

The UN Panel’s arguments are fueling our multi-pronged approach for a #NextGenerationInternetGovernance in the 2020s and ought to be harnessed in the run-up to WSIS +20 in 2025. Our approach towards an #IGforTheFuture highlights the potential value of the event: responsible stewardship, accountability, inclusiveness and norm-generation, allowing outside solutions but importing them into the process and thus keeping a firm hand on the fragmentation of Internet policy-making.

This paper is a beginning, not an end: It is meant to fuel a multistakeholder-based normative dynamic that - over the next ten years - will be crucial to develop an Internet governance framework that collaboratively maps the problem space, defines the roles and responsibilities of relevant stakeholders and grows a loose coupling between related areas. We must overcome the trends of polarization between the west and the east, as well as the dystrophic tendency to balkanize the policy / legal space into a multitude of national and regional “solutions” that make it difficult to do business but also impossible for people to use the net and their services and devices internationally. Let us stop complaining and start collaborating on a #NextGenerationInternetGovernance based on a trans-national, decentralized architecture that makes the Internet a technology and space through which individuals are empowered by access

to information, knowledge and increased participation in a public discourse and political participation space. Companies can grow in monetary terms and as socially responsible actors, and states can exercise their rights and responsibilities. **The Internet has brought significant change to all sectors of society and fundamentally altered the interrelation of stakeholders in public policy.** As we have shown, it is now time for the Internet, and its governance regime, to become responsive to sensible change. **It is time to become responsible stewards of the internet and our planet.**

PART 1: STAKEHOLDER

GOVERNMENT

Strengthening Digital Cooperation: The Future is Now

Houlin Zaho

A digital revolution is unfolding before us. Breakthroughs in information and communication technologies (ICTs) are transforming sectors as diverse as health, education, employment, transportation, agriculture, nutrition, social inclusion and poverty. With the potential to accelerate progress across each and every one of the 17 UN Sustainable Development Goals (SDGs), ICTs holds great promise to deliver digital dividends for people everywhere. At the same time, they also bring with them profound challenges and significant implications of risk for widening digital divides.

This gives rise to the question — what can we do to ensure that this digital revolution turns into a development revolution for all?

As the Secretary-General of the International Telecommunication Union (ITU) — the UN specialized agency for ICTs — I believe that all stakeholders need to work together to focus our collective efforts on connecting the unconnected by prioritizing action on the following “Four Is”:

- Extending infrastructure to unconnected communities, as well as upgrading the current infrastructure, with new technologies such as 5G;
- Mobilizing public-private and private investment by fostering an attractive environment for investments, for e.g. through ITU international standards;
- Finding innovative ways to do business. Competitiveness, in an increasingly open global economy, requires new approaches to develop an enabling digital environment across sectors. Small and medium enterprises (SMEs) and entrepreneurs are critical to this effort.
- Making inclusiveness a priority and building the principles of non-discrimination, transparency and accountability into the technologies themselves. Bringing traditionally marginalized groups (such as women, persons with disabilities, youth, indigenous people, rural populations, older people etc.) into the fold through targeted programmes for digital literacy and skill development.

Having been at the centre of advances in communication and innovation for over 150 years — from the telegraph to the telephone, mobiles to satellite, the Internet and now emerging technologies such as Artificial Intelligence (AI), Internet of Things (IoT), 5G etc. — ITU has led the UN's efforts to bring us to a more inclusive and connected world today than ever before. As society stands on the cusp of the fourth industrial revolution, ITU once again stands at the forefront of this digital revolution with the mission to ensure that no one is left behind.

ITU strongly supports cross-sector collaboration, and in that, it benefits from a wide membership of 193 Member States and nearly 900 companies, universities, and international and regional organizations, thereby reflecting the rapidly changing nature of today's digital society. Together with these members, among other things, ITU promotes investment in infrastructure; develops global standards on communication technologies and services; manages spectrum and satellite orbits; encourages innovation and participation by SMEs, start-ups and young entrepreneurs in its activities; assists developing countries in strengthening and implementing their digital development strategies; and drives the development of new and emerging technologies.

Going forward, all current paradigms will be tested by emerging technologies such as AI, Blockchain, IoT and 5G that are currently changing economies at warp speed and scale. As industries and technologies converge, and new market structures, business models, investment strategies and revenue streams emerge, it is vital to ensure the trusted, safe and inclusive development of these technologies and to prevent any deepening of existing inequalities and social biases – all of these being areas where ITU devotes significant effort.

A core function of ITU is the harmonization of world-wide use of spectrum and the ITU World Radiocommunication Conference from 28 October to 22 November 2019 in Egypt will identify and allocate globally harmonized spectrum for a wide variety of services, including for 5G above 24GHz, and will finalize the 5G radio interface standards, among many other decisions.

The annual World Summit on Information Society (WSIS) Forum plays a critical role as the world's largest multi-stakeholder ICT4D platform that facilitates global discussions on concrete ICT solutions for development issues. The WSIS Forum is hosted by ITU and organized together with UNESCO, UNDP and UNCTAD, in close collaboration with the entire UN system, and this year it celebrated its 10th anniversary, attracting over 3000 stakeholders from over 150 countries. The WSIS Forum, focusing on ICTs for development, and the IGF focusing on Internet governance matters, complement each other as outcomes of the 2003 and 2005 Summit.

As a global platform, ITU provides many such opportunities for all key stakeholders to come together and develop a common understanding of the challenges facing the ICT sector and the solutions required, whether through events such as the AI for Good Global Summit, Global Symposium for Regulators and ITU Telecom World or its study groups. It is a unique platform where all voices are heard and where any resulting standards have the consensus-derived support of the growing and diverse ITU membership.

ITU Telecom World, for instance, provides a leading global platform for governments, companies, investors and other stakeholders to create new business opportunities in areas as diverse and promising as mobility, 5G, artificial intelligence and smart cities to name a few. This year, more than 150 SMEs from over 40 countries joined the dialogue. SMEs are on the frontline of today's digital transformation and their positive impact on innovation and job creation is unmatched. I am pleased to see more and more SMEs engaging with such platforms.

Given that society is now at an inflection point, the role of multilateral, multi-stakeholder, consensus-based organizations, such as ITU, will continue to remain critical to strengthen action and cooperation towards bringing the benefits of ICTs to everyone everywhere.

We must bear in mind that the digital divide has many faces – gaps in coverage, speed, skills, local content, access, security and affordability between developing and developed nations, between cities and villages, and even between men and women online – and the path to a transformative but also a safe, trusted and inclusive digital space will, therefore, require unprecedented collaboration at a global and local level between government, industry, academia and civil society.

At a time when almost half of the world's population – 3.7 billion people – is still not connected to the Internet, and growth is dangerously slowing for many of the access indicators, there is an urgent need for all stakeholders to come together and develop agile and innovative models of partnership as well as utilize trusted mechanisms/platforms for collaboration that can evolve to keep pace with the rapid rate of technological change.

At the end of the day, multi-stakeholder cooperation and collaboration is the cornerstone of a truly inclusive and empowering global digital space. I am confident that we will continue to strengthen our efforts together to effectively bring the power of ICTs to all nations, all people and all segments of society.

Once upon a time .... in cyberspace

Uri Rosenthal

Once upon a time information and communication technology, with special reference to the internet, was the exclusive domain of idealists, optimists and daring explorers. At Brazil's 2014 Netmundial, a large part of the audience carried badges declaring the people's ownership of the internet. But when, at the same time and in a similar vein, Google's Eric Schmidt and Jared Cohen told us that "the Internet is the largest experiment involving anarchy in history", they immediately added: "Consider too what the lack of top-down control allows: the online scams, the bullying campaigns, the hate-group websites and the terrorist chat rooms. This is the Internet, the world's largest ungoverned space."[13]

Over the years, we have experienced dramatic changes in cyberspace. Not too long ago, ICT and the internet were an integral part of high-trust society. The future was theirs. With billions of people to get access to the internet, it would be just a matter of time for the North-South divide to dwindle. Digital technology was to be the enabler of the enabling technologies. Estimates had it that at least 30% of the growth of global trade would be based on the production and consumption of ICT- and internet-dependent goods and services. And the golden age of digital democracy seemed in the offing.

Today, we are sadder and wiser. When we talk cyber, the straightforward association is with security and, to a lesser extent, safety concerns. Increasingly, cyberspace and the digital world are looking like a double-edged medal. On the one hand, we should cherish the indispensable benefits of digital technology, including big data and artificial intelligence. Although the United Nations are warning against an upcoming digital divide between North and South, there are remarkable instances of leap-frogging in the Southern continents. A number of emerging, if not big powers are leaning heavily on a felicitous combination of domestic software development and the conversion of high-tech into low- and medium-tech products and services that enables them to reach out to remote areas and scores of people left behind in the past.

On the other hand, there have been negative developments. Several states, especially authoritarian ones, repudiate the free, creative and entrepreneurial flow of information and communication, and do indeed claim full ownership of the internet. As President Putin said, "the internet is mine." His offer to the other BRICS countries to follow suit on his Russian Internet Law is not very reassuring. Unfortunately, on the domestic front, all this is going hand in hand with the increase in high-tech surveillance methods that more often than not put the upholding of human rights at serious risk. In the global arena, they engage into industrial espionage and direct or proxy attacks against cyber-sensitive or physical domains in other countries. On the escalation ladder, the prospect of cyber wars activates questions about the application of the Law of Armed Conflicts.

At the same time, the unconditionally golden era of the American Big Four/Five/Six (Google, Amazon, Facebook, Apple, Microsoft, Netflix) and other software and data providers is history. Consumers have come to understand that there is no such thing as a free data lunch. On top of their increasing awareness of the business case underpinning the seemingly free provision of data, their concern about intrusions into their personal life is growing. The Big ones are under increasing pressure to acknowledge that they have a pivotal role to play in countering the abuse of the social media by criminals, terrorists, anti-democratic extremists and circulators of fake news. That to play this pivotal role is easy to declare but loaded with dilemmas and predicaments, is clear.

Let us then focus on the institutional setting behind this mix of positive and negative developments and look at appropriate ways to reinforce the positive side, while mitigating the adverse trends in cyberspace.

In 2011, when I served as Minister of Foreign Affairs of The Netherlands, I launched the Freedom Online Coalition. By now more than thirty countries are participating in this intergovernmental institution. The chief objective is the advancement of internet freedom, including free expression, association, assembly, and privacy online. One could call the coalition a gathering of like-minded countries and ask oneself whether it would not be more useful to spend scarce resources involved to engage in encounters with governments that take a different stance on the need for a free and open internet. But apart from the fact that there is no shortage of discussions and efforts encompassing governments with varying and indeed antagonistic views, it is important for the like-minded members of the Freedom Online Coalition to create sufficient critical mass to counter those who controvert internet freedom.

It is crucial to adhere to a comprehensive well-balanced strategy promoting three complementary objectives: firstly, safeguarding the access to a free, open and privacy-guided internet; secondly keeping the internet safe and secure, all the way from fostering cyber hygiene to fighting cyber crime and other abuses; thirdly, utilizing ICT and the internet to stimulate economic

growth and social development. Global platforms like the Internet Governance Forum and the Global Conference on Cyberspace would render a tremendous service to all stakeholders to strike that balance with due perseverance.

In order to prevent misplaced claims between the various stakeholders in cyberspace, it is crucial to endorse the multistakeholder approach to ICT and internet governance – governance not being the same as government. It goes without saying that the competences, rights and duties, and responsibilities of the relevant stakeholders in cyberspace differ to a significant degree. This applies to states, private actors, the non-governmental players, the technical community, academia, and the end users. Despite quite some setbacks, obstacles and hiccups, there is sufficient support for the multistakeholder approach to stand its ground.

On the path towards a Global Framework for Cyber Peace and Digital Cooperation, diplomatic efforts should be stepped up. In many ways, there is still a lot to be done. It is not so long ago that in many countries the political leaders took no interest in cyber matters, if only because they felt more comfortable to leave the intricacies of cyber and the internet to the administrative experts and the technical community. First and foremost, then, cyber peace as well as digital cooperation demand the undivided attention of the political leaders. Secondly, cyber diplomacy should reach beyond the exclusive domain of governments – the so-called 1.0 track. Within the United Nations and other supra- and inter-governmental settings cyber issues require active multistakeholder participation. If the technology companies want to prevent over-regulation on the part of governments, they should take a pro-active stance in setting the cyber agenda.[14]

To ensure that the political leaders pay proper attention to proposals concerning the governance and, for that matter, the stability of the cyberspace, such proposals should be clearcut. Because of the vital interests involved, such proposals also need to be compelling. One promising proposal has been brought forward by the multistakeholder Global Commission on the Stability of Cyberspace. Among other things, the Commission has identified an urgent need for non-interference with the public core of the internet: “Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the internet, and therefore the stability of cyberspace.” The Commission defines the public core of the internet to include packet routing and forwarding; naming and numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media – for non-experts undersea cables, landing stations and data centers.[15]

I would say it would be just a matter of well-understood national and respective self-interest for governments and other stakeholders to adopt this kind of proposal.

Source

[13] The New Digital Age: Reshaping the Future of People, Nations and Business, London 2014, p. 3

[14] The Global Tech Accord and their commitment to the Paris Call for Trust and Security in Cyberspace. In: Jurrien Hamer et al.: Cyberspace Without Conflict: The Search for De-escalation of the International Information Conflict, The Hague 2019.

[15] Global Commission on the Stability of Cyberspace, work in progress.

From IGF to IGF+

Marina Kaljurand

Future of digital cooperation, inclusive approach, role of different stakeholders, multistakeholder model (MSM) have been on digital agenda for years. Finally, it seems that national and international actors have accepted the need for MSM. But still there are open questions, starting with who should be included into the MSM and finishing with the process - how exactly MSM should take place.

States are making politically right statements on importance of cooperation with other stakeholders, like the Paris Call[16] but working with stakeholders such as the private sector and civil society is still not in the DNA of majority of Governments.

Launch of a High-level Panel on Digital Cooperation (HLP)[17] by the Secretary-General of the UN was a timely and necessary initiative. Among other things HLP was asked **to consider models of digital cooperation to advance the debate surrounding governance in the digital sphere.**

Unfortunately, HLP did not have time to discuss all topics in full length. The Panel strove for consensus but did not always agree. HLP Report (Report) notes areas where the views differed and tries to give a balanced summary of the debates and perspectives. It reiterates what has been already agreed internationally, including applicability of international law to cyber, respect for human rights, identifies nine values that should shape the development of digital cooperation – inclusiveness, respect, human-centeredness, human flourishing, transparency, collaboration accessibility, sustainability and harmony - and proposes architectures for global digital cooperation.

In this paper/article I would like to discuss the following two topics from the Report: **multistakeholderism and future of digital cooperation - IGF+.**

Report states in the Executive Summary that "effective digital cooperation requires that multilateralism, despite current strains, be strengthened. It also requires that multilateralism be complemented by **multi-stakeholderism** – cooperation that involves not only governments but a far more diverse spectrum of other stakeholders such as civil society, academics, technologists and private sector." This understanding is one of the cornerstones of the Report. Multistakeholderism was discussed in all Chapters, starting with inclusive digital economy (Recommendation 1C – "We call on the private sector, civil society, national governments, multilateral banks and the UN to adopt specific policies to support full digital inclusion…") and finishing with cyber security ("Private sector involvement is especially important to evolving a common approach to tracing cyber-attacks, assessing evidence, context, attenuating circumstances and damage"). Recommendation 4A calls for "a multi-stakeholder Global Commitment on Digital Trust and Security to bolster these existing efforts". Recommendation 5B declares that "We support a multistakeholder "systems" approach for cooperation and regulation that is adaptive, agile, inclusive and fit for purpose for the fast-changing digital age."

HLP Report is very clear and strong on multistakeholderism. Now it is time for practical steps. Hopefully the ongoing GGE[18] and OEWG[19] processes that are convened under the auspices of the UN will follow the recommendations of the Report. As well as other forums.

The Panel had many discussions about the future architecture for global digital cooperation. It agreed that improved cooperation is needed, it even identified six gaps but did not agree on a single scenario.

HLP proposed three models aiming at generating political will, ensuring the active and meaningful participation of all stakeholders, monitoring development and identifying trends, creating shared understanding and purpose, preventing and resolving disputes, building consensus and following up on agreements:

1. **Internet Governance Forum Plus (IGF+)**
2. **Distributed Co-Governance Architecture** which builds on existing mechanisms
3. **Digital Common Architecture** which envisions a "commons" approach with loose coordination by the UN.

IGF+ enhances and extends the multistakeholder IGF. The Panel saw the strengths of this model in the fact that IGF is the main global space convened by the UN for addressing internet governance and digital policy issues. IGF+ concept would provide additional multi-stakeholder and multilateral legitimacy by being open to all stakeholders and by being institutionally anchored in the UN system. UN can play a key role in enhancing digital cooperation by developing greater organisational and human capacity on digital governance issues and improving its ability to respond to member states´ need for policy advice and capacity development. IGF already has a well-developed infrastructure and procedures, acceptance in stakeholder communities, gender balance in IGF bodies and activities, network of 114

national, regional and youth IGFs. HLP took also into account the shortcomings of the IGF that could be addressed by the IGF+: decision-making process, lack of actionable outcomes, limited participation of Governments and private sector, not very active participation from developing countries etc.

The IFG+ would comprise of 5 bodies:

1. **Advisory Group** that prepares annual meetings and policy issues. It could be appointed by Secretary General for 3 years.
2. **Cooperation Accelerator** that accelerates issue-centred cooperation across a wide range of institutions, organisations and processes. It should consist of members of multidisciplinary experience and expertise.
3. **Policy Incubator** that proposes norms and policies. It could provide a missing link between dialogue platforms identifying regulatory gaps and existing decision-making bodies. It should have a flexible composition involving all stakeholders concerned by a specific policy issue.
4. **Observatory and Help Desk** that will deal with requests from drafting legislation to tackling crisis situations. It will also coordinate capacity and confidence building activities, monitor trends, identify emerging issues and provide data on digital policies.
5. IGF+ Trust Fund – a dedicated fund for the IGF+ comprised of contributions by all stakeholders. Should be linked to the Office of the UN SG to reflect its interdisciplinary and system-wide approach.

To conclude – HLP Report is not a dogma. It is a living document that should be discussed, improved and implemented. IGF Berlin 2019 is a good place to continue the discussion that was taken to a new level in 2018 at the IGF Paris where the UN Secretary-General for the first time delivered an opening statement in person.[20]

Source

[16] Paris Call for Trust and Security in Cyberspace has been endorsed by more than 550 official supporters, including 67 states. USA, Russia, China have not acceded to the Paris Call. https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf.
[17] https://www.un.org/en/digital-cooperation-panel.
[18] https://undocs.org/A/RES/73/266.
[19] https://undocs.org/en/A/RES/73/27.
[20] https://www.un.org/sg/en/content/sg/speeches/2018-11-12/address-internet-governance-forum

Evaluating digital governance strategies

Virgilio Almeida

Digital technologies, especially internet, algorithms, artificial intelligence, and IoT, are transforming the world, modifying how we communicate, live and work. Digital technologies can be valuable tools to create better services, promote security, safety and economic prosperity that benefit society as a whole and in particular the most vulnerable groups. The difference between digital technologies that enhance society and the ones that weaken it is shaped by our capacity to create effective models of digital governance. As the development of the digital world expands and accelerates, it is crucial for stakeholders to gather from multiple sectors and multiple countries to understand how to evaluate the effectiveness of digital governance policies and strategies. Although many policies and principles have been proposed for digital governance, their effectiveness has rarely been systematically evaluated for expected outcomes. It is evident that there is a need for systemic mechanisms and performance criteria for assessing the governance structure of the digital world. The aim of this article is to examine elements that should be used to analyze the effectiveness of national, regional and global digital governance strategies.

The Nature of Digital Governance

Although there is not yet a strong consensus on how to define 'digital governance', the concept is generally used to describe a framework for establishing accountability, roles, and decision-making authority for governing the digital world. A digital governance framework should be able to align the main policies and strategies of the different governance systems, such as internet governance, digital platform governance, AI governance, IoT governance and cybersecurity governance. Like the internet governance process, the digital governance framework could be viewed as a distributed and coordinated ecosystem involving various organizations and fora. It must be inclusive, transparent, and accountable, and its structures and operations must follow an approach that enables the participation of all stakeholders in order to address the interests to the global society[21].

Good governance aims at ensuring inclusive participation, making governing institutions (i.e., public and private) more effective, responsive, accountable, and respectful of the rule of law and international norms and principles[22]. A set of key principles of good governance include accountability, transparency, participation and integrity. For example, the structure of the Internet governance ecosystem relies on democratic, multi-stakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical

community, the academic community, and users[23]. Integrity means that actions and behaviors of the main players (e.g., tech industry and global platforms) of the digital world follow ethical principles and standards. Good digital governance should rely on legal frameworks that are enforced impartially, with equity and in a non- discriminatory way[24].

Digital Governance Effectiveness

Before implementing a specific governance strategy or regulatory measure, governance bodies should analyze the choice between different alternatives. Three criteria commonly used[25] are as follows.

1) Impact/Effectiveness. It indicates how much a specific policy will lead to improvements in specific conditions? For example, how much a given policy would minimize the impact of AI applications on human rights violations?

2) Cost-effectiveness. It indicates what would be the cost of implementing a specific governance policy. For example, what would be the cost of implementing a policy that requires some sort of certification for critical algorithms?

3) Net Benefits/Efficiency. It indicates how to compare alternative policies for solving a specific issue in the digital world. Which alternative will yield the highest net benefits? For example should content moderation practices be regulated by self-governed policies implemented by the global platforms or should they be regulated by national legislation?

The time has come to create frameworks and mechanisms to evaluate the effectiveness of digital governance strategies. We need empirical evidence on the performance and effectiveness of different governance strategies[26]. We need appropriate studies to assess the effectiveness of regulatory measures. We need systemically oriented evaluation frameworks for governing the digital world at different levels, such as national, regional and international. We need to establish empirically justified governance strategies that can help to improve the process of governing the digital world with benefits for people, governments and private sector.

Source

[21] NETmundial Multistakeholder Statement of São Paulo, April 2014; http://netmun- dial.br/wp-content/uploads/2014/04/NET- mundial-Multistakeholder-Document.pdf
[22] G. Wingqvist, O. Drakenberg, D. Slunge, M. Sjöstedt, and A. Ekbom: The role of governance for improved environmental outcomes', Swedish Environmental Protection Agency, June 2012.
[23] V. Almeida: The Evolution of Internet Governance: Lessons Learned from NET- mundial, IEEE Internet Computing, vol. 18, no. 5, 2014, pp. 65 – 69.
[24] G. Wingqvist, O. Drakenberg, D. Slunge, M. Sjöstedt, and A. Ekbom: The role of governance for improved environmental outcomes, Swedish Environmental Protection Agency, June 2012.
[25] C. Coglianese: Measuring Regulatory Performance: evaluating the impact of regulation and regulatory policy, OECD, Expert Paper No. 1, August 2012.
[26] R. E. Kenward, et al.: Identifying governance strategies that effectively support ecosystem services, resource sustainability, and biodiversity, Proceedings of the National Academy of Sciences (PNAS), March 2011, 108 (13); Ruth Potts, et al.: Evaluating Governance Arrangements and Decision Making for Natural Resource Management Planning: An Empirical Application of the Governance Systems Analysis Framework, Society & Natural Resources, 29:11, 2016, pp. 1325 - 1341.

A vision, values, principles and mechanisms for cooperation and governance fit for purpose for the digital age

Thomas Schneider

Inspired by the "flower power" movement's **vision of a world free of power and control** with people connecting to transcend (physical) borders, the internet was designed by Californian researchers to share knowledge and ideas, and instead of using mechanisms of command and control, decisions were taken in **open-ended fora** based on mutual trust and by means of **"rough consensus"**. This approach has allowed the internet to become a carrier of unprecedented societal and economic innovation.

With the spread of the internet and the growing impact of digital tools and services worldwide, we had to realize, however, that **human beings do not behave more altruistically online** than offline and that – in the absence of appropriate incentives and checks and balances – whoever has power is tempted to abuse it and criminals are using digital technologies like they used other technologies before.

In the past decades, globalisation and digitization have **increased differentiation and interdependence** of our economies and societies. Private sector actors have become important drivers of innovation and a few **tech-startups have become global powers** with massive influence on the rules and norms that shape our daily lives. While, on national and global levels, **some people have been able to benefit** from globalisation and digital transformation, **others are falling behind** or are afraid of doing so in the future. With the traditional governance systems on national and global levels becoming more polarized and failing to produce stability and trust and to balance inequalities, some people fear that digital technologies may be used to dominate to subdue other people or nations rather than to improve our lives.

In 1945, after years of killing each other using latest technologies (at that time broadcast, airplanes, submarines, etc.), **former enemy countries** in Europe decided to get together and to create mutual trust through **engaging in rule-based economic** (and then later also political) cooperation. On a global scale, the **United Nations** were created with the aim to **foster peace and security through worldwide cooperation** to solve international economic, social, cultural, and humanitarian problems, based on human rights, rule of law and on the principles of peoples' equal rights and self-determination.

So how do we further **develop this global cooperation and governance ecosystem** to provide for freedom, peace, security and prosperity in the digital age?

At the UN World Summit on the Information Society in Geneva 2003 and Tunis 2005, we adopted a **vision of an inclusive, people-centred and development-oriented information society**. And in 2015 we agreed on the **UN Sustainable Development Goals** which represent a holistic vision for a better and more sustainable future for us all so that no **one is left behind**. These visions build on the values and principles established after 1945: **fundamental rights and freedoms, rule of law and democratic self-determination** remain key also in the digital era.

At WSIS, we all agreed that **all stakeholders need to work together** in order to achieve this vision. But since then, we have been **stuck in abstract ideological debates** about the role of governments and other stakeholders.

At least, the UN Internet Governance Forum (IGF) , an open platform for **multistakeholder-dialogue** created by the WSIS, has played an essential role in identifying emerging topics, fostering mutual understanding and preparing the fertile ground for the creation of informal and formal networks of cooperation. The IGF has served us well over the last decade, as the information society was unfolding. But **the IGF needs to be further developed to effectively interconnect – globally – the wide range of new issues and actors** now taking part in and being affected by the digital transformation.

In its report titled "the age of interdependence" presented in June 2019, the **UN Secretary General's High-Level Panel on Digital Cooperation** identified some of the gaps in the current cooperation system. One is the fact that still not all stakeholders from all over the world are able to make their voices heard. So the Panel recommends to create a **support function** ("help desk") to help stakeholders from small and developing countries to identify needs, opportunities and challenges and to provide guidance on where to invest their scarce resources so that they can also benefit from the opportunities the digital transformation offers.

In order to fill the gap between expert dialogue and political and economic decision making, the **Panel proposes to connect multistakeholder experts and decision makers into horizontal networks** that should cooperate and develop specific norms and solutions in an inclusive and transparent way so that they would be supported by all parties concerned and thus have a chance to actually be implemented.

In the past years, we have already seen a number of networks produce such norms and solutions, be it through initiatives of a more holistic nature such as the NetMundial Conference[28] or the Global Commission on Internet Governance[29] or others focussing on specific issues, such as the Internet

& Jurisdiction Policy Network[30], the Global Commission on Stability of Cyberspace[31] or the "Tech Accord"[32] and the "Charter of Trust for a Secure Digital World"[33].

The High Level Panel recommends to connect these to form a **multistakeholder network of networks "for cooperation and regulation that is adaptive, agile, inclusive and fit for purpose for the fast-changing digital age".** The Panel proposes three concrete options for the set-up of such networks. These merit to be discussed broadly, also here at the IGF in Berlin. While all three models have their merits, we propose to build on existing mechanisms such as the IGF and develop these further.

Since we know that human beings are not only good and altruistic, we **need to develop a rule-based cooperation and governance system** that creates the right incentives for all state and non-state actors to respect these values and principles and to use digital technologies to facilitate and not obstruct the achievement of the SDGs.

In this context, I would like to share with you the **experience** that Swiss people made, that it **is actually possible to create such incentives** and which has fundamentally shaped the political culture and system of modern Switzerland: in the civil war of 1847, the general of the army of the progressive-protestant cantons – knowing that they would win the war – was convinced that both sides would be better off in the future sharing the same country, if his side would **not apply a "winner takes it all" approach** and provoke feelings of hatred and revenge. But rather, both sides should sit together and start building a governance model based on **inclusive, participatory, consensus- and compromise-oriented decision-making procedures** following a federated and subsidiarity-based approach that would allow both sides to maximize freedom and self-determination and to keep exercising different religions and cultures and thus enable sustainable trust and pragmatic cooperation. After less than four weeks of war and not more than 100 people killed, he managed to convince the other side to **stop fighting and sit together** and build the architecture of the modern Swiss Confederation. Since then, there are regular intense debates and hard-fought popular votes about the balances between competition and solidarity, with the people winning at any one time knowing that they'd better voluntarily compromise with the losing side, as they might be on the losing side in the next decision. This experience has helped the Swiss people cooperating for freedom, peace and prosperity and avoiding war and destruction. And I hope that this may serve as an inspiration in the discussion of the HLP's recommendations with a view to develop a cooperation and governance architecture that allows us all to benefit from digital opportunities where no one is left behind.

Source

[27] *http://www.intgovforum.org/multilingual/*
[28] *http://netmundial.br/*
[29] *https://www.cigionline.org/initiatives/global-commission-internet-governance*
[30] *https://www.internetjurisdiction.net/*
[31] *https://cyberstability.org/*
[32] *https://cybertechaccord.org/*
[33] *https://new.siemens.com/global/en/company/topic-areas/cybersecurity.html*

Digital Governance

Peter Major [34]

The 10-year overall review of the World Summit on Information Society (WSIS) was conducted by the General Assembly of the United Nations (UNGA) at the end of 2015. The results of intense negotiations are reflected in the WSIS+10 Outcome Document. Member States of the UN during the high level meeting of the General Assembly approved the document (Resolution A70/125) with consensus and reaffirmed their commitment to the outcomes of the two phases of WSIS, and the value and principles of multi-stakeholder cooperation outlined in the Tunis Agenda.

The UN GA resolution extended the mandate of the Internet Governance Forum (IGF) until 2025 recognizing that the IGF was implementing the recommendations of the UN CSTD Working Group on the Improvements to the IGF (CSTD WGIG). The resolution also recognized the work of the UN CSTD Working Group on Enhanced Cooperation (CSTD WGEG)[35]. The UN GA resolution invited the Chair of the CSTD to establish another Working Group on EC to give recommendations as how to implement enhanced cooperation taking into account the results already achieved in the previous working group[36].

During subsequent negotiations of the second CSTD WGEG we could not achieve consensus because some delegates stated that some proposed recommendations could lead to changing the Tunis Agenda.

It has become evident that the WSIS+10 Document does not reflect adequately the evolution in technology, changes in societies, transformation of economies and modifications in political approaches in the UN system since 2005. Emerging new technologies have significant social and economic impacts that go beyond the scope outlined in the WSIS+10 Document. Job security and transformation of the job market, educational system to mention a few are of major concerns. Multilateral (let alone multi-stakeholder) approach is being questioned by some.

The UN 2030 Agenda of the Sustainable Development Goals does not show explicitly the crosscutting aspect and the significant role of ICTs in achieving the Goals. The UN and Specialized Agencies of the UN of the system, however, reacting to the benefits and challenges of new technologies, created, within their mandates, working groups, expert groups and other forms of discussions to deal with specific issues impacted by emerging technologies.

The UN SG's High-level Panel on Digital Cooperation in its report "The Age of Digital Interdependence" calls for identifying functions and mechanisms of digital cooperation, establishing linkages and identifying gaps. The Report in one of its recommendations proposes a new version of the Internet Governance Forum, IGF+, as a platform to continue discussions on Digital Cooperation with eventual recommendations.

In order that IGF+ to be truly inclusive retaining its original bottom-up and open character confidence-building measures are needed to bring on-board more governments, big technical companies to be part of the discussions. Strengthening the multi-stakeholder model may result in strengthening the multilateral discussions as well. There are however some concerns about IGF+:

- How to change IGF without going outside its mandate to include discussion on digital cooperation and how to resolve the problem of "two distinct processes" (IGF and enhanced cooperation)[37]?
- How to reconcile the bottom-up approach of the IGF with the top-down political discussions and intergovernmental processes?
- What is the role of UN and the specialized agencies?
- How to avoid creating a new process?
- How to bring all stakeholders on board, including governments, GAFA, Chinese tech companies?
- How to align digital cooperation to WSIS?
- How to streamline results of existing processes/working groups involved in WSIS in the UN system to help digital cooperation?
- How to go from discussions to principles, norms, recommendations and resolutions?

The impact of rapid technological change on sustainable development requires new approaches in the implementation of WSIS to ensure that the divides are closed and all groups of societies benefit from digital innovation. I believe that CSTD having its mandate on WSIS as should play a central role in the implementation WSIS[38] including Digital Cooperation.

I propose the following process:

- Results related to Digital Cooperation produced by working groups of the UN and its specialized agencies should be made available as input to IGF+ discussions,
- IGF+ is to include these inputs in its discussions and outcomes are to be reported to CSTD through Action Line facilitators

- CSTD should discuss and include results in its report on WSIS implementation to UN GA and in its draft ECOSOC resolution on WSIS Follow-up including recommendations , as appropriate,
- Alternatively a multi-stakeholder WG in the UN CSTD on Digital Cooperation may be established with the mandate to give recommendation as how to implement Digital Cooperation
- Further discussions on policy questions related to Digital Cooperation may be held at the annual UN High Level Political Forum
- Results achieved and the way forward are to be included in the WSIS + 20 review

The success of the process is based on trust and confidence and CSTD is considered by most stakeholders where tangible results may be achieved in Digital Cooperation.

Source

[34] Views expressed in the paper are those of the author in his private capacity and do not necessarily reflect those of the UN Commission on Science and Technology for Development.
[35] Note that CSTD WGIG and CSTD WGEC were constituted to include all stakeholders in the discussions on equal footing.
[36] The major result of the CSTD WGEG was the gap analysis: functions related to enhanced cooperation were determined; mechanisms to deal with the functions or the absence of them were identified. In the first CSTD WGEC some members of the group prevented consensus on recommendations because they would have liked to shift the stewardship of the enhanced cooperation process from the UN to one of its specialized agencies.
[37] IGF and enhanced cooperation are two distinct processes and this distinction is formulated in ECOSOC and UNGA resolutions related to WSIS.
[38] Reviews and assesses progress at the international and regional levels in the implementation of action lines, recommendations and commitments contained in the outcome documents of the Summit.

ICANNs multistakeholder-model and the Internet Governance Ecosystem

Manal Ismail

Not so long ago, we used to refer to two separate worlds, online and offline, virtual and real. Nowadays, both worlds are converging, same rights are called for, and almost all aspects of daily activities and services, from health to education, and from entertainment to business and trading, are being performed online. In parallel, cybercrimes have also developed significantly evolving from hacking and virus dissemination to blackmailing, cyber stalking, trafficking, credit card - frauds and identity thefts. Accordingly, the issues of jurisdiction and how to map national sovereignty in a borderless Internet, that emerged to be part of nations' critical infrastructures, became serious and pressing matters.

Given how the Internet has developed as an indispensable part of our lives, introducing new opportunities, unprecedented challenges and unintended consequences; and given the accelerated change, continuous evolution and growing reliance on digital technologies; Internet Governance (IG) advanced to be a priority on national agendas. This increased the interest of governments, driving political forces to start shaping the future of the Internet and bringing the role of governments in IG to the core of the debate. Although driving forces converged to foster greater interest and more focus on IG by all stakeholders, from governments, businesses, technical communities, academia and individuals, yet the lack of resources and lagging behind the global agenda are clear disincentives for meaningful and active participation from the developing world.

With the Internet of Things being deployed, interconnecting people and objects equally, and Artificial Intelligence on the road, where we need to remain in control and ready to bear responsibility of all decisions, more Internet Governance challenges are expected to emerge. Likewise, with data being the currency of today used for legal and legitimate requests but also for profiling and invading privacy, we should be ready to protect our personal information and preserve our own privacy.

As we start considering collaborative ways to address digital technologies' impact – societal, ethical, legal and economic – maximizing its benefits and minimizing its harms, it's essential and timely to investigate and agree on digital cooperation and governance models that can contribute to the achievement of the Sustainable Development Goals (SDGs) set by the United Nations General Assembly in 2015 for the year 2030. Effective Digital Cooperation, mandates the need for a holistically coordinated approach to

Internet Governance, respecting and taking into account interdependencies of stakeholders but also of the various sectors described by the main four baskets of the global Internet Governance Ecosystem, namely cybersecurity, digital economy, human rights and technology. This doesn't necessarily mean that we need to have a unified rigid mechanism rather we need to agree and commit to common principles and goals.

Experience shows that both multilateralism and multistakeholderism would continue to co-exist and should work to complement each other. Additionally, other new innovative models may develop in the future and should be allowed to plug into the overall Internet Governance Ecosystem, expected to be more of a network of networks matching the very unique nature of the Internet. Hence, we need to agree on an ultimate agenda, that is human-centric, promoting peace, future-proof, enhancing the quality of life for everyone, aligned with the 17 global SDGs, and abiding by the 9 values and principles identified by the report of the UN Secretary-General's High-level Panel on Digital Cooperation; namely: Inclusiveness, Respect, Human-centeredness, Human flourishing, Transparency, Collaboration, Accessibility, Sustainability and Harmony. At the same time, we need to ensure that such an IG network of networks is inclusive, transparent, accountable to all stakeholders, flexible, dynamic, agile, and open-ended with channels that can accommodate diverse current, evolving or future mechanisms, as far as they align with, are guided by and committed to the same goals, objectives, principles and core values.

The three models proposed by the High-level Panel's Report all have benefits and drawbacks, and despite being offered as alternatives, they don't seem to be mutually exclusive. In fact, despite the different approaches, they all share common elements that constitute the basic needs for any successful model. It is important though to secure global commitment to sustainable funding, enough resources and any necessary support needed. In that respect, a hybrid solution would be appropriate and possible with some keen efforts to allow harmonization, funding and a venue for periodical reporting on progress towards agreed values and principles. The IGF could serve to be such a venue.

At the end, unless a model is able to evolve, it will eventually die. Hence, review and evolution of any agreed solution is crucial in order to ensure that it continues to be efficient, effective, productive and future-proof; and the involvement of the relevant community is key for a successful process and a trusted model. A good example here is the ongoing process initiated by ICANN to improve and enhance the effectiveness of its own multistakeholder model, trying to hit the right balance between the increasing need for inclusivity, accountability and transparency and the imperative of being timely, effective and efficient.

No one knows how technology will evolve, and despite the efforts to ensure it enhances the quality of life of those who are benefiting from it, the digital divide seems to be widening with more than half the world's population either lacking affordable access or has not yet unleashed the full potential of the digital world. With this in mind, we need to focus our efforts to leapfrog the next billions so that they are not left behind, are part of the digital economy and enjoy the Internet, as we know it, or even better, as they need it: safe, trusted, available, affordable and multilingual. In addition, we need to be creative, flexible and agile in governing the Internet to ensure that it flourishes in a healthy way, as one stable, secure, resilient and scalable global public common, not only for those already using it but also for those yet to join or yet to benefit from the full spectrum of opportunities offered by and on the Internet.

Global Digital Cooperation: Conditions for Success

Fiona Alexander

High on the agenda as Internet stakeholders gather in Berlin, Germany for the 14th annual meeting of the Internet Government Forum (IGF), is discussion of the recently released Report of the UN Secretary-General's High-level Panel on Digital Cooperation. The report is the next step in an international dialogue on the benefits and challenges of technology that began in 1985 with the Maitland Commission's The Missing Link, and the subsequent 34 years of conferences, meetings and negotiations, including the UN World Summit on the Information Society. This most recent effort shifts the discussion away from the underlying infrastructure issues to the societal and social impacts that technology is having in the 21st century. Called by some, governance **on** the Internet as opposed to governance **of** the Internet. As stakeholders grapple with how best to meet the challenges of today while preserving prosperity and innovation, it is worth reflecting on the conditions that enabled a successful global Internet governance solution.

The U.S. government's efforts to privatize and internationalize the global coordination of the Internet's domain name system (DNS) took nearly two decades to complete. Initiated in 1998 with the Memorandum of Understanding signed between the Department of Commerce and the Internet Corporation for Assigned Names and Numbers (ICANN), it culminated with the transition of the stewardship of the Internet Assigned Numbers Authority (IANA) functions to the global Internet community in 2016. Arguably one of the most convincing displays of global digital cooperation via a multistakeholder process, the IANA functions stewardship transition involved hundreds of stakeholders all around the world.

Participants spent more than 800 working hours in meetings on the proposal, exchanged more than 33,000 messages on mailing lists, held more than 600 meetings and calls and incurred millions of dollars in legal fees to develop the proposal. The proposal was evaluated against the initially announced criteria, assessed against the Committee of Sponsoring Organizations (COSO) internal risk controls framework and evaluated by a team of independent corporate governance experts on the possibility of institutional capture. The transition faced a series of political hurdles in the United States, including a last-minute federal lawsuit. On October 1, 2016, the IANA functions contract expired, signifying the end of the transition.

In the face of legal, political and technical complexities, below are four conditions that enabled the success of the IANA stewardship transition.

- **Resilient political commitment:** The DNS project as it was called, spanned three U.S. presidential Administrations and initially enjoyed bipartisan support from Congress. It was not fully supported by the international community and featured prominently in the heated debates of the WSIS process, several meetings of the International Telecommunication Union (ITU), and the first ten years of the IGF agenda. These discussions often pitted the U.S. and a handful of allies against a majority of other nations. As ICANN matured, and coalitions of support grew over the years, the Obama Administration announced in March 2014 its intent to transition key Internet domain name functions to the global multistakeholder community. The response from a limited domestic political base was swift and hostile. As global stakeholders worked tirelessly through the proposal development process, the Administration had to defend the effort in Congressional hearings, federal budgeting debates and legal challenges, among other things. Without a robust and durable political commitment from the Clinton, Bush and Obama Administrations, the IANA stewardship transition would not have occurred.
- **Engaged participants:** The development of the IANA stewardship transition proposal and the accompanying improvements to ICANN accountability were developed by ICANN community volunteers from industry, civil society and governments. Participants spent more than 800 working hours in meetings on the proposal, exchanged more than 33,000 messages on mailing lists and held more than 600 meetings and calls. This was often in addition to individuals existing workloads. Without incentivized and willing stakeholders, the IANA stewardship transition would not have occurred.
- **Agreed problem set:** The announcement of the transition was specifically about the role played by the Department of Commerce's National Telecommunications and Information Administration (NTIA) in the coordination of the Internet DNS. As part of the response to the NTIA announcement, stakeholders raised a number of an unrelated DNS issues, both political and technical. Ultimately an ICANN accountability workstream was added so that the final proposal had two components. The ability of all involved to identify, describe, understand and agree the scope of the issue was critical. Without a stable and clear problem set, the IANA stewardship transition would not have occurred.

- **Available resources:** There is not a monetary estimate of the work hours and travel that stakeholders and the U.S. government spent on developing, evaluating and implementing the IANA stewardship transition. ICANN projected that it spent $34.4 million between personnel, travel and meetings, external legal advice, other professional services, and program administration costs on the proposal development alone. Without clear and sustainable revenue streams and human capacity, the IANA stewardship transition would have occurred.

As the next phase of global Internet governance and digital cooperation discussions move forward, it is worth reflecting on the history of the field. There are lessons to be learned from previous successes and failures. Without the above-mentioned conditions being met, new efforts at global digital collaboration will be limited at best.

PARLIAMENT

Germany's host role opportunities

Jimmy Schulz

In Germany, digitization is no longer a topic only interesting to nerds and a handful of quirky politicians - as it was a few years ago. On the contrary, the debate about digitization is one of the central topics of political discussion today. However, the term „digitization" does not even come close to describing the extent of the revolutionary change we are currently experiencing. In addition to the actual (technological) digitization, the global interconnectedness of digital data is an essential feature of these changes. All this is happening at an unprecedented speed, with the result that in many cases we are only able to watch, unable to step in and change the course of new developments.

This situation of radical change frightens many people and often they tend to focus only on the negative aspects of this change. But neither fear and insecurity, nor a naive and careless approach to new developments will help us shape our future. Fear is not a novel reaction to new technologies – especially if they have a revolutionary impact. The invention of letterpress printing, industrialization, the first railway and television are just a few examples. Every single time there were people who predicted the downfall of civilization. The Internet is a great opportunity for mankind and we can influence where we are going. All we have to do is to take action.

To this end, it is necessary to give technological progress as much free rein as possible while at the same time setting up „guardrails". However, at this point in time we are still lacking a consensus on where these boundaries should be drawn. The digitized society is currently in a kind of „digital puberty". We are testing boundaries and often crossing them. There are no tried-and-accepted rules of conduct yet, and we must still learn that a perceived technological anonymity is not a free ticket for forgetting our good manners. National legislation is only of limited help here. The Internet knows no borders, so we need a global approach in order to find a „common sense": A common understanding of what we want to allow and what not, how to behave and how we can deal peacefully with each other. The Internet Governance Forum (IGF) of the United Nations offers a platform for this.

This year, Germany is the host country of the XIV Internet Governance Forum, which will take place from 25. – 29. November 2019 in Berlin. Under the

motto „One World. One Net. One Vision“, thousands of participants, including representatives of governments, parliamentarians, entrepreneurs, scientists and representatives of civil society from all over the world, are expected to discuss the future and urgent issues of the digitized and networked world for a week. In particular, the importance of cross-border data traffic (data governance), network security and the integration of groups at risk of exclusion (e-Inclusion) will be the main topics. This year, the IGF steering committee has set itself the goal of strengthening the parliamentary aspect of global Internet Governance within the framework of the IGF. This is a great chance for us as parliamentarians and therewith in our role as representatives of the people to address important issues. The President of the German Bundestag, Dr. Wolfgang Schäuble, and me, as the Chairman of the Bundestag's Committee on the Digital Agenda, together invited members of parliaments from all over the world to actively join the discussions and the first parliamentary meeting during the IGF.

As this year's host country, we have the unique opportunity to encourage building lasting relationships between parliamentarians all over the world and promote „German Mut" (engl. Courage) as our core brand in the digitized and interconnected world. In my opinion, it is clear that we can only transfer our democratic values into the digitized and interconnected world using reason and courage. Germany has the potential to do pioneering work here. I advocate that we initiate a digital enlightenment movement – in the tradition of Kant's ideal - at the political, entrepreneurial, scientific and civil society levels which aims at liberating people from their "selfimposed immaturity". For this I would like to win supporters from all over the world within the framework of the IGF. Since 2003 I have been following and designing the activities of the IGF. I actively participated in three events: 2011 in Nairobi, Kenya, 2012 in Baku, Azerbaijan and 2013 in Bali, Indonesia. My experiences there have immensely broadened my perspective and allowed me to look beyond the German and European horizons. For example, I was able to get to know Arabic, Chinese and African visions of an interconnected world.

The particular importance of the IGF stems from its multi-stakeholder approach which enables a lively discussion on digital policy with experts and interested parties from a wide range of disciplines and countries worldwide. This has allowed me to get to know an incredible variety of viewpoints, ways of thinking and interpretation. I would like to recommend this experience to everyone – it educates and promotes tolerance.

One World, one Net, one Vision

Pilar del Castillo

The importance of the Internet Governance Forum multi-stakeholder approach towards Internet Governance, has always been a high priority for the European Parliament.

Indeed, for the European Institutions sustainable governance of the Internet involving all stakeholders is essential to preserve an open and free Internet in which all rights and freedoms that people have offline also apply online, making of the Internet an extremely powerful tool for social and democratic progress worldwide.

The **Fourteenth Annual Meeting of the IGF** under the overarching theme: **"One World. One Net. One Vision" will not be an exception.**

Indeed, many are the issues that need to be in the IGF agenda. Clearly while our daily lives and economies become increasingly dependent on "digital"; we also become increasingly exposed to cyber threats, making cybersecurity vital to both our prosperity and economies.

In this regard, particular attention must be paid to the fast evolving cyber threat landscape that accompanies the digital transformation of the World's economy as the Internet of Things, smart infrastructures, quantum computing, connected cars, digital health and eGovernment applications are massively deployed.

In addition, as the latest development with regards some international vendors has shown, cybersecurity requires essential policies, and global cooperation. No single country, or region, in the World can go about it alone, it is very important to work together with international partners and create initiatives by building a mutual and international consensual regarding an open, interoperable, secure and reliable cyberspace. The IGF is, in this context, a very valuable instrument that we must preserve and cherish.

The added value of the IGF is in any case much larger. Looking at the increased amount of events and articles that have seen the light in the last months, Artificial Intelligence can be considered the latest hot digital topic.

The European Union is currently consolidating its AI strategy. The EU has adopted legislation that will improve data sharing and open up more data for re-use, it has established a regulatory framework that will promote the deployment of the needed infrastructure and now is in the midst of adapting the first pan European digital fund that will help provide Europe with the right capabilities for AI to reach its full potential.

Nevertheless, and although Artificial Intelligence has a purely technological research and innovation component, research on AI must also be undertaken in the social, ethical and liability areas.

For example, from a labour perspective a reskilling revolution is needed. Consequently, every country around the World should: support digital skills and competences in science, technology, engineering, mathematics (STEM), entrepreneurship and creativity, modernise their education and training systems and participate in the elaboration a set of AI worldwide ethics guidelines. Once again, the IGF will have an important role to play:

"One World. One Net. One Vision"

Internet governance needs tough love

Marietje Schaake

Participating in internet governance gatherings has often left me feeling both very inspired and deeply frustrated. Inspired by the energy, ideas and goodwill from volunteers, the endless patience to listen to different perspectives and to negotiate an agreed text. Frustrated because internet freedom has been declining for 8 years in a row according to Freedom House and the many multi-stakeholder initiatives are not stopping that trend.

Mass surveillance, disinformation, privacy violations and cyberattacks are exacerbating conflict and eroding trust. Not only is the internet less open and its users less free; companies and governments alike see the internet as a place for power and control. The stakes are high for these stakeholders. But as states build sophisticated surveillance ecosystems, individual empowerment is becoming a distant dream. And as private companies design for ever more profit, the public interest is squeezed. Technology is not neutral, and governance is key.

At internet governance gatherings I often meet people who are idealistic and assume shared goals. These goals usually sound something like this: 'towards a resilient, safe and open internet, which allows people the world over to reap the benefits of digitization, while their human rights are respected'. But internet governance events tend to be self-selecting, and some of the most powerful decision-makers can opt out. While democratic governments tend to invest in the multi-stakeholder model, authoritarian regimes do not. In fact, they benefit from processes without teeth.

It is time for a serious reality check. For governance to have impact, ideals have to be implemented. The United Nations has confirmed its commitment to universal human rights online, as offline. This is of vital importance as a principle but is only truly meaningful when violators face consequences, and if the offline world is an indicator, we should not be reassured. It is high time to close the accountability gap. Whether we see personal data used to undermine democracy, cyberattacks deployed to paralyze critical infrastructure or zero-days spread to infect devices with ransomware, the perpetrators hardly ever face justice.

So it is time to move beyond declarations of Independence or of Interdependence, Magna Carta, Social Compact, New Deal or Geneva Convention Online. Soon there will be no more big words unused, while the actual impact of them will not have followed suit. Multi-stakeholder gatherings

should focus less on new processes, statements, and more on results and enforcement. This will require articulating the responsibilities of various stakeholder more clearly, as well as ensuring mechanisms for compliance, oversight and accountability exist.

All this is not to say internet governance through multi-stakeholder processes should not happen, on the contrary. The internet would be a better place if it would actually be governed by the stakeholders who care to join in inclusive processes, to work towards shared declarations. In a time of zero-sum politics, they are a welcome relief, but in order to remain relevant and legitimate, it is now essential to move beyond words. The IGF is the perfect moment for a reality check and some tough love.

A Voice from Kazakhstan

Byrganym Aitimova

In our contemporary society, the Internet is an intrinsic and inseparable aspect of everyday life for most people on the planet, to the extent that some even feel discomfort without being able to access it. Indeed, the Internet does not only provide incredible opportunities but is an indispensable means for communicating with the world, receiving and sharing information, doing business, accessing public services, and all other essential functions. Digital technology completely pervades and almost dominates our entire life.

Yet paradoxically, the Internet is independent of the laws of individual states, with the exception of legal acts on the protection and process of information and digitalization. At the same time, the Internet poses serious threats which the demands that the global Internet community must respond to critical risks posed regarding the protection of personal data of users around the world, ethics, equal access, freedom of speech, reliability of information, copyright, and other issues.

Equally important is the ever increasing and expansive abuse of the Internet with user accounts infiltrated by virus programs, fraud, ransomware and hacking. This calls for the urgent need to review and upgrade policies of receiving, providing and using personal data of the Internet community, as well as the requirements for software and equipment that processes and stores important data. Attention must also be paid to the use of the dark web, encryption and other concealed modes of internet operations used for radicalizing innocent populations, recruiting fighters by terrorist organizations and spreading hate crimes and violent extremism.

The escalating threats of cybercrime and cyber warfare need immediate action to prevent attacks on the banking, commercial, transport and telecommunications system as well as on critical infrastructure that can complete cripple societal functioning.

Of equal relevance is the safety of children and adolescents in the Web world. It is no secret that nowadays many children, even of preschool age use different gadgets with access to the Internet to view entertainment content. Teenagers use the Internet as one of the main sources of getting all kinds of information, whether it be school assignments, hobbies, entertainment or other activities. Moreover, they spend a lot of time on social networks and instant messengers which impact their learning performance and even warp their sense of values and morality due to exposure to undesirable elements on the Internet.

If even adults are caught in the trap of not always being able to filter content judiciously, adolescents are all the more vulnerable. Consequently, large segments of our population receive inaccurate and unverified information, which is taken for truth, ending up in unfavorable communities, associating with dubious individuals and viewing prohibited content.

These are just a few of the numerous hazards. The list is countless. It is up to the world community to avail fully of the immeasurable gains of the Internet and yet have an open dialogue on best practices and find a balance between regulation and personal rights and freedoms. This is the greatest challenge of our time.

The Internet Governance Forum is absolutely vital in addressing these issues and seeking common ground regarding regulations, processes and mechanisms in light of the structure of the Web and the processes taking place in it. Hence, an international platform, such as the IGF, serve as the compass to ensure confidence in a safe and open future for the Internet.

PRIVATE SECTOR

Fostering trust in the digital economy

Roland Busch

Digitalization and globalization are shifting paradigms and bringing new opportunities. Billions of devices are connected by the Internet of Things, interacting on an entirely new level. These technologies are changing the way we live, communicate and work. They are enabling new applications and business models across all industrial sectors and verticals.

Fundamentally, these advances are a great sign of progress. But while they improve our lives and economies, they also increase our risk of exposure to malicious cyberattacks. According to the Center for Strategic and International Studies, threats to cybersecurity in 2018 caused 500 billion euros in losses worldwide. More and more, critical infrastructures such as financial institutions, government agencies, healthcare systems and utilities are becoming targets.

The message is clear. Failing to protect the systems that connect and control our homes, hospitals, factories, power grids and infrastructures could have devastating consequences. The digital world needs baseline security, to match the commonly accepted safety measures we take for granted in the non-digital world.

Cybersecurity determines how people and organizations embrace new digital technologies. Trust in it, therefore, is the basis for any growth and progress in the digital economy.

Current cybersecurity efforts are strong – but don't go far enough

Companies and governments must take decisive action to keep pace with rapid technology advances, as well as with growing cyber threats. Digital players including IBM, Microsoft, Google and Amazon are working hard to achieve high levels of security and protect their reputation. The same applies in the industrial world, which is becoming increasingly digitalized. For example, Siemens has adopted a "defense in depth" comprehensive security approach that combines physical security, network security and system and software security.

Governments are also taking action. The EU Cybersecurity Act, which came into effect in June this year, establishes a strong agency for cybersecurity and EU-wide rules on cybersecurity certification. Many countries around the world are committed to facilitating more extensive and effective regulations.

While these efforts are helpful, businesses and governments must take joint ownership and responsibility for cybersecurity throughout the entire digital value chain. Every stakeholder should be part of a cybersecurity network that collaborates in fighting cybercrime and that shares common and reliable standards.

It is clear that no single entity can implement all the measures necessary. That is why Siemens initiated the “Charter of Trust” initiative, which calls for binding rules and standards to build trust in cybersecurity.

Since it was launched in February 2018, the charter has grown from nine to 16 members. In addition to Siemens and the Munich Security Conference, the signatories include AES, Airbus, Allianz, Atos, Cisco, Daimler, Dell Technologies, Deutsche Telekom, IBM, NXP, Mitsubishi Heavy Industries, SGS, Total and TÜV Süd. The Charter, which cooperates with government representatives and universities, also includes associate members: the BSI German Federal Office for Information Security, the CCN National Cryptologic Center of Spain, and Graz University of Technology in Austria.

One of the Charter’s initial focus areas has been to strengthen cybersecurity across supply chains. Third party risks in supply chains are becoming a prevalent issue and are the source of 60 percent of cyberattacks, according to Accenture Strategy. Charter of Trust member companies have developed baseline requirements to make digital supply chains more secure. Other focus areas include “Cybersecurity by Default“ and „Education“ – meaning predictive cybersecurity settings embedded in products and other environments, and continuing global training efforts both inside and outside companies.

Information, product and solution security must be an integral part of our digital world. Businesses and countries that want to play leading roles in the global digital markets will have to engage jointly in cybersecurity in order to sustain the trust of societies, customers and business partners.

Towards a Global Framework for Cyber Peace and Digital Cooperation: An Agenda for the 2020s - African perspective

Abdul-Hakeem Ajijola and Natasha Aduloju-Ajijola

The International Telecommunications Union (ITU) estimates that by the end of 2018, 51.2% (3.9 billion people) of the global population will be online[39]. The next three billion Internet users will likely come from the Global South especially Africa, Southeast Asia, and Latin America. This influx of new users are predicted to use the Internet in innovative ways to address different needs[40]. Whether they do or not[41], this will require a rethinking of the global Internet governance frameworks, to place human well-being, sustainable prosperity and collaboration as the basis for cyber peace. The path to this peace is through digital cooperation as manifested in the multi-stakeholder model practiced in the Internet Governance Forum (IGF) and other similar organisations.

As we consider the governance issues, we appreciate that we have a responsibility to all constituents who must live with the consequences of our decisions and actions. Groups that have been historically overlooked such as women, people living with assorted challenges especially in developing nations, and generations to be born should be given special consideration. To do this, we must be forward looking, review trends, incorporate multiple stakeholder perspectives while simultaneously understanding the past, present and future environments. A new framework must incorporate justice, respect for the dignity of life (including integrity and ethics), human rights, equity and access to knowledge.

A crucial role for the IGF is to support the Global South, especially Africa, to significantly improve its’ current cybersecurity posture. The Global South needs to focus on three key areas – capacity building, policy implementation (including investment) and recurrent expenses. There are three aspects of cyber capacity building that should be considered – building awareness about cybersecurity and risk management; training and implementation of lessons learned; and building the cyber pipeline towards the creation of sustainable streams of capable people.

At its’ core, cybersecurity is about risk management. However, the preliminary results of an ongoing study we are conducting show that many individuals in top management positions, do not have a real understanding of this, like what others have found[42]. Given the relationship between the scale of cybercrimes (it is estimated that in 2017, African economies lost $3.5 billion USD[43]) and the general lack of cyber hygiene and insight, concerted effort is needed to raise the awareness of cyber maleficence and how best to prevent and mitigate

it. We find that organisations are more likely to conduct themselves by the standards of international good practice have either international affiliations or are in highly regulated sectors such as Banking and Finance. It is important for organisations especially in the Global South, to share information about attacks with their peers, members and stakeholders to mitigate risks. Regular cyber training that can help create a culture of cyber hygiene and understanding of risk management, will help to reduce the amount lost to cybercrimes and other cyber malfeasance annually.

The rate of technology change demands regular and flexible training that evolves with technology. According to Alvin Toffler, "the illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn and relearn."[44] Some organisations, routinely send people to train- however there is a difference between attending a training session and implementing the lessons learned. In regard to training, we have observed that:

1. The people sent may not be the people that are best suited to help the organization move forward in enhancing their cyber defense – honest, transparent and fair mechanisms to help decision makers make the optimal decisions on who should participate in what training, and when, are required.

2. Unfortunately, the primary purpose of attending a training session is not always the training per-se but the indirect benefits that accrue from "attending" – organizations should limit payments to core overheads, and instead make direct payments to service providers and avoid cash pay-outs to participants.

3. Though organisations send many people to be trained, participants often keep the knowledge accrued to themselves – organisations must evolve mechanisms that oblige beneficiaries to "step-down" the knowledge they have acquired to their colleagues, thereby deepening the organisations institutional knowledge base. Such peer based train-the-trainer situations create social pressure on the primary beneficiaries to pay more attention during the external training because they know they will subsequently impart what they have learnt to their colleagues.

4. Often travel for expensive foreign training occurs even when such training can (should) be acquired locally. African countries must endeavour to provide basic training locally while aspiring to develop the capacity for intermediate-level training locally. We thus expect that at some point in the relatively near future that only exceptional higher-level or specialised training will require foreign travel. It is imperative that Africa empowers a critical mass of local computer knowledge as soon as possible. One of the paths to empowering this desired critical mass of local knowledge is by building the capacity of local IGF affiliates to provide introduction/ basic capacity building activities, and trigger local ecosystems that can migrate up various capacity building value chains.

5. Drills are irregular and ad-hoc – deliberate programs of various cyber drills complimented by online/ e-tutorials to bolster capacity building are required to complement and enhance local capacity building efforts. The IGF needs to initiate change management processes relating to Bug Bounty programs and Vulnerabilities Equities Process (VEP). For software or related solutions to become robust they must be "immunised." For immunisation to occur the software, or process, must be exposed to "friendly" hackers who will subject the product or service to real world rigors and document any failings in a credible VEP so that solutions to identified flaws can be addressed in a timely manner. Such mimicking of nature requires a significant mindset shift from an excessively secretive disposition to a more open posture which the IGF should encourage.

Among organisations that devote resources towards cybersecurity, many of their staff lack the capacity, training or authority to adequately fulfil their roles. We found that there is often an assumption that having basic protections in place (firewall, VPN, and antivirus software) means that an organisation is protected from all cyber threats. For the global south to fulfil its' digital promise, we must take action to increase positive cyber capacities. Our ongoing study indicates that the single most important challenge is human resource capacity. Capable staff with poor equipment will always do much better than incapable staff with excellent equipment. To address this, the IGF and its affiliates must encourage:

1. Management, especially in the Public sector, to tie certification and training to perks and promotion while effectively monitoring the results – the IGF should facilitate related advocacy given that its members will be prime beneficiaries.

2. Raising, for example, the profile of cybersecurity, and other technology roles, noting that cybersecurity is NOT an Information Technology (IT) issue per se but a corporate risk management issue. If IT Projects experience massive breaches, then associated organisations and economies lose credibility and stakeholder confidence. Unfortunately, such risks are often not fully appreciated until after a major breach. The IGF needs to support the development and implementation of confidence building initiatives to foster stability (not stagnation) and trust in cyberspace.

3. The creation of national cyber capacity pipelines from primary schools to secondary schools through Higher Education Institutions. Such pipelines will help ensure that the loss of a single individual does not cripple an organizations' cyber defense activities and that the haemorrhaging of professionals (as experienced in many global south economies) does not stall the development of needed cyber based economies. In many organisations, we find that there is a level of frustration that talented and capable individuals whom these organisations have invested in, leave and take their skills with them. There are examples of countries that have taken this pipeline approach and have created "an ecosystem that feeds itself, rather than an ecosystem that feeds on itself"[45]. The IGF can form a clearing house for sharing global good practice to ensure that decision makers avail themselves of insight into what works and challenges to be mitigated.

Technology, good and not so good, moves significantly quicker than most governments can respond. As noted by Barry Raveendran Greene, "Cyber-criminals operate at the speed of light while law enforcement moves at the speed of law."[46] The rise in cyber related malfeasance against governments, organisations, and citizens in the global south is due in part to inadequate infrastructure that includes laws, policies and related processes. A 2016 report by the African Union and Symantec found that the majority of African States (30) did not have specific legal provisions on cybercrime and electronic evidence in force and only 20% had a basic legal framework in place[47]. The implications are that activities that are crimes in certain jurisdictions, are not crimes in the ones that do not have the requisite laws in place. This undermines trust, digital cooperation, cyber stability and cyber peace. This also undermines the private sector as the engine for sustainable development and economic growth. Beyond national policies, organisations also need to have cyber policies in place and implement them. There seems to be a misconception among decision makers that once a policy is in place, action will be taken. However, we have observed that this is not always the case.

It is important to examine the recurrent expenditures that are associated with sustaining cyber infrastructure. Stakeholders need to assess the total cost of ownership of any cyber investment, because too often the focus is on capital expenditure, not recurrent expenditure. Experience across the global south demonstrates that more consideration needs to be given with regards to maintenance, upgrades, and "refresh" given the turnover of decision makers and haemorrhaging of technical specialists impacting institutional memory and operations.

Multi-stakeholder driven initiatives like the Internet Governance Forum (IGF) can provide the critical global frameworks that are key to developing and driving digital cooperation for sustainable and inclusive cyber peace based on natural universal principles of justice, equity and respect for human rights. The IGF should seek to position itself as the "translators and shock absorbers" of choice between various stakeholders including but not limited to Political/ Policy/ Paymasters who often seem to demand immediate solutions at no cost, and the Technical community who sometimes seem to seek unlimited time and budget to solve the problems at hand. Furthermore, as many us will attest, decision makers and the technical community often use different jargon and have difficulty understanding each other. This presents the IGF with the opportunity of evolving into a bridge, and bridge builder, between stakeholders. In doing so, the IGF will have reinforced its relevance and ensured its survival. These are legacies we will all be honoured and grateful to have contributed to.

Source

[39] ITU: https://news.itu.int/itu-statistics-leaving-no-one-offline/
[40] Pisa and Polcari: https://www.cgdev.org/sites/default/files/governing-big-techs-pursuit-next-billion-users.pdf
[41] Arora, Payal: The next billion users: Digital life beyond the West. Harvard University Press, 2019.
[42] Serianu: Demystifying Africa's Cybersecurity Poverty Line. 2017 : 88. http://www.serianu.com.
[45] Ferreira V.: How Israel became a cybersecurity power – and what Canada can learn from it. In: Financial Post. 2019. https://business.financialpost.com/investing/how-israel-became-a-cybersecurity-power-and-what-canada-can-learn-from-it.
[46] Barry Raveendran Greene bgreene@senki.org
[47] African Union, Symantec: Cyber Crime and Cybersecurity Trends in Africa. 2016 : 96. https://www.thehaguesecuritydelta.com/media/com{_}hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf

Why we need a New Digital Deal

Christoph Steck

Look around: nearly everything is going digital. Never in history has humankind enjoyed so much technology. The combination of internet, broadband connectivity, smartphones, Big Data and Artificial Intelligence is helping to tackle some of today‘s greatest social and environmental challenges. Nevertheless, dystopian visions of technology dominate the public opinion. People increasingly perceive digitalization as a driver of inequalities, degradation of living standards and lack of confidence.

A key reason is that today´s policy and legal frameworks were not built for the digital age and the fast changes brought about by the digital transformation have left many norms, policy and international processes outdated. There is an urgent need to modernize and create a better digitalization that is sustainable and empowers people. Both governments and businesses should adopt a more responsible behaviour and collaborate closer to achieve such a **human-centric digitalization.** It is time for our societies to debate and agree what we want our digital future to look like. Telefonica has published a Manifesto that asks for a **New Digital Deal** to create an inclusive, fair and trusted digitalization, focusing on five building blocks:

1. **Connect everyone.** Without broadband connectivity, there is no digitalization and the public and private sector should cooperate to connect the unconnected, focusing on creating sustainable business models and innovation for rural areas.

2. **Support people through digital transformation.** Artificial intelligence and automatization will profoundly disrupt work and job markets. Education, fiscal and social systems will need to be reformed to avoid a new digital divide. Technology should help diminish inequalities, not broaden them, and our common objective therefore needs to be to leave no one behind.

3. **Deliver trust in data.** Data can enrich people’s lives, benefiting businesses and advancing society as a whole. However, people increasingly do not feel in control of their data, resulting in a lack of trust and confidence. A human-centric model would enable everyone to decide how and when their data is used by improving transparency and giving real choice. Such new data ethics goes beyond pure compliance with data protection regulation and strives to empower people and put them in control.

4. **Foster ethical and accountable use of Artificial Intelligence and algorithms.** Business should make sure that algorithms do not take decisions that are unethical, undue discriminate or create anti-competitive outcomes. Companies will be held accountable for negative impacts of Artificial Intelligence on societies and people in much the same way as for damaging the environment.

5. **Modernise our policies and institutions** to make them fit for the digital era. Policies, regulation and authorities have not kept up with the fast pace of technological change and need a profound review. **A “Digital Bill of Rights” could protect fundamental rights of people online based on broadly accepted values like fairness and non-discrimination, responsibility, inclusiveness, accountability and transparency.** Policies need to make sure that companies can compete on fair grounds on a Level-Playing-Field and consumers are protected. Regulators should strive to promote innovation and leave room for experimentation, but also closely monitor market developments to be able to intervene quickly, if necessary.

A New Digital Deal might be defined on national or regional levels, but would need to be underpinned by close international cooperation and improved transnational governance mechanisms. Such a **“Smart Digital Governance”** should be collaborative, transnational and agile:

1. **Collaboration** among many stakeholders is necessary because public administrations often do not have all the information, intelligence and resources necessary in a fast-changing digital environment. T**he vast majority of internet infrastructure and digital services are owned and operated by the private sector, so finding the best solutions will often need their collaboration and knowledge.** Similarly, involving civil society´s view early will make solutions closer aligned with public interest and thus easier to implement Public and Private stakeholders share often the same objectives, but specific responsibilities for each stakeholder group would improve their collaboration.

2. **Transnational** alignment of norms and policy is needed due to the global nature of the internet and digital services. Issues like cross-border data flows or cybersecurity can best be treated through international cooperation and aligned approaches. Policy processes and instruments might differ in relation to the issues tackled. Positive examples vary from the Budapest Convention on Cybercrimes by the Council of Europe, a traditional international treaty negotiated and signed by over 60 states, to the NETmundial Multi-stakeholder Statement that defined Internet Governance principles through and open, multi-stakeholder process. Sometimes, especially for value-related issues, initially only a regional approach might be possible, but can later be broadened and aligned

with other jurisdictions. An example is the EU General Data Protection Regulation (GDPR) that has harmonized privacy regulation across the EU Members States and is now enabling international data flows through so-called adequacy decisions with other states like Japan or Canada, avoiding ultimately fragmentation.

3. **Agile** governance would include using principle-based approaches, self- or co-regulation mechanism and fostering platforms for learning and debate. Self-regulation initiatives of private companies like the Cybersecurity Tech Accord have been acting on improving cybersecurity when international policy agreement between states has not (yet) been possible. Regulatory sandboxes where companies are allowed to experiment, but are supervised by authorities, might provide a way forward to improve trust for new disruptive technologies like AI and Blockchain. The Internet Governance Forum has been an important platform for debate and catalyst of common views and should be better resourced to be able to provide also learning and best-practice sharing in a more institutionalised way.

In today´s challenging geopolitical environment we might see for international digital governance most likely a patchwork of diverse solutions and processes, often only on regional levels and rather including incremental improvements. Nevertheless, now is the time to move to the next level of Internet Governance, to create a Smart Digital Governance, where stakeholders, both public and private, work together on collaborative solutions for increasingly complex, global digital issues. We need keep evolving existing policy and governance processes and experiment with new approaches.

One thing is for sure: More, not less, collaboration between stakeholders will be needed to define a New Digital Deal and create a sustainable digitalization that focuses on people and is inclusive, trusted and fair.

SMEs and Internet Governance

Michael Rotert

DE-CIX is an SME and provides interconnection services such as peering, the settlement-free exchange of Internet traffic, with just below 100 Employees and is owned by the eco association, Europe's largest non-profit association for the Internet industry

DE-CIX was founded in 1995 as Internet Exchange in Frankfurt[48] and is today the world's leading interconnection platform, managing more than 6 Terabits per second peak traffic. In addition to Frankfurt, DE-CIX offers interconnection services at four more Internet Exchanges in Germany[49].

In 2012, DE-CIX took abroad its specific know how and experience in establishing and operating Internet Exchanges and now operates interconnection platforms in the many metro markets.

DE-CIX provides network interconnection platforms which are the heart of today‘s and tomorrow‘s Internet infrastructure. To ensure that the Internet runs securely and smoothly, more than 1,500 networks worldwide trust its experience and service quality.

Carrier and data center neutrality is a basic principle at DE-CIX. All its platforms are distributed platforms, offering access via multiple carriers and multiple data centers. With just one connection, networks get access to hundreds of networks.

Ever since its inception, DE-CIX has been motivated by the ambition to improve the quality of the Internet and access to information around the globe, and to grow new markets. This ambition remains just as valid today, as it paves the way for the 2020's and 2030's. In the digital world of today and tomorrow, access to global data flows is as essential for business as the provision of electricity was for the industrial world. DE-CIX, and its customer base that interconnects over DE-CIX's ever-growing global family of Internet Exchanges, brings connectivity to the world, and will continue to provide access to information and digital services to an increasing number of developed and developing markets in all corners of the world.

To date, DE-CIX has created and is growing eighteen Internet Exchanges on four continents, including Europe, North America, the Middle East, and India. Its goal for the coming years is to enable new and existing ecosystems in all major telecommunication-markets across the globe. The geographic coverage of DE-CIX, paired with the variety of interconnection services, will

allow connected networks, whether they are acting regionally or globally, to get DE-CIX interconnection services customized to their needs from both a geographical perspective and in terms of their respective business models.

Digital is reshaping how business is done:
DE-CIX is at the cusp of a completely new age in global economics, with organizations redefining their activities and their sectors on the basis of digitalization. As they become more digital, organizations will need a new interconnection service regime for their new services. New and transformative technologies, like IoT, Artificial Intelligence, and 5G are accelerating the pace of change in markets around the globe.

Long and well-established digital companies are changing their business models and going into new sectors. The classic network operator as the historical core customer of DE-CIX is no longer just a network operator: tech companies are entering different sectors and the variety of different products is increasing. We no longer have the clear delineation of network operators that we had even five years ago.

But it's not only the digital companies that are transforming. Old industry is redefining itself and its products in the digital era. Organizations are leveraging their digital strength to reshape their own business models, in turn transforming how business is done within and across entire sectors, including the automotive/mobility, healthcare, finance, and media sectors.

Classic network operators as we know them today are historically the core for DE-CIX and they remain key to DE-CIX's activities. However, we see a need for new interconnection services for enterprises, paired with cloud connectivity and with global capacity interconnection needs.

Digital markets demand high-performance, flexible, and customized interconnection:
For this reason, the DE-CIX platforms and ecosystems need to be able to cater for a variety of different services. The interconnection regime in the future will require flexibility in terms of different interconnection models and will need to cater for different types of capacity needs, such as peering, cloud connectivity, security services, and many more.

To satisfy modern enterprises' requirements for reliable, high bandwidth, and secure connectivity within their exclusive supply chain networks, DE-CIX is preparing the ground for the "Enterprise-IX". Enterprise-IX will tailor the benefits of the cutting-edge DE-CIX connectivity platform to the requirements of digital enterprises, with specialized security services, SLAs, and easy-to-manage connectivity to distributed production facilities and corporate partners. The goal of Enterprise IX will be to generate greater value for verticals through world-class connectivity, allowing them the freedom and flexibility to optimally profit from the digital revolution.

At DE-CIX, we have created an extremely successful and vibrant interconnection ecosystems over a period of decades. We are using these ecosystems to introduce new services following the route of innovation, disruption, and neutrality. At the heart of the DE-CIX strategy is the continued promotion of the direct, cost-efficient, and resource-efficient use of interconnection.

DE-CIX will continue to follow the path of terrestrial and sub-sea traffic flows; new, non-terrestrial dimensions are now being added to global connectivity potential. The combined power of the DE-CIX interconnectivity platforms and the ever-stronger satellite industry can be leveraged to bring connectivity solutions to hard-to-reach corners of the planet, opening up new locations and new market potential for connected customers. With the vision of the "Space-IX", DE-CIX continues to lead the way in developing innovative connectivity solutions for a changing world and wants to do justice to its mandate of improving the quality of the Internet and access to information around the globe.

With these approaches and with all our activities, our goal is to improve the quality of the Internet and access to information wherever it is required. Digital infrastructure is essential to allowing people to gain access to information, education, and improved health care services, and to have the chance to enjoy full and equal participation in digital life. This is all the more important in rural areas that do not have proper connectivity today.

Source
[48] https://www.de-cix.net/en/locations/germany/frankfurt
[49] https://www.de-cix.net/en/locations/germany

Internet Governance: multistakeholderism, trust and effectiveness

Michael Yakushev

It happened to me to participate in Internet governance agenda, starting with the Okinawa Charter in 2000. I represented Russian Civil Society in DOT-Force, and I was happy to participate in initial discussions how the future digital world should look like.

Twenty years have passed. The Internet from a magic and unclear "future" has become a convenient "everyday reality". Is it managed properly? May its governance be somehow improved?

Well, of course there are evident achievements. The most important one is worth mentioning from the beginning: the Internet is developing rapidly, and it is developing according to the same principles that were laid many years ago. It means that such principles were chosen correctly. It also means that people who are directly involved in governing the Internet turned out to be worthy of this noble task. In addition, it is important to emphasize that all the innovations, all the technological "surprises" that civilization has received from the development of the Internet in recent years, have been integrated into the already existing framework of the Net.

Although, as we see, a lot has changed during this time – the composition of the "big players": it moved from mainly telecommunication operators and DNS service providers to search engines, cloud computing operators and social services owners, who play an increasingly important role. We also notice radical changes in the preferences (patterns) in using Internet technologies. Unfortunately, there are also changes in positions of many states regarding freedom of information, especially on the Internet. The worst thing is that the discussions about turning the Internet into a war domain have begun and do not stop. And this exactly what cannot be admitted by all means ...

The list of issues that remain relevant for Internet governance is very large and it constantly "swells". Therefore, in the next twenty years we will all have a lot of work. What seems most important here?

First, it is a very successful experience of using the principle of **multi-stakeholderism**. Introduced by WGIG (Working Group on Internet Governance under the U.N. Secretary General) in 2005, it has proven to be correct and viable. The participation of various stakeholders in their respective roles, the mandatory consideration of the views of each interested party is definitely a huge step forward. Based on the traditional and time-tested principles of democratic decision-making process, multi-stakeholderism has shown its effectiveness in an environment where there are hundreds of millions and even billions of concerned participants (users). Many types of Internet governance stakeholders (consumers, providers, owners of Internet resources, government bodies, etc.) have similar interests. In existing multi-stakeholder mechanisms (such as the functioning of ICANN or IETF), these interests are reflected in the development and adoption of policies and procedures that ultimately satisfy everyone. This is a perfect example.

Second, what is often forgotten, is a factor of trust. The Internet of the 1970s and 1980s was mostly created on the trust between those who designed and developed this technological system, being primarily outstanding scientists and researchers. They adhered to the highest standards of professional ethics. That is why it is so important that we take into account the factor of trust and pay attention to everything that strengthen trust in all future projects of the digital cooperation. It is not only trust in communication between people, it's also trust in technologies, their reliability, and in the open and comprehensive development of "rules of the game" for everyone. The more trust we enjoy the greater is the reliability of the system, which includes not only computer devices, but also millions (billions!) of users. I am sure that the development and practical implementation of confidence-building measures, including those applicable by states, will largely prevent or minimize the risk of turning cyberspace into a battlefield.

Third, we need to constantly improve the **effectiveness** of existing and future Internet governance mechanisms and their institutionalization. It becomes clear that the existing instruments of the international public law are not sufficient to cover the full variety of issues arising with the use of the Internet technologies in social life. Many experts call for the development of Corpus Iuris Internetis, but valuable objections to this idea are also numerous. However, even in the situation of a much sharper global political confrontation during the Cold War, both antagonists managed to find compromises.

Thus, there appeared universal conventions on the partial ban on nuclear tests, on nuclear non-proliferation, in peaceful activities in outer space etc. In my opinion, the multi-stakeholder approach is able here to ensure coordination of the positions of all interested parties. For example, this may be implemented by transforming the Secretariat of the global IGFs (Internet Government Forums) into a platform for drafting a possible universal agreement on the Internet Governance – and the IGFs themselves should then focus on discussing and agreeing the principles and norms of such universal agreement. Of course, any multilateral international legal document can be

approved only by the UN General Assembly. Nevertheless, with this approach the drafting process will certainly be balanced and will take into account the interests and wishes of all participants.

Last, but not least. We should engage **young people** in digital cooperation as much as possible. They have already grown in a world where there are no digital boundaries and everyone can communicate with everyone, which would have been hard to imagine thirty years ago. They are free from psychological limitations and unnecessary prejudices of past eras. Therefore, the more young men and women understand how the Internet works, how it may be governed, and how the Internet governance may be improved, the better and more convenient the Internet will be for the new generations of its users.

CIVIL SOCIETY

Towards a holistic approach to Internet Governance

Anriette Esterhuysen

The combination of multilateralism and multistakeholderism in global Internet policy making

Multilateral and multistakeholder approaches are indeed not mutually exclusive. We need both, and both need to improve. States have fundamental responsibilities and accountability as duty bearers for protecting and promoting human rights (and ensuring that corporate actors do so as well); for creating enabling policy and regulatory environments for development; for ensuring that there is equity in access to education, health and other social services and for growing and upholding the rule of law. While most of this plays out at national level, global targets such as the Sustainable Development Goals (SDGs) and the World Summit on the Information Society (WSIS) goals and interactions with other states at international and regional level play a role in building common ground and cooperation. Multilateral processes and institutions have a vital role in ensuring fair trade, peace and security, and cooperation between states, as well as in holding states accountable when they violate agreements. These institutions need be stronger, supported with political will and financial resources to maintain spaces where all states can be heard and participate in decision-making, irrespective of their wealth and power.

If intergovernmental processes and the institutions that support them are to be legitimate and effective they need to be more efficient, inclusive and accountable. They also need to collaborate with one another, share information and coordinate internally. Government representatives who speak and make decisions in multilateral forums need to do so informed by the interests and views of the citizens, communities, civil society organisations, businesses and technologists from the countries they represent. And they need to report back, debrief, check-in, debate, disagree, listen to criticism and act on it. They also need to interact internally when ‘at home’ with other government departments and public institutions.

Embracing and applying inclusive multistakeholder approaches and participating in multistakeholder processes is a way of achieving this interaction, transparency and accountability. In my view multistakeholder approaches should never be a used as a substitute for inclusive and accountable governance; but they can help make governance better, and, in contexts where there is a lack of functioning legislatures and state-led

inclusive and accountable governance, they can help facilitate relationship-building and collaborative implementation among individuals and institutions from all stakeholder groups, disciplines and sectors.

However, rather than combining multilateral and multistakeholder approaches, I believe we need both; and both need to be effective and inclusive. Combining them risks undermining the role and responsibility of states to hold companies accountable for, for example, upholding rights, paying taxes, not harming the environment, and fair labour practice. In fact, it is the diversity, shared learning, and sometimes the tension between these multilateral and multistakeholder processes, particularly in their interaction with social movements and civil society, that often catalyses positive change in governance. A recent example of how multilateral and multistakeholder processes can complement one another is in the field of cybersecurity. In 2015 the United Nations General Assembly's (UNGA) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) agreed on norms for responsible state behaviour related to cyber conflict. The next round of GGE discussions in 2017 did not reach consensus, but, partly in response to this, a multistakeholder group, the Global Commission on the Stability of Cyberspace, was convened to look at norms for both state and non-state actors that can help ensure the stability of cyberspace. When the GGE as well as another UNGA body, the Open Ended Working Group on security in the use of information and communication technologies were constituted in late 2018 they had the GCSC norms and a body of research that informed these norms to draw on, as well as the work of an industry-led initiative, the Digital Tech Accord initiated by Microsoft.

The need for a holistic approach to Internet Governance

Digitisation in general, and the internet in particular do not operate in an alternative or parallel universe, nor do related governance concerns. They cut across all sectors of society and the economy, from agriculture to gender equality to peace and security. I agree completely with the editors that a holistic interdisciplinary and cross sectoral approach is required. Taking this on board is a task not just for so-called digital cooperation or internet governance processes but for all sectors and disciplines. For example, the issue of fair taxation of internet companies, and unfair taxation of individual social media users (a worrying trend in several African countries) are internet-related but not internet specific. Free expression and association online and countering misinformation and extremist speech needs to be addressed online and offline, by technologists, journalists, feminists, educators and human rights defenders, social media platforms and national human rights institutions. Responding to the impact of more children being exposed to pornographic content cannot be addressed just through online age verification or content filtering, it needs gender sensitive responses from parents and sex education programmes in schools. Ensuring that the internet of things does not result in the violation of individuals' rights to privacy is the responsibility not just of online platforms and service providers, but also of the manufacturers of "smart" devices and home appliances; and, by implication, the regulatory processes relevant to these sectors.

A holistic approach to internet governance must also include addressing and mitigating the harmful impact on the environment of increased digitisation. The production and use of digital technologies is likely to contribute to the climate crisis in proportion to their increasing share in the creation of e-waste and consumption of raw materials and energy. Internet and environmental governance processes need to join forces to create policy and regulatory frameworks that consider the environmental impact of the internet, from its development, the energy it consumes, to the production and disposal of the servers that run the internet and the devices used to interact with it.[50] We need manufacturing standards that will result in devices that last longer, that can be updated and upgraded and recycled. Environmental and digital rights activists and affected communities need to work together to hold companies and states accountable for measuring and mitigating the environmental impact of digitisation.

The idea of enhancing existing or creating new global mechanisms to frame the future development of digital cooperation.

Mechanism is a suitably open-ended concept. It can refer to institutions, norms and principles, treaties or processes. The need for new global mechanisms has been debated since the WSIS. India's failed proposal in 2011 to the UNGA for a new Committee on Internet-related Policies (the CIRP proposal[51]) kept it on the agenda and lack of agreement on whether such a new mechanism is needed or not was the primary contributing factor to the inability of the Commission on Science and Technology for Development's second Working Group on Enhanced Cooperation (CSTD WGEC)[52] to reach consensus in 2018.

We need to first enhance existing mechanisms before a justifiable argument for new mechanisms can be made. Existing mechanisms will have to change, and adapt to absorb digital cooperation and concerns as digitisation permeates almost all spheres of human, social economic and political

development. In fact, to some extent creating new specialised mechanisms could undermine the adoption of a holistic approach to internet governance.

An example of an existing mechanism effectively taking internet governance-related challenges on board is the UN Human Rights Council (HRC) through its internet resolutions, Universal Periodic Review process, and the recommendations made by its special mechanisms (e.g. the Special Rapporteur on Freedom of Expression and Opinion). All these have had a demonstrable impact; including on national legislation and initiatives monitoring companies compliance with human rights such as Ranking Digital Rights[54]. Linked to this is the work of the human rights treaty bodies who regularly review states' human rights records with respect to the exercise of these rights on and through the internet.[53]

What holds back progress in internet governance in my view is not the lack of mechanisms, but the lack of commonly agreed and monitored (and where relevant, enforced) approaches, principles, norms and values. The reason that United Nations' human rights mechanisms have been relatively successful in taking on board internet governance is because they have a common framework of principles, laws and standards, and because the HRC agreed, in 2012, by formal resolution, that the rights that apply offline also apply online.

Internet governance for the future: facing kryptonite and vampires

In their framing text for this volume the editors point out that there is no single solution to the challenges of clarifying and consolidating digital cooperation and internet governance. I agree completely. There is no silver bullet, no single super power, superhero or super institution to coordinate or rule it all and save the internet from the forces of "misuse" and abuse. But, not believing in silver bullets or super powers does not mean that there are no vampires to confront in internet governance, or that there is no kryptonite that disrupts progress in digital cooperation or that may prevent achieving the positive goals[55] articulated in the HLPDC report.

Internet governance's kryptonite – in my view – has two primary sources. First, is the fact that there is still no agreed understanding of how, from a public policy perspective, to conceptualise – and by implication, govern - the internet[56]. Without such an understanding, it is difficult to establish the agreed norms and principles that would form the basis of a common approach to internet policy and regulation, and maintain the overall stewardship that would get us closer to a more coherent approach to internet governance. There is general acceptance of the broad definition of internet governance – reflected in the WSIS outcome documents and affirmed during the WSIS +10 process in 2015 - and rough consensus that internet governance, like the development and management of the internet, needs to involve multiple actors and stakeholders. But exactly how and where this involvement should play out, and in particular, what the role and authority of governments and intergovernmental institutions and processes should be, remains contested.

Second, is the notion that internet-linked (or cyber or digital) problems, like digital exclusion, or violent extremism of misogyny online, need internet-based solutions. I am not proposing that internet policy and regulation should not consider, and address lack of affordable meaningful access, or the proliferation of online misogyny, hate speech and misinformation. But as long as there is social and economic inequality between and within countries digital exclusion will, in one form or another, persist. Similarly, as long as white supremacy, patriarchy and religious intolerance continue in the offline world, it will find its way online and can even be encouraged by ad-based business models that monetises sensationalised and extremist content. This is why we need a holistic approach to internet governance, as discussed above.

This brings us to internet governance vampires, there are many, and true to legend they are elusive, shifting shape and form. Like many vampires in literature and popular culture, they are also often not one-dimensional villains easily dismissed as being simplistically evil. But that does not make them any less dangerous, such as, for example, the large internet companies who, as described by Shoshana Zuboff, provide "free services that billions of people cheerfully use, enabling the providers of those services to monitor the behaviour of those users in astonishing detail – often without their explicit consent."[56A] But these companies have also provided free services, used for "good" causes and have used their resources to contribute to internet development and the expansion of access to infrastructure. They are far harder to dismiss and demonise than the global multinationals of, for example, the mineral extractive industry, even though their economic, social and environmental impact is probably even greater, and they pay, proportionally, less tax in the countries where they operate. Non-state actors (sometimes with the support of state actors) who use the internet to promote violent extremism, misogyny and hate speech are also vampires of a sort, infecting a platform that was viewed as a force for global understanding and peace, with fear and mistrust. States who shut down or disrupt internet services and violate the rights to privacy and free expression and association of individuals are also like vampires, casting a shadow of authoritarianism over those who use the internet to protest and demand democratic, transparent, just and accountable governance.

Internet governance for and of the future must find ways of overcoming its kryptonite and fighting vampires. The starting point, from my perspective is to reach agreement, formally and informally, that the internet is a global public good and that it should be governed and managed as such. This position is progressively getting more support as the internet has grown to be increasingly global and ubiquitous. It is also reinforced by the growing impact of surveillance capitalism and recognition that the behaviour and practices of internet companies need to be scrutinised and regulated.

This is not to say that the internet as a network of networks should be regulated, or that by referring to it as a public good that it should be controlled by governments. Quite the contrary. "Global public goods are goods with benefits and/or costs that potentially extend to all countries, people, and generations. Global public goods are in a dual sense public: they are public as opposed to private; and they are global as opposed to national. Like publicness in general, globalness is in most instances a matter of policy choice."[56B] I believe that if both multilateral and multistakeholder institutions and internet governance processes agree that we need to protect and look after the internet as a global public good, and then act on this policy choice, it will help clarify many current policy challenges. Recognition of the internet as a public good will provide clearer guidance to responses from policy-makers, technologists and activists to inherent abuses in internet business models, to some states wanting to claim national jurisdiction over the data generated by their citizens, or shutting it down when it is being used for political protest.

There is no better place to have this conversation than one where it has already started and where multilateral and multistakeholder approaches have been interacting since 2006: the Internet Governance Forum and its national and regional and intersessional processes (NRIs, dynamic coalitions and best practice forums). The global IGF needs to be strengthened; as do national and regional IGFs. There are many proposals on how this can be done, including, but not exclusively, from the APC to the CSTD WGEC in 2017 and those made by the HLPDC in its report earlier this year.

Without putting the IGF front and centre of the future of internet governance I fear that the ground that has been gained in exploring internet governance challenges holistically, cooperatively and inclusively, will be lost.

Source

[50] From the 2020 strategic plan of the Association for Progressive Communications

[51] https://itforchange.net/indias-proposal-for-a-united-nations-committee-for-internet-related-policies-cirp

[52] https://unctad.org/en/Pages/CSTD/WGEC-2016-to-2018.aspx

[53] A strength of the HLPDC report on digital cooperation is that it recognises the value of strengthening and building on an existing mechanisms like the Internet Governance Forum. However, it does not fully commit to this and also suggestions two other models for digital cooperation. Nevertheless, all three models proposed by the HLPDC have merit and useful elements to draw on for internet governance of the future.

[54] https://rankingdigitalrights.org

[55] I refer here specifically to the goals in the report quoted by the editors of this volume: "every adult should have affordable access to digital networks, as well as digitally-enabled financial and health services, as a means to make a substantial contribution to achieving the SDGs"; that "a platform for sharing digital public goods, engaging talent and pooling data sets, in a manner that respects privacy, in areas related to attaining the SDGs" is created; that "specific policies to support full digital inclusion and digital equality for women and traditionally marginalised groups" are adopted and "a set of metrics for digital inclusiveness" agreed upon.

[56] The concept of the internet as a network of networks is itself evolving. The use of terms like 'digital' and 'cyber' reflects this evolution and this also adds a further challenge to consolidating ideas of "internet governance".

[56A] John Naughton in 'The goal is to automate us': welcome to the age of surveillance capitalism. The Guardian, 20 January 2019. https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

[56B] https://nautilus.org/gps/applied-gps/global-public-goods/what-are-global-public-goods/#inge-kaul-and-raul

Essential but Vulnerable: the Centrality of Civil Society in the Future of Internet Governance

Brett Solomon

We depend on information and communications technologies to advance human rights, peace, and development. More and more, we also struggle to live with dignity in this wired world, reliant as we are on channels and platforms that can seem better built for amplifying division and intolerance than raising awareness and good conscience. By convening in open and inclusive forums like the Internet Governance Forum, we break the walls between conversations and work towards a common language to understand and address the challenges of the digital age.

Just as climate debates must start from accepting we have no "Planet B" or alternative to Earth, internet governance discussions must hold top of mind the goal of one global, interconnected, interdependent, open, and secure network of networks. All the internet, for all people, all the time.

We bring one stakeholder's perspective. In our daily work at Access Now, we see civil society under attack. Our Digital Security Helpline works with individuals and organizations around the world to keep them safe online. We provide preventive support, helping to assess threats and keep people safe from harm. We provide rapid response services, reacting to attacks in real time.

The numbers of clients and requests seeking our interventions climbs each year. We see the percentage of reactionary cases, where something has already gone wrong, outnumbering preventive cases, and the divide is growing. The internet is not secure, least of all for civil society, including human rights defenders.

But it's not just the cyber attacks on civil society that causes concern. It is the onslaught of ill-conceived public policy, regulations, and laws emerging in countries across the globe that are securitizing the internet, criminalizing speech and violating our rights to privacy.

What role can and do multi-stakeholder convenings play? The actors delivering abuse and spreading disinformation use the very same channels and platforms upon which we construct the information society. We are not apart, but inextricably linked. We craft the policies and architectures, or influence their design, in ways that potentially enable these harms, while also forging a path toward the knowledge society. The builders, designers, and constructors must hear from those most at risk – the reason we fully support the High Level Panel's exhortation that no one be left behind.

We have various and growing forums to express these grievances and form stronger bonds, including our very own RightsCon. At the national and global levels, governments as well as companies are setting up exchanges and adjudication bodies to facilitate open dialogue and accountability. Yet none has the imprimatur of the UN Secretary General nor the legacy of broad participation by governments of small, medium, and large nations that the IGF enjoys. These increasingly specialized forums, whether focused on cybersecurity, corporate-level policies, must be exposed to wider audiences, and work to properly engage civil society – the reason we support the Panel's work toward coordination and mapping of processes.

But norms must become real: implemented robustly and observed with accountability. Now we must expand internet access to the rest of the world's population and enhance rights-respecting digital security across vulnerable populations. We must keep a close eye on the perils of digital identity and call for transparency across the algorithm and machine learning. We must resource civil society that is overtaxed and under attack, struggling to participate in every new forum and body. The IGF is useful for centralizing our efforts and providing us as civil society and all other stakeholders with a platform to address the governance challenges that have not yet even become apparent.

Towards a Governance Protocol for the Social Hypergraph

Bertrand de la Chapelle[57]

A free, open and secure digital society cannot develop without innovative governance mechanisms to address the dangers that threaten it.

A distributed institutional ecosystem was progressively developed for governance OF the internet[58]. It efficiently enabled this unique creation of mankind to now serve more than half the world's population.

However, equivalent efforts were not devoted to developing the necessary policy-making tools for governance ON the internet, i.e. to organize its uses and mitigate in respect of human rights abuses it can allow.

As a result, we witness a legal arms race.

Uncoordinated unilateral measures are adopted under the pressure of urgency, governments increasingly exercise their authority extraterritorially, and company guidelines regulate online communities larger than most countries' populations.

The resulting legal uncertainty, conflicts of laws and long-term unintended consequences could threaten the very benefits of the global network.

The history of institutions reflects the constant effort of mankind to organize itself in larger and larger communities. Enabling the coexistence of several billions of people connected through the internet is nothing short of a civilizational challenge.

Yet, our international system of territorially defined national jurisdictions was adapted to a world with few cross-border interactions. It is now challenged when transnational becomes the new normal.

The principle of non-interference and the strict separation of sovereignties also too often prevent the cooperation that is more necessary than ever to manage common digital spaces.

For the first time, online social applications reveal the social graphs mapping some of our complex individual connections. They also reflect the numerous[59] and heterogeneous groups of all sizes and purposes that humans use to organize themselves, with public or private governance structures.

Our digitally interconnected world needs an approach reflecting this hypergraph[60] structure of society beyond the mere paving of the earth's surface into 190+ separate nations states.

In particular, enabling all stakeholders to address their common challenges requires overcoming the longtime mistrust between states and non-state actors.

Neutral spaces are therefore needed for them to communicate, coordinate and jointly develop policy standards regarding internet uses and abuses.

Governance in cyberspace can only be built issue by issue, with joint agenda setting and policy development by all relevant stakeholders progressively fostering the mutual trust needed for implementation.

Inspiration in that regard can be drawn from the technical interoperability approach that enabled the distributed internet infrastructure we enjoy today.

In a context of increasing normative pluralism where public authorities and private actors concurrently set, implement and enforce norms according to their own internal institutional processes, legal interoperability can help achieve policy coherence and structure the increasingly direct interactions between these diverse actors across borders.

Protocols could make heterogeneous governance frameworks interoperable, like TCP/IP and HTML/HTTP respectively allowed the global internet and the World Wide Web to emerge out of heterogeneous networks and distributed databases.

The importance of fostering this legal interoperability was highlighted at the 3rd Global Conference of the Internet and Jurisdiction Policy Network[61], which took place in Berlin on June 3-5, 2019, in partnership with the Government of Germany.

The Internet & Jurisdiction Policy Network explores how to apply this concept on three concrete and representative transnational issues: content moderation and restrictions, cross-border access to electronic evidence, and actions at the DNS level to address abuses.

The corresponding multistakeholder Contact Groups set up in 2018-19 produced Operational Approaches documents[62] proposing voluntary operational norms, criteria and mechanisms to organize the mutual relationships and responsibilities between different categories of stakeholders.

The outcomes of the policy processes facilitated by the Contact Groups are open for implementation by any actor around the world, unilaterally or through mutual affirmation of commitments.

The concrete results of this collective effort demonstrate the benefits of dedicated thematic neutral spaces and innovative engagement procedures to collaboratively address transnational digital issues.

A governance protocol for the social hypergraph can reduce tensions and enable permission-less policy innovation to create the distributed institutional ecosystem for governance ON the internet that the world urgently needs.

This pioneering methodology could ultimately be replicated to help the progressive development of a global governance architecture that is as transnational and distributed as the internet itself.

Source

[57] This contribution is provided by the author on a personal basis and not on behalf of the participants in the Internet & Jurisdiction Policy Network or its Secretariat.
[58] The complex network of institutions managing the technical architecture, including the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), the Regional Internet Registries (RIRs), the root server operators, ICANN and the DNS Operators.
[59] More than 600 million groups exist on Facebook alone.
[60] For any set of individuals and entities, the collection of all groups (or sub-sets) connecting its members is called the hypergraph of that particular population. https://en.wikipedia.org/wiki/Hypergraph
[61] https://conference2019.internetjurisdiction.net
[62] https://www.internetjurisdiction.net/news/operational-approaches-documents-with-concrete-proposals-for-norms-criteria-and-mechanisms-released

The Future of Work, AI and the German Trade Union Approach

Anette Mühlberg

The “age of digital interdependence”, as referred to by the “UN High Level on Digital Cooperation”, will have fundamental consequences for the future of work. The International Labour Organisation (ILO), headquartered in Geneva, has those challenges discussed since years. In January 2019, a “Global Commission on the Future of Work”, co-chaired by the Swedish Primeminister Sven Lofgren and the President of South Africa, Cyril Ramaphosa, published its final report where they state that “technological advances – artificial intelligence, automation and robotics – will create new jobs, but those who lose their jobs in this transition may be the least equipped to seize the new opportunities. Today’s skills will not match the jobs of tomorrow and newly acquired skills may quickly become obsolete.”[63]

With other words, how to create opportunities for a decent work in the age of digital interdependence is a key element in the development of digital cooperation in the 2020s. The ILO Commission did propose “a human-centred agenda for the future of work that strengthens the social contract by placing people and the work they do at the centre of economic and social policy and business practice.” And it puts “education” in the center of a long-term strategy by calling for “a universal entitlement to lifelong learning that enables people to acquire skills and to reskill and upskill. Lifelong learning encompasses formal and informal learning from early childhood and basic education through to adult learning. Governments, workers and employers, as well as educational institutions, have complementary responsibilities in building an effective and appropriately financed lifelong learning ecosystem.”

In this context, one of the fundamental challenges in the forthcoming decade will be the handling of Artificial Intelligence (AI). As the OECD has outlined “Artificial intelligence is reshaping economies, promising to generate productivity gains, improve efficiency and lower costs. It contributes to better lives and helps people make better predictions and more informed decisions. These technologies, however, are still in their infancy, and there remains much promise for AI to address global challenges and promote innovation and growth. As AI’s impacts permeate our societies, its transformational power must be put at the service of people and the planet. At the same time, AI is also fuelling anxieties and ethical concerns. There are questions about the trustworthiness of AI systems, including the dangers of codifying and reinforcing existing biases, such as those related to gender and race, or of infringing on human rights and values, such as privacy. Concerns are growing about AI systems exacerbating inequality, climate change, market concentration and the digital divide. No single country or actor has all the

answers to these challenges. We therefore need international co-operation and multi-stakeholder responses to guide the development and use of AI for the wider good."[64]

The ethical dimension of Artificial Intelligence is a key component of the future of work in a connected world. Insofar it was very helpful and important that the OECD adopted also a document with five principles which should guide future discussions and actions around AI.

The OECD Recommendation identifies five complementary values-based principles for the responsible stewardship of trustworthy AI:

1. AI should benefit people and the planet by driving inclusive growth, sustainable development and well-being.
2. AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society.
3. There should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them.
4. AI systems must function in a robust, secure and safe way throughout their life cycles and potential risks should be continually assessed and managed.
5. Organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles.[65]

Those OECD principles got broad international support. The fact, that the G20 Summit Meeting in Osaka in June 2019 confirmed the principles gives them even a more universal character.

However, much more has to be done to understand the implications of AI for the future of work as well as for other key issues related to the "age of digital interdependence" as peace and international security, sustainable developmet and the protection of human rights.

The German Trade Union ver.di has those issues on its agenda since more than ten years. 2008, ver.di adopted a document called "The Berlin Manifesto" where it was stated that "open access to the Internet is now an essential feature of any information society. Not having Internet access means being excluded from vast areas of social and family life, being unable to avail

oneself of educational opportunities and access information, and being excluded from the democratic process – both in one's private and working life." And the Manifesto made clear that "education and access to knowledge are increasingly important basic rights. New technologies have made it significantly easier to access and exchange information and knowledge. We want to secure, use and expand these opportunities for social, economic and cultural participation."

Just recently, in January 2019, the German Confederation of Trade Unions has published a special working paper on AI.[66] Like ILO or OECD, the paper recognized the hypbid nature of the role of AI in the age of digital interdependence. To maximise the opportunties and to minimize the risks is a good general guideline. But the real problem is how to translate such a guideline into the day to day activties of inolved stakeholders.

"Ultimately", says the paper, "the aim is to achieve a good balance between new, data-based business models and the improvement and optimisation of processes on the one hand, and the interests of employees, above all job security and better working conditions in the future, on the other. This requires openness and commitment to the participation, co-determination and negotiation processes described above. At the same time, ethical limits, social standards and 'fail-safes' should be set: The human user should always have the right of final decision. In addition, labour law consequences for employees which could theoretically result from 'digital management' or surveillance must be strictly excluded. Failing this, acceptance issues could become a serious obstacle to the implementation of AI systems in the workplace even if ergonomics were improved."

To achieve such a "good balance" it needs a multistakeholder discussion where all involved and affected parties are having the opportunity on equal footing to participate in policy development and decision making around the future of AI in the digital age. The UN sponsored IGF is a great opportunity to disucss next steps. And an IGF+, as proposed by the UN High Level panel could be helpful to translate the outcome of the multistakehololder IGF discussions into more concrete decisions.

Insofar, the recommendation of the ILO "that all relevant multilateral institutions strengthen their joint work on this agenda ... and establish substantive working relations between the World Trade Organization (WTO), the Bretton Woods institutions and the ILO" is useful. There are strong, complex and crucial links between trade, financial, economic and social policies. The success of the human-centred growth and development agenda depends heavily on coherence across these policy areas.

Source

[63] *Work for a brighter future, Final Report of the Global Commission on the Future of Work, ILO, Geneva, January 2019, see: https://www.ilo.org/global/topics/future-of-work/publications/WCMS_662539/lang--en/index.htm*

[64] *Artificial Intelligence in Society, OECD, Paris, June 2019, in: http://www.oecd.org/going-digital/artificial-intelligence-in-society-eedfee77-en.htm*

[65] *https://www.oecd.org/going-digital/ai/principles/*

[66] *Artificial Intelligence and the Future of Work A discussion paper of the German Confederation of Trade Unions concerning the debate on artificial intelligence (AI) in the workplace. Berlin, January 2019*

The Future of the IGF

Carlos A. Afonso

Since the IGF process began, based on the Internet governance conceptualization established in the 2005 UN Working Group on Internet Governance and sacralized in the Tunis edition of WSIS, a growing, diverse set of Internet governance-related initiatives has sprouted.

On the one hand, actions by specific sectors or multistakeholder and multilateral initiatives launched international events in which sets of commitments or recommendations have been established, frequently with no meaningful or explicit relation to each other. Reinventing the wheel has been part of the outcomes of some of these events and processes – and the wheels reinvented so far do not run as smoothly as expected.

On the other hand, the welcome proliferation of national and regional Internet governance dialogue spaces, not directly related to the IGF (in many cases their timing does not sync with the IGF, do not take into account the themes defined by the MAG for their own dialogue program, and might not even be considered part of the IGF intersessional efforts), but somehow converging to the main event – the dozens of events baptized more or less informally as national or regional IGFs.

This is a non-exhaustive list of initiatives (not necessarily coordinated or interacting with the IGF), which keeps growing:

- Internet & Jurisdiction Policy Network (2012-ongoing)
- Alliance for Affordable Internet (A4AI, 2013-ongoing)
- Smart Africa (2013-ongoing)
- Global Commission on Internet Governance (GCIG, 2014-2016)
- NetMundial Conference (2014)
- Global Cyberalliance (2015-ongoing)
- IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems (2016-ongoing)
- Global Commission on Stability of Cyberspace (GCSC, 2017-ongoing)
- Charter of Trust (2018-ongoing)
- Cybersecurity Tech Accord (2018-ongoing)
- Web Foundation‘s Contract for the Web (2018-ongoing)

- High Level Panel on Digital Cooperation (HLPDC, 2018-2019)
- Paris Call for Trust and Security in Cyberspace (2018)
- International Panel on Artificial Intelligence (2019)

These initiatives generate many recommendations (with several overlaps), basically under the general goal of proposing actions to ensure a single, open and secure Internet for everyone. The list is testimony to the intense interest in finding ways to tackle several global challenges of Internet governance, but they lack a much needed coordination or integration of efforts in order to be more effective – something the HLPDC report recognizes as one of the six main gaps in these processes as a whole.

I trust several other commentators have covered the relevant aspects of the HLPDC proposals. I wish to make just a few observations.

The IGF Plus proposal contemplates a MAG with additional functions. On the basis of my experience in earlier and current MAGs, I need to remind proponents that nearly all MAG members are volunteers who have their other time-consuming jobs. To cope with the current challenges is already hard enough, and the HLPDC proposal for the MAG seems to overlook this aspect. One of the proposed additional functions would be identifying „moments when emerging discussions in other forums need to be connected". Here is another reason for including the above non-exhaustive list of „other forums" – this task would be an impossible challenge for a voluntary group. In addition, this would be a function better carried out by the proposed Observatory/Help Desk, if these were to be implemented.

While recognizing the need of efforts to monitor and consolidate so many processes, this would ought to be the job of a specialized staff on a full-time basis. Should this be done as part of a UN-led forum? Some critics of the report think the whole idea of the Observatory/Help Desk, or even the Cooperation Accelerator, does not belong to the IGF at all, and should be thought of in other formats and fora. I agree with this view.

As to the Policy Incubator, I have to say that the intersessional activities (the many Dynamic Coalitions, the Best Practice Forums and so on) try to do just that, with the difficulties inherent to a voluntary effort, practically since the beginning of the IGF. There is a need here for qualified help in gathering and consolidating their ongoing work and recommendations.

ACADEMIC COMMUNITY

Three Eras of Digital Governance

Jonathan Zittrain [67]

To understand where digital governance is going, we must take stock of where it's been, because the timbre of mainstream thinking around digital governance today is dramatically different than it was when study of "Internet governance" coalesced in the late 1990s.

Perhaps the most obvious change has been from emphasizing networked technologies' positive effects and promise – couched around concepts like connectivity, innovation, and, by this author, "generativity"[68] – to pointing out their harms and threats. It's not that threats weren't previously recognized, but rather that they were more often seen in external clamps on technological development and upon the corresponding new freedoms for users, whether government intervention to block VOIP services like Skype to protect incumbent telco revenues, or in the shaping of technology to effect undue surveillance, whether for government or corporate purposes.

The shift in emphasis from positive to negative corresponds to a change in the overarching frameworks for talking about regulating information technology. We have moved from a discourse around rights – particularly those of end-users, and the ways in which abstention by intermediaries is important to facilitate citizen flourishing – to one of public health, which naturally asks for a weighing of the systemic benefits or harms of a technology, and to think about what systemic interventions might curtail its apparent excesses.

Each framework captures important values around the use of technology that can both empower and limit individual freedom of action, including to engage in harmful conduct. Our goal today should be to identify where competing values frameworks themselves preclude understanding of others' positions about regulation, and to see if we can map a path forward that, if not reconciling the frameworks, allows for satisfying, if ever-evolving, resolutions to immediate questions of public and private governance.

The Rights Era

The original consideration of threats as external to the otherwise-mostly-beneficial uses of tech made for a ready framing of Internet governance issues around rights, and in particular a classic libertarian ethos of the preservation of rapidly-growing individual affordances in speech – "now anyone can speak

without a gatekeeper!" – against encroachment by government censorship[69] or corporate pushback motivated by the disruption of established business models.

A good example in the first category are the debates around the U.S. Communications Decency Act of 1995, which sought to keep indecent material away from minors by penalizing those who indiscriminately made it available online. The Supreme Court struck down[70] the core provisions of the CDA in 1997 on First Amendment grounds, holding that too much protected speech would be chilled by the law, and successor laws met a similar fate.[71] Another example can be found in the early and then not-officially-acknowledged efforts by the Chinese government to block citizens' access to websites critical of the state, something viewed among those studying Internet governance as an unalloyed wrong, not least because of the lack of due process, including notification, in effecting any blocks.

When the Internet's affordances for near-instant file transfer led to objections by publishers and other copyright holders over copyright infringement, those against stepped-up enforcement or new requirements for intermediaries relied on a rights-centric account.[72] Copyright itself establishes legally protected interests – rights – but the sorts of interventions required to continue to secure those rights in practice were described early and often as overly burdening individual rights, whether through content takedown schemes to be effectuated by intermediaries, or individual lawsuits filed against those engaged in the sharing of copyright material.

It is in intermediary liability that the most significant regulatory battles have unfolded, and that is likely to remain so. The shaping of end-user behavior through rule and sanction was, and is, difficult. But intermediaries can be persuaded or required to shape users' technological experiences to channel them away from objectionable or illegal behavior, whether through hardware or operating system design of smart phones, or the shaping of software and services used by billions, such as by the most prominent social media platforms. The rights framework generally finds that such shaping should be limited, and in the late 1990s that was reflected in American law. For example, section 230 of the Communications Decency Act[73] – a part of the Act that remained after the Supreme Court struck down the rest – provided for immunity by platforms against many forms of potential liability occasioned by those platforms hosting and amplifying the speech of others, including end-users. And the notice-and-takedown safe harbors of the Digital Millennium Copyright Act[74] offered a low-impact, routinized way for platforms to respond on a case-by-case basis to copyright complaints for others' material. Still, some scholars advocating for a rights framework thought these provisions went too far.[75]

It was also in this rights-centric era that ICANN came about, chartered to bring consistency and "stakeholder" representation to policy-inflected decisions around global Internet naming and numbering, such as the number and nature of top-level domains (TLDs) like .com and .uk, including who would be charged with giving out or selling second-level names under those domains, and under what conditions. Apart from the simple desire to establish and regularize who would be earning money from the sale of domain names, the main concern aired as ICANN came into its own was about whether ICANN would itself become a censor of Internet content.[76] ICANN could, the theory went, use its certification of TLD registries to, through a cascade of contracts, make for the suspension or transfer of domain names comprising or pointing to "bad stuff." Describing material in more precise terms of outright illegality has been difficult, since it would require a choice of which jurisdiction's definition of illegality to apply.[77]

As it has happened, concerns about ICANN becoming the Internet police – infringing on individual rights – has so far seen ICANN's catalyzation of a suspension power to be only in the area of domain names whose very nature indicate a bad faith registration amounting to a form of trademark infringement.[78] Domain names that are not so infringing, but that are used as mnemonics for destinations containing harmful or illegal content, have generally not been touched by ICANN's policies.[79]

The Public Health Era

I was among those who celebrated the benefits of a rapidly-expanding Internet, both in scope and capability, thanks to the generative contributions of millions of users in code and content. For example, Internet protocols made possible the growth of the World Wide Web as an Internet application without any approvals sought or needed; the Web facilitated the rise of online wikis, and those wikis made possible the phenomenon of Wikipedia, which in turn invited contributions of content from people who themselves were not interested in coding software. Even amidst this celebration, in my case circa 2007, lay a new round of problems, which I described as part of the Generative Pattern[80]:

1. An idea originates in a backwater.
2. It is ambitious but incomplete. It is partially implemented and released anyway, embracing the ethos of the procrastination principle.
3. Contribution is welcomed from all corners, resulting in an influx of usage.
4. Success is achieved beyond any expectation, and a higher profile draws even more usage.
5. Success is cut short: "There goes the neighborhood" as newer users are not conversant with the idea of experimentation and contribution, and other users are prepared to exploit the openness of the system to undesirable ends.
6. There is movement toward enclosure to prevent the problems that arise from the system's very popularity.

Indeed, the cutting short of success by those who subvert the system and take advantage of its now-many users – a problem arising from the very openness of the system itself – began in earnest by 2010.[81] Cybersecurity had been my central worry; it was clear those problems were no longer wholesale, business-to-business issues, but something touching all of users' online activities. Without urgent attention given to developing a collective, generative defense, I worried about the Generative Pattern's conclusion: top-down enclosure to protect everyone by curtailing everyone's freedoms, demanded by the users themselves.[82]

These kinds of concerns and how to meet them don't much benefit from a rights discourse, especially as they involve the mutual (if surely not symmetric) violation of rights by users against users, at least from a technical network point of view. Rather, they have much in common with how we talk about public health.[83] They emphasize the interlinkages among us, the way that problems can all too easily spread from one person or node to another, and the need for systemic intervention and shaping to prevent harm from accruing, regardless of who might be to blame for first injecting harm into the system. Worries around viral malware hopping from one server to another have grown to be worries about mis- and disinformation hopping from one credulous person to another, abetted by social network intermediaries who amplify controversial or outright false content if it increases user engagement with the platforms. Indeed, there is a literal public health dimension to misinformation today, as screeds and videos against even basic public vaccination, long proven to be beneficial, circulate and previously-near-defeated illnesses like measles make a startling comeback.[84]

A public health framework is much more geared around risks and benefits than around individual rights. Pointing out harmful speech in a rights discourse might typically result in what amounts to a shrug and a declaration that such excesses are the "price of freedom," a sign that our commitment to rights requires sacrifice precisely where people would otherwise find the exercise of rights objectionable. In the public health frame, we instead are asked to gather empirical data about benefits and harms, and to brainstorm ways that the latter might be decreased without unduly trimming the former.

The Process, or Legitimacy, Era

Reconciling rights and public health frameworks is not easy, not only between two people whose normative commitments fall into the respective camps, but also often within a single person: each framework can speak powerfully to us, favoring both individual liberty – including a skepticism over the responsible exercise of state power – while also sensitive to the fact that we live in a tightly-coupled, interlinked society, all the more so with the rise of networked technologies, and there are times when collective security calls for organized and perhaps even mindful architectural intervention. Moreover, the rise of intermediaries that not only facilitate communication with people we already know we want to reach – think email, or instant messaging – but also discovery of new ideas and people, means that there's a less-agreed-upon conception of neutrality or non-intervention. When Facebook or Twitter has millions of candidate items with which to salt a feed, any decision about what to show or recommend to you next is going to be freighted in a way that speeding delivery of a note between two discrete people is not.[85]

We also happen to be in a time of very little trust in many if not most civic and private institutions, especially national and transnational ones. A simple vote in a legislature, or split decision from a court, seems not to well settle the complex and deeply debated issues that spring around digital governance.

This may be why we've lately seen some of today's most powerful private intermediaries, such as Facebook, Google, and Cloudflare, expressing uncertainty or contradiction about their own policies for intervention, a.k.a. intermeddling, vs. abstention, a.k.a. abdication.[86] The rise of mainstream AI means that even detailed policies can be applied – or misapplied – in real time to the activities of billions of people so voluminous to otherwise be beyond moderation.

These companies have made some attempts to take decisions about content or user behavior out of their terms-of-service, customer support channels, and into some new institutional configuration meant to match the gravity

of the questions around abuse, harassment, and the promotion or stifling of political speech.[87] Facebook has proposed an independent review board, whose decisions would be binding upon the company. Others have sought internal boards to reflect upon ethically-freighted decisions before making them. And regulators, loathe to try to make the decisions themselves at scale, have sought to require private intermediaries to impose particular standards without offering much by way of detail, such as in the current implementation of the European right to be forgotten.

What the field of digital governance, and indeed the world at large, needs, are ideas for new institutions and institutional relationships that can come to closure, however temporary, on some of these questions, and, like the project of law and political processes themselves, understand that all views will not and cannot be reconciled. But ideally even those who feel they have lost in a particular dispute or debate will not feel that they have been taken advantage of, or that the project to which they are contributing and are subject to – some digital expression of ideas and power – is not morally bankrupt.

The key to the next era of digital governance lies not in some abstract evaluation of whether our affordances are structured in ways that are correct or incorrect on one person's view, but rather if they are legitimate because of the inclusive and deliberative, and where possible, federated, way in which they were settled.

Source

[67] I thank John Bowers for top-notch research assistance.

[68] http://yupnet.org/zittrain/

[69] Two noteworthy entries in this genre are Timothy May's "The Crypto Anarchist Manifesto" https://www.activism.net/cypherpunk/crypto-anarchy.html (1988), and John Perry Barlow's "A Declaration of the Independence of Cyberspace" https://www.eff.org/cyberspace-independence (1997). Both May and Barlow inveigh against governments bent on applying conventional rules and governance standards to the new terrain of cyberspace, a practice which they portray as being both intellectually bankrupt and doomed to fail. Both argue that cyberspace represents a fundamentally new and different sort of social and political construct, with a rights paradigm that is entirely its own. Per Barlow, "Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions." Both – in these writings and elsewhere – are fascinated by questions of intellectual property, fertile ground for the disruption of traditional structures of right and privilege. Gleefully anticipating the reconfiguring effects of cryptography, May writes that "just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery [of cryptography] come to be the wire clippers which dismantle the barbed wire around intellectual property."

[70] https://www.law.cornell.edu/supremecourt/text/521/844

[71] https://www.law.cornell.edu/supct/html/03-218.ZO.html; For an account of the protracted 10-year judicial struggle over the constitutionality of the Child Online Protection Act, itself developed in the wake of the CDA strikedown, refer to this blog post from Lauren Gelman at Stanford Law School: http://cyberlaw.stanford.edu/blog/2008/11/child-online-protection-act-still-unconstitutional

[72] Here too Barlow's writings comprise a well-known exemplar. In his 1992 essay "Selling Wine Without Bottles: The Economy of Mind on the Global Net" https://www.eff.org/pages/selling-wine-without-bottles-economy-mind-global-net Barlow once again takes aim at the lawyers and corporations vigorously defending what he sees to be entirely obsolete copyright doctrine: "Intellectual property law cannot be patched, retrofitted, or expanded to contain the gasses of digitized expression... Most of the people who actually create soft property – the programmers, hackers, and Net surfers – already know this. Unfortunately, neither the companies they work for nor the lawyers these companies hire have enough direct experience with immaterial goods to understand why they are so problematic. They are proceeding as though the old laws can somehow be made to work, either by grotesque expansion or by force. They are wrong." Barlow's words contra governments and corporations alike presage the copyright wars of the late 1990s and early 2000s, in which old and new theories of rights competed – and ultimately compromised – to become doctrine.

[73] https://www.law.cornell.edu/uscode/text/47/230

[74] https://www.law.cornell.edu/uscode/text/17/512

[75] Many of these concerns relate to the DMCA notice-and-takedown system's potential utility as a private censorship tool. In a New Republic article from 2000 entitled "Call it the Digital Millennium Censorship Act: Unfair Use" http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/5238/unfairuse.pdf?sequence=1&isAllowed=y, intellectual property scholar Julie Cohen argued that "DMCA's notice and takedown provisions – which don't require prior court review of takedown demands – threaten to substitute private censorship for judicial process." These concerns persisted as the DMCA matured. In 2004, Siva Vaidhyanathan wrote that "DMCA...has emerged as the law of choice for censoring criticism and commentary in the electronic environment."(https://firstmonday.org/article/view/1133/1053) In 2019, Eugene Volokh wrote about the continuing use of fraudulent DMCA takedown requests to suppress online content – including, bizarrely, his own writings on fraudulent DMCA takedowns, see here: https://reason.com/2019/01/23/attempt-to-get-google-to-vanish-my-artic

[76] Indeed, ICANN's potential capabilities in the censorship domain struck some as being particularly troubling exactly because ICANN was formed as a non-governmental entity, and therefore functioned at some distance from conventional modes of democratic recourse. In a widely-cited article titled "ICANN and the Problem of Legitimacy" https://scholarship.law.duke.edu/dlj/vol50/iss1/5/ – published in 2000, soon after ICANN's 1998 founding – Jonathan Weinberg warned that "ICANN's role is on generally played in our society by public entities. It is setting rules for an international communications medium of surpassing importance. That task had historically been performed by a U.S. government contractor in an explicitly public-regarding manner. ICANN is addressing important public policy issues. Further, it is implementing some of its choices via means that look uncannily like command-and-control regulation. If ICANN is to establish its legitimacy, it must be able to answer the charge that its exercise of authority is inconsistent with our ordinary understandings about public power and public policy making." Milton Mueller's 1999 paper "ICANN and Internet Governance: Sorting Through the Debris of 'Self-Regulation'" https://papers.ssrn.com/sol3/papers.cfm?abstract_id=203973 offers analysis of a range of other potential issues with a "self-regulating" ICANN: "ICANN looks and acts more like an incipient inter-governmental agency than a private sector corporation. The process of forming ICANN has been mired in so much factionalism and political controversy that references to 'consensus based' self-regulation are laughable." Skepticism towards ICANN even had a homepage: icannwatch.org (2002 archive: https://web.archive.org/web/20020325085800/http:/icannwatch.org/) was launched as a sort of watchdog to monitor these concerns and others.

ICANN's charter established that substantive decisions regarding the rights and privileges of individuals seeking to take part in a transformative communications technology would be delegated to a non-public entity. As this essay will go on to argue further, we've seen similar – and perhaps less technocratic, more visible – tensions play out in controversies around the content governance practices of contemporary internet platform companies.

[77] What's more, the impracticality of the notion of an "extraterritorial" internet unbound by the laws of any given country – favored by many rights mavens of the early internet era – factors into the analysis here. These narratives were complicated by the fact that, in the early days of the internet and now, governments, and particularly those with authoritarian characteristics, have a tendency to pressure Internet companies to police content and expression in accordance with localized laws and norms. Jack Goldsmith and Tim Wu offer a thoughtful reflection on this tempering of the dreams of the techno-utopians in their 2006 book Who Controls the Internet: Illusions of a Borderless World. So even if ICANN were to attempt to establish itself as an interventionary global governance body, its actions would nonetheless remain subject to those of governments themselves.

[78] ICANN's process for adjudicating copyright disputes over domain names is the Uniform Domain-Name Dispute-Resolution Policy (https://www.icann.org/resources/pages/dndr-2012-02-25-en), launched in December of 1999. The UDRP holds that, in order to wrest control of a domain name from a registrant, a complainant must prove three elements, See here: https://www.icann.org/resources/pages/dndr-2012-02-25-en:

"(i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

(ii) you have no rights or legitimate interests in respect of the domain name; and

(iii) your domain name has been registered and is being used in bad faith."

The apparent ambiguity of the UDRP has long been a topic of consternation amongst lawyers and policymakers. A Berkman Klein Center analysis(https://cyber.harvard.edu/udrp/analysis.html) from soon after its implementation points to dozens of precedential proceedings, with each one offering refinements to an interpretation of concepts like "bad faith" and "legitimate interests" under the UDPR.

[79] The idea that ICANN might for some reason begin to police forms of abuse – illegal or otherwise – unrelated to trademark protections has long concerned advocates for individual online rights. In 2013, ICANN revised its agreement with registrars to include what Electronic Frontier Foundation Jeremy Malcolm called, in a series of blog posts titled "EFF to ICANN: Don't Pick Up the Censor's Pen" (https://www.eff.org/deeplinks/2017/10/eff-icann-dont-pick-censors-pen), a "provision requiring registrars to 'receive reports of abuse involving Registered Names' and to 'take reasonable and prompt steps to investigate and respond appropriately.'" Much was made of the ambiguity around this phrasing – what might a "report of abuse" entail beyond the domain of copyright? – prompting ICANN to release a lengthy 2015 blog post decisively titled "ICANN Is Not the Internet Content Police" (https://www.icann.org/news/blog/icann-is-not-the-internet-content-police). In the post, ICANN Chief Contract Compliance Officer Allen R. Grogan argues that

"Though the appropriate interpretation of 2013 RAA is the subject of debate, there are clear-cut boundaries between ICANN enforcing its contracts and the enforcement of laws and regulations by the institutions mentioned earlier. A blanket rule requiring suspension of any domain name alleged to be involved in illegal activity goes beyond ICANN's remit and would inevitably put ICANN in the position of interpreting and enforcing laws regulating website content. At worst, it would put ICANN squarely in the position of censoring, or requiring others to censor, Internet content."

In 2017, however, EFF and other allied organizations were raised a cry – detailed in the same EFF blog post – over ICANN's appointment of a former law enforcement official to the post of Consumer Safeguards Director. Per Malcolm, "a draft report [PDF - https://www.icann.org/en/system/files/files/cct-rt-draft-report-07mar17-en.pdf] of ICANN's Competition, Consumer Trust and Consumer Choice Review Team recommends that strict new enforcement and reporting obligations should be made compulsory

for any new top-level domains that ICANN adopts in the future. ICANN's Non-Commercial Stakeholder Group (NCSG - https://community.icann.org/display/gnsononcomstake/Home) has explained [PDF - https://mm.icann.org/pipermail/comments-cct-rt-draft-report-07mar17/attachments/20170520/f90bb73f/CCTRTInitialDraftCommentsforNCSG.pdf] why many of these recommendations would be unnecessary and harmful.

A subteam of this same Competition, Consumer Trust and Consumer Choice Review Team has also recently released a draft proposal [PDF - https://community.icann.org/download/attachments/59649268/DNS%20Abuse%20Chapter%20Draft_2017_10_18.docx?version=1&modificationDate=1508319002000&api=v2] for the creation of a new DNS Abuse Dispute Resolution Procedure (DADRP) that would allow enforcement action to be taken by ICANN against an entire registry if that registry's top-level domain has too many „abusive" domain names in it... If this proposed DADRP goes ahead, registries could come under pressure to go on a purge of domains if they wish to avoid being sanctioned by ICANN."

[80] http://yupnet.org/zittrain/2008/03/14/chapter-4-the-generative-pattern/#122

[81] In many cases – before and after 2010 – some use of the internet's affordances to abuse others was met with encouragement. The practice of „trolling," for its own sake, intentionally seeking to shock, annoy, or enrage other internet users, became both a hobby and a sort of spectator sport, with content consumers watching, often gleefully, the sowing of chaos. Whitney Phillips argues in a 2019 paper titled "It Wasn't Just the Trolls: Early Internet Culture, 'Fun,' and the Fires of Exclusionary Laughter" that the widespread acceptance (even embrace) of an internet culture comfortable with many forms of insensitivity and abuse laid much of the groundwork for some of the toxic online dynamics of today. Her account asks us to review the internet libertarianism of the rights era, whose proponents typically might not in person have been on the receiving end of attacks against already-marginalized groups.

[82] The "walled gardens" of today's platforms are, in some sense, a manifestation of this natural conclusion. But these ostensibly tightly-controlled spaces have been the site of some of the most sustained claimed abuses and most immediately-apparent harms of public health era, from allegedly social media-fueled genocides in Myanmar (https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html) to the Cambridge Analytica (https://www.theguardian.com/uk-news/2019/mar/17/cambridge-analytica-year-on-lesson-in-institutional-failure-christopher-wylie) scandal. Concentration creates new levers for governance over what might otherwise be messy generative networks, but it also offers up target-rich environments to those seeking to do harm.

[83] One clear marker of the shift from a discourse of rights to a discourse of public health has been careful reevaluation of the stipulations of CDA 230, with critics arguing that it often unduly insulates culpable internet platforms from responsibility for the harms arising from their actions. In their 2010 book The Offensive Internet, for example, Martha Nussbaum and Saul Levmore describe how the internet has generated unprecedented opportunities for reputational harm to individuals. This harm, they argue, has been enabled in large part by CDA 230: "A withdrawal of [CDA 230] immunity could, without constitutional difficulty, restore the symmetry between website operators and publishers of newspapers, which can of course be sued for damages if they publish defamatory material." Even many scholars uncomfortable with an aggressive rollback of CDA 230 have placed its provisions under a microscope. In her paper "The New Governers"(https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf) Kate Klonick details the often unwieldy mixture of constitutional analogies, one-off decisions, and economic and political incentives which drive platforms' content governance paradigms under CDA 230.

The recent case of Herrick v. Grindr has furnished an illustration (https://www.lawfareblog.com/herrick-v-grindr-why-section-230-communications-decency-act-must-be-fixed) of how CDA 230 protections can insulate companies complicit in facilitating real-world harms from liability. The plaintiff's ex-boyfriend used the gay dating app to manipulate upwards of 1,000 men into threatening and harassing the plaintiff, often in real life, over the course of almost a year. The U.S. Court of Appeals for the Second Circuit confirmed a dismissal of the complaint on the grounds of Grindr's CDA 230 immunity in March of 2019.

[84] *Many criticisms of platform behavior relating to vaccine controversies center on the sorting and ordering of content (https://www.mobihealthnews.com/content/facebook-instagram-limit-spread-vaccine-misinformation) feeds, whether in the context of a search engine or social media site. It's worth noting, however, that public health concerns relating to content ordering are nothing new. In 2004, a Google search for 'jew' would return the anti-semitic website jewwatch.com. Google refused (https://www.snopes.com/fact-check/found-out-about-jew/) to alter its results, stating that "We find this result offensive, but the objectivity of our ranking function prevents us from making any changes." In the case of vaccine misinformation, however, pressure from lawmakers (https://schiff.house.gov/news/press-releases/schiff-sends-letter-to-google-facebook-regarding-anti-vaccine-misinformation) and the public (https://www.businessinsider.de/doctors-warn-google-twitter-facebook-anti-vaxxers-2019-3?r=US&IR=T) has driven commitments to action on the part of Facebook (https://newsroom.fb.com/news/2019/03/combatting-vaccine-misinformation/) and Twitter (https://www.theverge.com/2019/5/14/18623494/twitter-vaccine-misinformation-anti-vax-search-tool-instagram-facebook), among others.*

[85] *Some platforms have struggled to develop workable frameworks for navigating the (algorithmically mediated) spectrum between driving the virality of content and taking it down. When it comes to public health considerations, platforms now have a tendency to lean on the language of demotion rather than that of removal. Whether this tactical shift represents a move towards or away from censorship (https://qz.com/1594392/instagram-will-demote-inappropriate-content-and-self-expression-along-the-way/) is very much up for debate.*

In a November 2018 blog post entitled "A Blueprint for Content Governance and Enforcement" (https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/) Mark Zuckerberg asserted – with visuals! – that "[internal Facebook] research suggests that no matter where we draw the lines for what is allowed, as a piece of content gets close to that line, people will engage with it more on average – even when they tell us afterwards they don't like the content." He proposes that this problem might be solved by demoting content as it approaches the line, inverting this engagement pattern and penalizing borderline content. But there may be good reason to believe that provocative content that plays close to Facebook's boundaries without violating them serves an important discursive function. Controversial forms of speech may well verge into toxicity much of the time, but such speech can also communicate strong emotions, drive changes in norms, and generally constitute free and productive expression.

[86] *In an August 2019 post (https://blog.cloudflare.com/terminating-service-for-8chan/) describing Cloudflare's decision to halt service to 8chan, a discussion board associated with hate groups and the perpetrators of a number of mass shootings, Cloudflare CEO Matthew Prince appealed for guidance from public decision makers: "Cloudflare is not a government. While we've been successful as a company, that does not give us the political legitimacy to make determinations on what content is good and bad. Nor should it. Questions around content are real societal issues that need politically legitimate solutions. We will continue to engage with lawmakers around the world as they set the boundaries of what is acceptable in their countries through due process of law. And we will comply with those boundaries when and where they are set."*

[87] *A number of scholars including Thomas Kadri and Kate Klonick have argued that the specificity and impact of these decision making processes call for a form of constitution-building within the platforms. In "Facebook v. Sullivan: Public Figures and Newsworthiness in Online Speech"(https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3332530) the two argue for the articulation of clear, oversight-friendly processes for the establishment and review of content governance standards. Striking a balance between the representation of user interests and the complex operational realities of administering a platform will be one of the greatest challenges to face internet platforms to date.*

Considerations on High-Level Panel's "Internet Governance Plus" Model

William Drake

The UN Secretary-General's High-level Panel on Digital Cooperation released its report in June 2019.[88] The report is to be discussed at the Internet Governance Forum (IGF) in Berlin in November 2019. The report proposes consideration of what it calls three possible architectures of global digital cooperation: an Internet Governance Forum Plus; a **Distributed Co-Governance Architecture** that would assemble transnational policy networks under an umbrella **"network of networks", apparently operating outside the United Nations system**; and a Digital Commons Architecture that would promote the UN's Sustainable Development Goals by assembling multistakeholder "tracks," each of which could be "owned" by a leading organization such as a UN agency, an industry or academic consortium or a multi-stakeholder forum.

In addition, the **report invites all stakeholders to commit to a Declaration of Digital Interdependence**. It also recommends a multi-stakeholder alliance, involving the UN, to create a platform for sharing digital public goods; the creation of regional and global digital "help desks" to assist governments and stakeholders in understanding digital issues and developing their capacities; a Global Commitment on Digital Trust and Security; and the marking of the UN's 75th anniversary in 2020 with a Global Commitment for Digital Cooperation.

It is important that the UN Secretary-General has taken a strong interest in digital issues and convened an effort to inject new ideas into the global governance discussion. Insofar as some of the panel's proposals are reasonably anodyne and focused on normative declarations and information-sharing, they may navigate the waters of inter-state rivalries to adoption. However, it could **prove more difficult to attract the necessary buy-in and commitment to a new operational model for global digital cooperation.**

The report's schematic presentation of the three alternative models may present hurdles to an inclusive and systematic assessment of their merits and feasibility. Indeed, just three of the report's forty-seven pages are devoted to specifying what are really the panel's main "deliverables." This was an interesting choice, inter alia because probing questions about the models were raised in some of the outreach meetings conducted during the panel's work.[89] In any event, the final product does not offer much more detail than the initial sketches that were shared.

One could argue that in some cases it makes sense to frame a proposal for international cooperation in general terms and then pursue elaboration and sense of collective ownership in the public vetting stage. After all, the 2005 report of the Working Group on Internet Governance did not provide extensive detail in proposing the creation of the IGF. But **the IGF was pitched as primarily a space for dialogue and collective learning,** which is a less demanding construct than a complex operational system intended to engineer new types of collaborative outcomes that include policies and norms. In addition, the historical context is very different today from that of the World Summit on the Information Society (WSIS), and the models go beyond the issues debated and the multi-stakeholder processes undertaken since that time. As such, one could argue that more functional and political explanation of the models would have helped to facilitate the international community's engagement.

To illustrate the challenges ahead, this brief chapter highlights some of the issues raised by one of the models: the Internet Governance Forum Plus. All three models merit analysis but space limitations allow room to assess just one, and as this volume is a contribution to an IGF meeting the choice seems apt. Moreover, the IGF+ might be viewed by some actors as the most viable of the three since as the IGF already has a UN mandate, an institutional form of sorts, and governmental and stakeholder support. In contrast, the other two models could require heavy lifting to get off the ground, especially in the midst of a recession in international cooperation that has extended even to the Universal Postal Union.

The one-page IGF+ model has four main components. First, there would be an Advisory Group based on the IGF's current Multi-stakeholder Advisory Group (MAG). It is not clear what the advantage would be in dropping "multistakeholder" from the group's name. **The report also explicitly limits the Advisory Groupsits role to preparing annual meetings and identifying policy issues to be explored.** One can imagine concerns being expressed on one or both of these points.

Second, there would be a **Cooperation Accelerator that would catalyze issue-centered cooperation across a wide range of institutions, organizations and processes.** The Accelerator would "identify points of convergence among existing IGF coalitions, and issues around which new coalitions need to be established; convene stakeholder-specific coalitions to address the concerns of groups such as governments, businesses, civil society, parliamentarians, elderly people, young people, philanthropy, the media, and women; and facilitate convergences among debates in major digital and policy events at the UN and beyond."[90]

This is a demanding mandate that would be difficult to fulfill. The old adage that everyone wants more coordination but nobody wants to be coordinated is relevant here. Given the diversity of actors' interests and orientations in the broad digital policy space, the case for pursuing such cooperation and convergence would have to be compelling. Making that case would require a well functioning team of actors with knowledge of diverse issue-areas, significant political skills, contacts and local knowledge needed to organize diverse transnational coalitions with different agendas, and sufficient status to be able to facilitate convergence among governments and stakeholders in multiple UN settings "and beyond." The report says that the Accelerator "could consist of members selected for their multidisciplinary experience and expertise," but the status of those members and the process for their selection are not indicated. **Assessing candidates for these roles and getting support for the selections made could prove challenging.** After all, just populating the MAG has proven controversial at times, and it is (apparently) just a conference program committee.

Third, there would be a **Policy Incubator that would help nurture policies and norms for public discussion and adoption.** This ambitious structure "should have a flexible and dynamic composition involving all stakeholders concerned by a specific policy issue." While their precise status and modalities of selection are not mentioned, presumably these stakeholders would need serious expertise as well since their mandate would be even more substantive than that of the Accelerator. The group would "incubate policies and norms for public discussion and adoption," something that is often difficult in more well-established and supported international institutions. And in response to requests from actors (who presumably would meet criteria that excludes e.g. trolls and promoters of purely private agendas), the Accelerator would "look at a perceived regulatory gap, it would examine if existing norms and regulations could fill the gap and, if not, form a policy group consisting of interested stakeholders to make proposals to governments and other decision-making bodies. It would monitor policies and norms through feedback from the bodies that adopt and implement them."

It is interesting to consider how this mechanism might operate in relation to the established patterns of (dis)agreement among governments and stakeholders on Internet governance and wider digital issues. For example, consider the question of identifying and filling policy gaps. The UN Working Group on Enhanced Cooperation on Public Policy Issues Pertaining to the Internet spent years locked in divisive debates about whether there were any gaps and "orphaned issues" that required new cooperation before it closed down without an agreement. Moreover, regulation is a complex arena

that is heavily institutionalized across governments and involves specialized and expert agencies. If the requests do not come from the entities with responsibilities regarding the gap, they may not welcome an IGF-based group approaching to say, "we hear that you have a gap and are here to help."

More generally, some actors might perceived the proposed Cooperation Accelerator and the Policy Incubator as insufficiently "bottom up" approach. Accelerator members would identify points of agreement among extant coalitions, consider whether new ones are needed, convene actors and facilitate the convergence of their preferences. **Incubator stakeholders would receive requests to look at gaps and then assemble groups to develop responses**. Finding the right balance here would take some refinement, and managing such processes could draw the IGF onto terrain that requires careful treading.

Fourth, there would be an Observatory and Help Desk that would direct requests for help on digital policy to appropriate entities and engage in related activities. Sharing knowledge and information should be a tractable challenge that is well suited to an international mechanism. This author is among those who believe that it would be useful to institutionalize an informational "clearing house" function that utilizes both technological tools and human support.[91] Indeed, as Wolfgang Kleinwächter has noted, the IGF already performs a diffuse kind of clearing house function by bringing together suppliers and demanders of knowledge and information on a wide range of issues, so one could argue that this would be quite a natural fit.[92]

That said, the panel was more ambitious in imagining not just a mechanism for aligning informational supply and demand, but rather a "help desk" that ministers and others would want to call on for rather more. The report proposes an IGF unit with the capacity to "direct requests for help on digital policy (such as dealing with crisis situations, drafting legislation, or advising on policy) to appropriate entities…coordinate capacity development activities provided by other organizations; collect and share best practices; and provide an overview of digital policy issues, including monitoring trends, identifying emerging issues and providing data on digital policy." All this could require a significant bureaucratic unit, and some of these tasks could be sensitive and are already performed by other international organizations. In parallel, the panel separately recommends "the establishment of regional and global digital help desks to help governments, civil society and the private sector to understand digital issues and develop capacity to steer cooperation related to social and economic impacts of digital technologies," so the IGF unit would need to coordinate with those entities as well. There are are some operational and political issues to be worked through here.

Turning from the four new units to the broader vision, it should be noted that the IGF+ proposal does not address the questions of IGF improvements that have been much debated over the years. A great many suggestions have been made by researchers, civil society advocates, the private sector and governments, as well as the Working Group on Improvements to the Internet Governance Forum and the UN's 2016 retreat on the advancing the IGF mandate. The report does include a footnote mentioning some of this activity but does not engage with the issues, as envisioning a "plus" layer is its sole focus.

Irrespective of what happens with the "plus," continuing attention is needed to improve the rest of the IGF. Indeed, the shape and dynamics of the host body would presumably impact the "fit" and operation of the proposed add-ons. Should the IGF remain an event annual that is mostly devoted to workshops, supplemented by some bits of intersessional activity like the national and regional IGFs, dynamic coalitions, and best practice forums? Or, for example, might it be worth considering having meetings focused on one or two themes per year in a NETmundial-style configuration, e.g. globally participatory preparatory processes and efforts to agree normative outcomes that could inform decision making institutions? The WGIG report and the Tunis Agenda mandate included the option of adopting recommendations, but concerns about "WSIS-style negotiations" and the political fragility of the new process made such a model too controversial to be considered in the IGF's early years. Perhaps by now conditions have matured enough to consider such an option. Maybe some of the other long-standing challenges could be addressed seriously in tandem, such as enhancing the involvement of governments, especially from the developing countries.

Finally, it merits note that the High-Level Panel was tasked with mapping out options for digital cooperation, which is broader, more inchoate, and perhaps even more contestable than Internet governance. Several considerations follow from this. First, not all of the digital issues of concern today may need additional forms of international cooperation, much less governance. Artificial intelligence, block chain, robotics, 3-D printing and so on may raise policy concerns, but determining the most suitable responses to these requires case-by-case consideration with potential forms following functions. Second, where international cooperation is needed, pursuing it in the IGF is only sensible with respect to clear Internet governance dimensions of the issues.

Third, the fact that "digital" issues are important would not justify changing the name and focus of the IGF, as some actors seem to contemplate. On the one hand, even though the Internet Assigned Numbers Authority transition has reduced the political heat level, Internet governance remains a substantial and

complex arena with many outstanding questions that require the international community's attention. On the other hand, Internet governance should not be subsumed under a broader "digital governance" rubric alongside very different issues. If careful analysis determines that we need new mechanisms for issues that are not about Internet governance, then these should be developed. Perhaps the High-Level Panel's second and third models could figure prominently in such a process, but that is a different conversation. In the meanwhile, hopefully the Berlin IGF and related discussions will be sufficient to determine whether the IGF+ model should serve as an important part of strengthening the IGF and enhancing its utility.

Source

[88] *The Age of Digital Interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation. The United Nations, 2019. https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf*

[89] *In contrast, the panel did an online Call for Contributions well before the report's release that did not delve into the models and therefore elicited rather little comment on them. See the inputs offered at https://digitalcooperation.org/responses/*

[90] *All quotes pertaining to the IGF+ model are from page 24 of the High-Level Panel's report.*

[91] *For a discussion, see, William J. Drake and Lea Kaspar: Institutionalizing the Clearing House Function. In: William J. Drake and Monroe Price (eds.), Internet Governance: The NETmundial Roadmap. Los Angeles: USC Annenberg Press, pp. 88-104. Efforts to launch something akin to this have included e.g. the European Commission-backed Global Internet Policy Observatory, the NETmundial Initiative, and (most successfully) the Geneva Internet Platform's Digital Watch Observatory.*

[92] *See, Wolfgang Kleinwächter: Multistakeholderism and the IGF: Laboratory, Clearinghouse, Watchdog. In: William J. Drake. (ed.), Internet Governance: Creating Opportunities for All – The Fourth Internet Governance Forum, Sharm el Sheikh, Egypt, 15–18 November 2009. The United Nations, 2010, pp. 76-91.*

[93] *The Age of Digital Interdependence, p. 5.*

Multistakeholder Cybersecurity and Norm Implementation

Alexander Klimburg

In 2004, UN Secretary General Kofi Annan challenged the Internet policy community to develop the right governance structures. "In managing, promoting and protecting [the internet's] presence in our lives, we need to be no less creative than those who invented it. Clearly, there is a need for governance, but that does not necessarily mean that it has to be done in the traditional way, for something that is so very different."[94] In the 15 years since, the rise of cyberspace, and the Internet as its most visible representation, has continued to challenge governments.

Not only does cyberspace stretch across every single domain of human behavior and touch on every aspect of government – it is even unclear to what extent it can be managed by government at all. Today it is obvious that while private sector own nearly all of the Internet, and the civil society (using a wider description of the term) is responsible for much of its basic coding and maintenance, the role of government is less clear. Of course, states can seek to regulate various behaviors, manage data, prescribe information security standards, and have some influence on how parts of the underlying hardware are used. Their most important behavior is however not constructive, but destructive – states remain the most powerful attackers in cyberspace. It is therefore not surprising that when states started to show an increasing concern with the Internet, it was in the context of national security, or in foreign policy in international peace and security. Unfortunately for them, they still decided to adhere to the standard formats of disarmament discussions with only government, and sometimes even only diplomats, responsible in pushing the discussion forward. This made international cybersecurity an outlier among all cyberspace policy fields – an intergovernmental-only discussion in a field dominated by the multistakeholder approach. This is despite the increasing awareness that international cybersecurity required a multistakeholder input – the only challenge so far has been exactly how this should be enabled.

The core of the multistakeholder approach to governance has always been an inclusive approach that, however, acknowledges leadership of relevant actors where appropriate. Both the 2005 and 2015 declarations of the World Summit on the Information Society (WSIS) made it clear that the main actor groups should each take the lead "within their respective roles and responsibilities". This can be interpreted that while naturally some groups would play a more important role than others depending on the specific fora, no actor group would completely "own" any specific field. This included national security.[95]

This realization was already starting to sink in by 2011, when the G8 stated that:

"The security of networks and services on the Internet is a multi-stakeholder issue. It requires coordination between governments, regional and international organizations, the private sector, [and] civil society (...) Governments have a role to play, informed by a full range of stakeholders, in helping to develop norms of behavior and common approaches in the use of cyberspace."[96]

The reference to the discussion on norms of behavior was important. The principal focus of the international cybersecurity discussions within the United Nations 1st Committee, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of Information Security (UN GGE for short), has long been on agreeing voluntary norms of behavior for states, so-called "rules of the road" for cyberspace. The most notable developments were the 2013[97] and 2015[98] reports of the GGE, the latter of which also included a number of clear peacetime injunctions to states – for instance to not interfere with another nation's critical infrastructure, or that CERTs should be protected from attack.

Unfortunately, these laudable norms were drafted and adopted without any discussion or consultation with the non-state actors that they referred to. As it became apparent in subsequent years, the vast majority of CERTs had no idea that they had been accorded special protected status, and therefore how they could contribute to the implementation or enforcement of the norm. This one example of many illustrates the practical shortcomings of not including relevant non-state actors in the consultations of the UN GGE – no matter how well-formulated the norms, without buy-in from the crucial "other" actors there was clearly going to be a missing step. Both the 2013 and 2015 GGE reports include references on the importance of including non-state actors in their work[99], but this was never executed – including in the subsequent round[100] (the fifth, which ended in 2017 without a report) and the present iteration[101] (the sixth, which was to start in December 2019).

A competing UN 1st Committee group, the Open-Ended Working Group, started its work in September 2019 with an initial promise to have a nonstate consultation.[102] At the first meeting it became apparent however that this consultation was to be very limited, and that the same lack of willingness to engage with civil society and the private sector persisted in the governmental arms control community.

Against this backdrop it is unsurprising that a number of multistakeholder initiatives have been formed to formulate their own norms, and seek to engage directly in international cybersecurity. Siemens and Microsoft have taken the lead with two different initiatives, the Charter of Trust[103] and Digital Peace Initiative[104], respectively. The French government, under President Macron's direction, has sponsored the multistakeholder Paris Call for Trust and Security in Cyberspace[105]. And a Dutch think-tank, The Hague Centre for Strategic Studies (HCSS), took the lead to establish the Global Commission on the Stability of Cyberspace (GCSC), which presented its report in November 2019.[106]

One of the conclusions of the GCSC is that the multistakeholder approach is not only needed to formulate norms (eight of which, including the protection of the pubic core of the Internet, were formulated by the GCSC)[107], but also to help implement and monitor them. Drawing on governmental and non-governmental experiences with like-minded groups[108], it is advocating for a select group of state and non-state actors to come together in small community of interest groups dedicated to one specific norm. These groups can help better define what exactly a specific norm means, what the requirements of implementation really are, and also potentially how monitoring and even enforcement of the norms should be construed.

The key here is that the work of a particular norm that already has widespread endorsement (for instance through the GGE, or Paris Call) is taken forward by a group of actors who are particularly interested in that norm's success. The exact weighting of the group – more governmental, or private sector, or civil society orientated - would change as appropriate to the norm in question. Like its cousins in precedent in international security and Internet governance, the legitimacy of the group derives from the widespread adoption of the general principle of the norm in question, and the ability of a subgroup of its supporters in supporting its implementation. In many of the norms in question, including many of the UN GGE itself, the input of private sector and civil society will undoubtedly be key to its success.

The multistakeholder approach has clearly established itself as the backbone of all Internet-related policy making. It is increasingly obvious that many of the challenges that international cybersecurity faces – specifically in the adoption and implementation of norms of behavior – would benefit from the application of this approach. How exactly this is accomplished will however require some more of the creative thinking that Kofi Annan demanded.

Source

[94] *https://www.un.org/press/en/2004/sgsm9220.doc.htm*

[95] *For instance, the 2015 WSIS report says „We recognize the leading role for Governments in cybersecurity matters relating to national security. We further recognize the important roles and contributions of all stakeholders, in their respective roles and responsibilities." (https://undocs.org/en/A/RES/70/125, Paragraph 3.)*

[96] *http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-en.html, Paragraph 17.*

[97] *UN General Assembly: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. U.N. Doc A/68/98, https://undocs.org/A/68/98*

[98] *UN General Assembly: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. U.N. Doc A/70/174, https://undocs.org/A/70/174*

[99] *For example, see the UN GGE Report /69/96 (2013), ¶12, 7; see also the UN GGE Report A/70/174 (2015), ¶31, 13*

[100] *UN General Assembly: Resolution adopted by the General Assembly on 5 December 2016. A/RES/71/28, https://undocs.org/A/RES/71/28*

[101] *UN General Assembly: Resolution adopted by the General Assembly on 22 December 2018 A/RES/73/266, https://undocs.org/en/A/RES/73/266*

[102] *UN General Assembly: Resolution adopted by the General Assembly on 5 December 2018 A/RES/73/27, https://undocs.org/en/A/RES/73/27*

[103] *Siemens Charter of Trust on Cybersecurity: https://assets.new.siemens.com/siemens/assets/public.charter-of-trust-presentation-en.pdf , 2019*

[104] *Microsoft Digital Peace Now https://digitalpeace.microsoft.com/. Microsoft will soon also launch a nonprofit calling out cyberattacks https://www.cyberscoop.com/microsoft-cyber-peace-institute-hewlitt-foundation-brad-smith/*

[105] *Paris Call for Trust and Security in Cyberspace, 2018: https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf*

[106] *The GCSC assembled 28 senior experts from different parts of the wider cybersecurity ecosystem and different regions of the globe, and is dedicated to developing "norms and policy initiatives". It is primarily supported by three governmental and three non-governmental organizations. https://cyberstability.org/*

[107] *Global Commission on the Stability of Cyberspace: Singapore Norm Package. 2018 https://cyberstability.org/wp-content/uploads/2019/04/singaporenew-digital.pdf*

[108] *In international security, the Proliferation Security Initiative generated its own smaller like-minded group to pursue implementation and enforcement. In the Internet Engineer Task Force both the Birds of a Feather (BOF) and Special Interest Group (SIG) represent similar like-minded sub-groups that self-organize, bottom-up, to address specific topics.*

Cyber Governance and the Moral Limit of the Market

Robin Mansell

The UN Secretary-General's High-level Panel on Digital Cooperation Report, The Age of Digital Interdependence, is a welcome call for a global commitment to digital cooperation. The Foreword says that 'no one knows how technology will evolve' (p. 3). No one can know exactly how technology will evolve, but history and current practice provide indications. There is ample evidence of an overemphasis on economic growth and technology innovation which downplays the preservation of human dignity in a competitive technology innovation race. The Report misses an opportunity to emphasise this core imbalance.

Multiple efforts are underway around the world to devise rules and norms to govern cyberspace in ways that mitigate social harms. **Yet the evolution of the digital ecology continues to be associated with an information crisis.** This crisis is visible in growing confusion, cynicism, fragmentation, irresponsibility and apathy among populations whose lives are intertwined with digital technologies.[109] The private sector business model for the digital age is based on an advertising model that plays into people's fears and prejudices. There is diminishing trust in authority, while power over the collection, processing and interpretation of data is held by organisations existing largely outside lines of accountability. Without fundamental change, the future of cyberspace is likely to bring more widespread surveillance and a privacy-invasive culture inconsistent with values of fairness, solidarity, accountability and democracy.

There is a need for processes for reaching consensus about standards, ethical codes, privacy and data protection, liability for illegal and harmful content, open data, and competitive practices. But neglected in the UN Report is the need for a challenge to a private-sector-led advertising supported drive towards increasing datafication. A core challenge facing participants in global efforts to strengthen cyber governance is to reach an agreement about where the moral limit of the private provision of digital technologies and services should rest. **What is the appropriate boundary between public or community provision and private sector supply?** Put differently, cyber governance needs to be underpinned by a commitment to tackle the logic of datafication and to decide what the moral limit of the profit logic of the market is if human dignity is to be preserved.[110]

Improving governance through global coordination to achieve more transparency and improved private sector accountability will not be sufficient to redirect the evolution of cyberspace to secure values associated with human dignity. Strengthened governance processes will succeed only if

they embrace the capacity to fundamentally contest a technology innovation pathway that risks increasing loss of human dignity, with social and economic inequalities being replicated along the way. The UN Report does signal the need for a data commons. It says that if advanced AI driven algorithmic data systems are to be consistent with the values of inclusiveness and respect for human rights, they must be provided in some instances as public goods, especially if they are to contribute to sustainable development. Missing, however, is an acknowledgement that a principal factor that will guide how digital technologies evolve is decisions about the boundary been public and private goods provision of digital services and applications upon which societies are coming to depend.

The report supports 'a multi-stakeholder "systems" approach for cooperation and regulation that is adaptive, agile, inclusive and fit for purpose for the fast-changing digital age' (p.5). **The emphasis is rightly on process (as well as on human and institutional capacity building).** But this emphasis on the process of cooperation means the fundamental problem which makes coordination of multiple interested parties challenging is neglected. That problem is conflicting preferences for the provision of digital services and applications as public or private goods.

A robust global governance framework for cyber peace and digital cooperation is sorely needed. But for progress to be made toward a cyberworld consistent with global security and stability, it is essential to embed a commitment to challenging existing unequal political and economic power relationships. This requires a process that will ensure that **cyber rules and norms are predicated upon commitments to openness and the protection of human rights, bolstered by recognition that market forces on their own cannot deliver this.** A prerequisite for cooperation is therefore a commitment to limiting private-led development of digital services and applications when it is shown that these developments risk diminishing the dignity and autonomy of human beings.

Neglecting this fundamental issue means that the information crisis is likely to worsen, yielding deeper socio-economic inequalities and an incremental devaluation of human dignity. The urgent need is for a forum providing opportunities to assess the limitations of the market and to devise policy solutions and norms, rules and standards in an environment where the limit of market provision can be contested and decided over time. The IGF+ model in the UN Report, given the IGF's track record, is a forum that is well-placed to tackle this core cyber governance challenge.

Source

[109] *Tackling the Information Crisis: A Policy Framework for Media System Resilience, LSE, London, 2018.*
[110] *Drawing on I. Kant: 'Transition from popular moral philosophy to the metaphysics of morals', 1785.*

Conservative "gatekeepers" and innovative multilateralism

Ilona Stadnik

Issues of Internet regulation, digital peace and security have been underrepresented in global policy debates for too long until the international community acknowledged the seriousness of the challenges digital technologies bring to us.

But even though we can see a global division regarding the approaches to tackle new problems of digital agenda – some nations see a positive potential and build their national policies of minimum restrictions and regulations towards technological innovation, development, and cooperation across sectors and countries; other nations choose more conservative way focusing on implications for national security and considering a state as the only and primary stakeholder to be responsible for it. They become guardians, or "gatekeepers" - a term widely used in the Russian political lexicon.

Multilateralism for digital agenda was a very inert tool on the background of the rapid Internet spread across the world accompanied by cyber instability in the international security domain.

Introduction of the multistakeholder model didn't add too much confidence in it for gatekeepers. The case of IANA transition and ICANN accountability didn't assure particular states in the legitimacy of all processes. This led to the acceleration of the trend on Internet fragmentation and spurred isolationist national policies aimed not only at the content and social layers but logical too.

Anyway, the multistakeholder model proved its right to exist. And even today, when particular stakeholders, namely IT giants, have become too powerful to avoid their claims, multistakeholderism seems to be a logical form of global Internet policy. The concentration of data and services in their hands – the new oil of 21 century – made states to seek ways for collaboration to keep the security component of policy in the government jurisdiction. Moreover, the private sector started to address governments to step in to stop the snow break of problems emerging in a variety of sectors – global cyber instability, social media content policy, personal data protection, violation of privacy, etc.

The recent report of the High-level Panel (HLP) on Digital Cooperation says for effective digital cooperation multilateralism must be strengthened itself and complemented by multistakeholderism. Of course, it is natural to seek a unified structural mechanism to address global digital policy comprehensively. And one of the proposed global architectures by HLP exactly tries to fulfil this task – IGF Plus with an extended mandate. Currently, IGF High-level sessions seem to be cut off the rest of the forum. Reinforcing IGF through a

reconceptualization of stakeholder roles to ensure the interdependence of cybersecurity, digital economy, human rights, and enhance the global policy process may not be met with enthusiasm among gatekeepers.

Seems that their understanding of interdependence has a different meaning – in order to provide the best policy to address security, economy, technology and human rights concerns they favour isolationism and sovereign principles against cooperation. Gatekeeper's logic is simple: the ability to plug out from the global digital space will let them build a safe digital enclave and protect the state and citizens from destructive influence and interference. However, current unequal distribution of digital resources – ranging from critical Internet resources to the production of hardware and R&D for software – make isolationism a hard trend to follow in full scale. Lack of trust not only between nations but in the private sector too, is the main reason for isolationist policies. Gatekeepers' way of thinking cannot let them respect and take into consideration other stakeholders' views, especially on security concerns.

If we believe that we urgently need a global mechanism for digital policy, or a combination of mechanisms, based on the idea of innovative multilateralism, we need to admit that gatekeepers will hamper the process impeding multi-stakeholder decision-making since it contradicts their normal policy-making process.

More decentralized mechanisms could be a solution to overcome this problem. However, it may require revolutionizing global governance system and focus on self-regulated communities instead of traditional stakeholders – far more challenging task than finding ways to global cooperation in current circumstances.

A human-centric approach to Internet Governance

Eileen Donahoe

In reflecting on how the global "Internet Governance" discussion should develop in the next decade, one top priority occurs to me: we need to articulate how to apply universal human rights principles more fully and advocate for the use of the existing human rights framework in governance of digitized, algorithmically-driven societies. We all know we are in the midst of a global battle for dominance in technology, particularly with respect to artificial intelligence. We also must recognize that we are in the midst of a geopolitical battle with respect to the norms and values that will guide regulation of technology and governance of AI-driven societies. Our shared priority should be to solidify global commitment to the existing human rights framework as the foundation for governance of digitized societies globally.

The work articulating how to apply the existing human rights framework to digitized societies will require both continuity with and creative adaptation of the existing doctrine and framework. It will also require cross-disciplinary, cross-sector, multi-stakeholder engagement, as well as multilateral reinforcement. We had a foundational moment in June 2012, when the UN Human Rights Council passed the first UN resolution on Internet Freedom by consensus. That resolution laid down the foundational principle that human rights must be protected online as in the offline realm. Efforts were soon made to apply existing human rights doctrine to the internet, but remarkable technological advancement has changed the "online" context dramatically.

In just a few years, with digitization of society, the online/offline distinction has basically collapsed, at least in the digitized half of the world. The internet has become the infrastructure of society and machine decisions have, somewhat invisibly, infiltrated many realms of governance. We now collect so much data that many sectors of society have turned to algorithmic decision-making for the simple reason that the quantity of data collected is beyond human processing capacity. In effect, digitization of society has necessitated a move to machine decision-making so all the data being collected can be processed and capitalize upon.

In the context of all this change, applying existing human rights doctrine in the digital realm has not been a simple move. Some features of our globalized, digitized ecosystem are inherently challenging to the existing framework. Most notably, the basic trans-border mode of internet operation is challenging to an international order built on the concept of nation states defined by territorial boundaries. Second, the original human rights framework placed primary obligation on states to protect and not violate human rights of citizens

and people within their territory and jurisdiction. Yet, in digitized societies, extraterritorial reach is the default rather than the exception. In addition, we have seen a dramatic trend toward privatization of governance, where private sector global information platforms and social media companies function as quasi-sovereigns and have dramatic effect on the enjoyment of human rights of both users and the larger societies in which they operate. In this regard, the adoption of the UN Guiding Principles on Business and Human Rights (UNGPs) in 2011 was a significant normative development. The UNGPs articulated the responsibility of private sector companies to respect human rights, as well as the responsibility to develop due-diligence processes to assess the impact of their products and services on human rights. But many private sector technology companies still are unfamiliar with human rights and too few engage in serious human rights impact assessments.

We are at a critical juncture when it comes to the governance of digital societies. While we need new policies and regulation for digital technologies, we do not need to reinvent the wheel or start with a blank sheet to develop a whole new set of principles. Many well-intentioned entities who are unfamiliar with existing human rights language are working to develop new ethical frameworks for AI. But we do not need new principles for digital society – we have that foundation in existing universal human rights. The important work that needs to be done is to articulate how to apply this existing human rights framework in AI-driven societies.

Several features of the existing human rights framework make it well-suited for this purpose. First, it starts with a human-centric approach and a rich vision of human dignity, which will become increasingly important in a machine-driven world. Second, it is universally applicable, with status under International law, and has been embedded in national constitutions and applied by governments around the world. Third, it is the product of global multilateral negotiation and multi-stakeholder engagement, so it enjoys a level of legitimacy and global recognition that would be very difficult to match. These are crucial advantages.

On a pragmatic level, it is not realistic to think we can get global agreement on a comprehensive set of new principles at this geopolitical moment, especially with as rich a vision of human dignity as the existing human rights framework. The bottom line is that we let go of the existing human rights framework at our own peril. Our shared global multistakeholder project for the next decade must be to do the hard work of adapting the existing principles to digital reality. Through that exercise, we will contribute to the development of innovative new mechanism for governance while providing continuity with enduring values.

Latin American perspective on Internet Governance

Olga Cavalli

Latin America is a region with an incredible combination of beautiful nature, vast geography and great biological, ethnic and cultural diversity. At the same time this marvelous region presents important challenges related with development and its very high unequal distribution of income and infrastructure.

As per a recent McKinsey´s Global Institute report, Latin America's economies have grown by around 3 percent a year, slower than any other developing region. The report says that without a change in productivity, GDP growth in Latin America would be 40 percent weaker over the next 15 years than it was in the previous 15.

In this context, the incorporation of technology in the region will be the key to sustainable development. The region still shows a digital gap, both in Internet access and mobile broadband, there is also a lower adoption of broadband Internet in the region when compared with the OECD countries. The development of connectivity infrastructure to close the digital gap which can support processes of productive transformation must be the main goal for the countries in the region. Many efforts have been done but there is still a lot to do. The problem of digital infrastructure must be first solved, if strong regional industries like agriculture want to profit from adopting digital and automation technologies.

In order to achieve real changes, leaders must understand digital technology and the advantages and challenges it brings. This also requires management of the relations between states business and universities. There is an imperative need to develop middle and long-term strategies for regional development based on the use of digital technology. Diversification of productivity focusing on knowledge base activities with the promotion of STEM careers, especially among women, may be a way to create value in the future development of the region. All leaders, both in the private and public spheres, must be able to dialogue and interact to build these strategies.

Internet Governance plays an important role in shaping the future of this great region. A well-informed leadership is a key element to address the needs and challenges of Latin America into the international Internet Governance agenda. Capacity building plays a relevant role where lawmakers, regulators and other state decision makers need to understand the value that digital technologies

can bring to development and, at the same time, they must be aware of the difficulties and challenges that may arise. The impact on employment, environmental issues, security and the concentration of industries must also be taken into consideration.

The different Internet Governance participation spaces could play an important role in creating this dialogue among different stakeholders. For example, within the Governmental Advisor Committee of ICANN (the GAC) some events have gathered together a strong Latin American regional presence which has expressed its voice in relation with different issues that are relevant for the region, for example the treatment of geographic terms in the Internet or the role of governments in the Internet Governance ecosystem. These Internet Governance spaces must be used to reinforce knowledge about how to deal with the increasing challenges in security, privacy and stability of critical infrastructures at the national and regional level.

One of the biggest challenges of the developing world, including Latin America, is that the urgent issues prevent the government and local companies to evaluate and design long-term strategies to achieve sustainable development and growth. This becomes more challenging when technology brings a very rapidly changing environment for the economy and society. According to World Bank estimates, Latin America invests only around 0.8 percent of GDP in R&D activities, compared with an average of around 2.4 percent in OECD.

Diversification of the economy is a key goal for development, and the region has a lot to do in this area. Knowledge based companies find difficulties in finding well qualified employees. Here is an opportunity where a combined work by state, universities and companies makes sense. There are several efforts at the national level, for example in Argentina, to fill this gap, but there is still much more to be done. Quality education in digital skills is fundamental, and it becomes a great opportunity to fill the gender gap as it represents a good way for women to get well paid work with a constant demand.

Some of the recommendations made by the Report of the UN Secretary-General's High-level Panel on Digital Cooperation fit perfectly into the needs our great Latin American region: affordable access to digital networks, platform for sharing digital public goods, engaging talent and pooling data sets, establishment of regional and global digital help desks to help governments, civil society and the private sector to understand digital issues and develop capacity to steer cooperation related to social and economic impacts of digital technologies.

The Internet Governance must address all these challenges of the developing world, promoting capacity building of key decision makers, involving universities and all kind of business sectors: global companies, SMES, entrepreneurs, among other. The new Internet Governance ecosystem must focus on concrete issues and concrete outcomes that make an impact in achieving Sustainable Development Goals.

This new "age of the digital interdependence" will have an impact on the digital economy and society. The developing world must find the key elements that boost their economies to profit from the advantages of the digital economy and avoid lagging in a rapidly changing world. Let's work together in the Internet Governance ecosystem to achieve these important goals for all.

Digital Interdependence as the Lever of Cyber Peace

Peixi XU, Professor, Communication University of China

1. Four Dimensions and Their relationships

Broadly speaking, reaching a new deal for Internet governance shall take into consideration at least four interrelated dimensions of Internet policymaking. The first dimension is the negotiation about the legitimacy and rules of cyber weapons, mainly involving military and intelligence entities and focusing on the applicability of international laws to the cyberspace. The first to the sixth United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) are typical negotiation forums in this regard.

The second dimension is the global dialogue on cybercrime governance. It mainly involves public security authorities and justice systems. Key texts include the Budapest Convention on Cybercrime, which the EU strongly advocates, and the Draft UN Convention on the Fight against Information Crimes submitted by the Russian Federation. In addition, the U.S. government has reached its first bilateral data-sharing agreement with the UK under the Clarifying Lawful Overseas Use of Data (CLOUD) Act.

The third dimension involves insights in the management and control of core Internet technological resources. A typical topic here is the jurisdiction of the Internet Corporation of Assigned Names and Numbers (ICANN) and other technical communities. These communities share global values. They “reject: kings, presidents and voting”, and “believe in: rough consensus and running code”.

The fourth dimension is the solid binding rules and practices in regard to cross-border data flow and digital trade. In recent years, state actors have taken actions to strengthen the role of their jurisdictions in cyberspace and these can be seen in the various legal instruments adopted, including the Cybersecurity Law of China and the EU General Data Protection Regulation (GDPR), and the digital trade terms in the U.S.-Mexico-Canada Agreement (USMCA). WTO and Group 20 are the key venues where the global rules on digital economy and trade are being debated.

These four dimensions are inseparable and interrelated for the simple fact that there is only one Internet. The division of the four dimensions is a human effort to make it easier to understand the whole scenario. In practice, lines cannot really be drawn to divide between the four. For one instance, the WannaCry Ransomware attack involves both the first and the second dimension and which category to put it in depends on which perspective we take when examining it. For another instance, a lot of senior experts are promoting a norm intended to protect the public core of the Internet and such a norm covers both the first and the third dimension. For still another instance, China’s Cybersecurity Law and the GDPR of the EU bring challenges to cross-border data flow, an issue that belongs to the fourth dimension, but the two instruments are to some extent responses to actions of U.S. military and intelligence agencies as exposed in Snowden Leaks, which falls into the first dimension

2. A Holistic Approach and the Lever of Cyber Peace

The concrete disputes of reaching a new deal of Internet governance covers a plethora of topics and subtopics such as applying existing laws vs. working on a new treaty, governance of cybersecurity vulnerabilities, relationship between a cyberattack and a physical attack, cyber espionage activities, integrity of the Internet infrastructure, financial institutions and data, social media and political stability, and, most important of all, visions of the Internet as a domain of conflicts or as a public good.

These disputes reflect the gap between more powerful nations and less powerful ones. Powerful nations are so far unwilling to accept restrictions to their cyber military capabilities and cyber ambitions. This is the major reason for the failure to fully ban cyber weapons and prevent a cyber arms race. However, due to the technical features and the asymmetry of the Internet, powerful nations actually also believe themselves to be vulnerable. They are worried about the possibility that their drones might be hijacked, their command and control systems might be attacked, their financial data might be manipulated, and their intellectual property might be stolen.

That is why the ongoing debate on international cyber norms have produced a lot of paradoxes, complexities, and ridicules. These worries, not the empty moral high grounds, provide real leverage upon cyber military ambitions. It is important to recognize this point when we are looking for a real new deal and building a global framework. The line of argument is to build cyber peace by enhancing digital cooperation, helping all stakeholders to realize that, in order to keep technological creativity and economic progress, it is needed to reduce cyber tensions in the first dimension but improve healthy cooperation in the second, third, and fourth dimensions. In one word, the prosperity of global digital economy is the lever of cyber peace.

It is in this way that the report published recently by the UN Secretary-General’s High-level Panel on Digital Cooperation strikes at the right point.

The report crystalizes its notion in its description and call for an age of "digital interdependence", and that has captured the key logic and shall become the working logic and departure of thought for a real deal of Internet governance. The current debate on a deal of Internet governance is as prosperous as it is frustrated. On the one hand, the debate has been lively, with new mechanisms and initiatives coming out one after another. A wide range of places such as Tallinn, the Hague, Geneva, Wuzhen, Washington DC, Moscow, Tel Aviv, New Deli, Singapore, and London have all marked themselves as producing sites of cyber rules. On the other hand, the debate is gaining in depth and sophistication and it has become more difficult to reach consensuses. The UN report reunites these elements by drawing our attention back to the right departure of thought- interdependence in the digital age.

3. China and President Xi's Cyber Commons Initiative

China has gained in recent years a clearer understanding of the cyberspace and formed a set of its own ideas. Since President Xi Jinping took office in 2013, China gradually formed its understanding of global governance. On December 16, 2015, Xi proposed at the Second World Internet Conference a cyber commons initiative, which has been consistent to the sixth WIC summit. He said that cyberspace is the common space of activities for mankind. The future of cyberspace should be in the hands of all countries. Countries should step up communications, broaden consensus and deepen cooperation to jointly build a cyber commons.

This initiative can be understood in three aspects. First, in the area of digital economy, China leads the way towards improving globalization and promotes digital interdependence. On January 17, 2017, President Xi explicitly expressed support for this point in his speech at the World Economic Forum, saying that we should seize the opportunities of the new industrial revolution and the digital economy.

Second, in the area of cybersecurity, China upholds national sovereignty and puts forward the relevant proposition as part of the initiative of building a cyber commons. The Chinese view of cyber sovereignty pays more attention to political and social stability, which is to some extent, different from the hardcore national security narrative of some other nations.

Third, in the area of cultural exchanges, China advocates respect for all cultures and civilizations. This was articulated in President Xi's speech at the UNESCO Headquarters on March 27, 2014, which was before the idea of a cyber commons initiative was first proposed. In the speech, Xi presented his basic views in regard to civilization, culture, and religion. He said: "Exchanges and mutual learning among civilizations must not be built on the exclusive praise or belittling of one particular civilization...an attitude of equality and modesty is required if one wants to truly understand the various civilizations. Taking a condescending attitude toward a civilization cannot help anyone to appreciate its essence but may risk antagonizing it. Both history and reality show that pride and prejudice are two biggest obstacles to exchanges and mutual learning among civilizations."

In summary, China believes that the cyberspace is a place where the most extensive communication occurs between civilizations, cultures, and nations and it should not see a repetition of the failures the world has had in the physical world or be weaponized based on an absolute division between allies and enemies. Instead, a worldview of reconciliation should prevail in the cyberspace so that different civilizations, cultures, and nations can respect one another and coexist in peace in the cyber world. All in all, a cyber commons initiative goes beyond the traditional confrontations between powers of the world, welcomes all stakeholders with their own interests and pursuits, and serves as the overarching guideline of China when dealing with cyber issues.

On Creating Internet Governance Organizations: A Comment on the ICANN Experience

Steve Crocker

Internet governance inevitably involves the creation and operation of specific institutions. This note regards one such institution, ICANN. Most of this note is a short summary of ICANN's history and structure with a brief comment on the relation between its form and function.

I have been involved in the Arpanet[111] and Internet from the beginning, including the creation of the Request for Comments series of notes and chairing of the Network Working Group 1968-71. I was the first area director for security in the Internet Engineering Task Force (IETF) 1989-94, founding chair of ICANN's Security and Stability Committee (SSAC) 2002-2008(TK), and ICANN board member 2003-2017, including board chair 2011-2017. This note reflects only my own opinions and do not speak for anyone else or any organization.

The Creation and Structure of ICANN

One of the first open Internet governance institutions was the Internet Engineering Task Force (IETF), though some might argue it evolved out of earlier organizations. Each Internet organization has grown out of specific needs. Usually something needs to be coordinated or managed, and often this is done first in an informal, low key way. As the needs grow, a more formal organization emerges. ICANN originated in this fashion. The domain name system (DNS) grew out of a need for a more flexible addressing system. For many years, Jon Postel and a small team at the University of Southern California (USC) administered top level of the DNS along with the underlying address space and protocol parameter registries. These functions were known collectively as the IANA functions.

With the explosive expansion of the Internet during the 1990s, and the inclusion of commercial networks, Postel's small operation was overwhelmed, and it became clear a more formal and robust organization was needed. ICANN was the result, but the creation of ICANN posed a somewhat peculiar challenge. The IANA function serves the global Internet, but its funding came entirely from the U.S. Government. The new organization needed to be less tied to the U.S. government and more visibly responsive to the entire global set of Internet users. The only existing worldwide organization that represented most nations was the United Nations and its various components such as the ITU. However, the U.N. works through the national governments. In contrast, the Internet was spawned and nurtured by the U.S. and other governments that successively removed themselves from their sponsorship and oversight in favor of private sector solutions. The challenge was how to create a global organization based on participation from all sectors, i.e. based on a multi-stakeholder model, not one whose primary coordination was via national governments, i.e. a multilateral organization. What resulted is ICANN's novel organization.

ICANN was created in 1998 as a not-for-profit corporation. As with any corporation, it has a staff headed by a president and chief executive officer (CEO) and is overseen by a board of directors. In addition, it was created with an unusual governance mechanism. Seven stakeholder groups formed by volunteers from the community also play a formal role in the governance of ICANN. These are called Supporting Organizations and Advisory Committees. The Supporting Organizations are the Address Supporting Organization (ASO), Country Code Supporting Organization (ccNSO) and Generic Names Supporting Organization (GNSO). The Advisory Committees are the At-Large Advisory Committee (ALAC), Governmental Advisory Committee (GAC), the Root Server System Advisory Committee (RSSAC), and the Security and Stability Advisory Committee (SSAC). These groups appoint several members to the board, develop formal policies that are in effect binding on the corporation, and provide advice. These groups all report to the ICANN board, not to the staff, though their work is often supported by ICANN staff members.

This aspect of ICANN's structure is unlike any other organization. In an outside review of the ICANN board several years, reviewers commented that in other organizations, including the American Red Cross, which involves a very large number of volunteers, the volunteers report to the staff. In contrast, in ICANN, volunteers have specific and binding powers and report to the board.

The Quest for Legitimacy

While the overt mission of ICANN is the continued administration of the IANA function and oversight of the companies that sell use of domain names in the GTLD space, another major albeit implicit mission of ICANN was to gain the acceptance of its global role. There was no de jure mechanism for accomplishing this. Instead, ICANN had to gain acceptance by a combination of delivery against its formal mission and a very substantial public relations effort conducted worldwide with governments, businesses, civil society, and academia. The main components of this quest have been regular, open, and

free ICANN meetings across all continents; travel support for students and members of each constituency, particularly from less developed parts of the world; and forceful responses to a variety of lawsuits. ICANN's budget has also increased from almost nothing when it was first formed to about $140MM annually, thus giving it the resources to carry out both its explicit and implicit missions.

By some measures, these efforts have been successful and ICANN's continued existence seems assured for the foreseeable future. On the other hand, ICANN's emphasis on recognition and its primary focus on inclusiveness and adherence to process have had a major effect. It is virtually impossible to do anything without making sure all parties are involved. Technical problems are almost always approached via negotiations among competing parties instead of a cooperative problem-solving task. As a consequence, it sometimes takes years – or longer – instead of days or weeks to adjust operating procedures.

The Transition

From its creation until October 2016, the U.S. Government continued to provide oversight over ICANN and a degree of institutional protection through two separate mechanisms. One was a formal contract for IANA services between ICANN and the U.S. Government's National Telecommunications and Information Administration (NTIA), an agency within the Department of Commerce. The other was a series of less formal documents that outlined the role of ICANN and called for regular reviews of various ICANN functions.

When ICANN was created in late 1998, it was expected both of these mechanisms would be phased out within two years, i.e. by 2000. Many governments and stakeholders were requesting such a move from the U.S. Government in supporting an ICANN governance model that was not dependent on a single government. For multiple reasons, the original arrangement continued for many years. Finally, in March 2014, NTIA proclaimed it was time for ICANN to be on its own and no longer under the stewardship of the U.S. Government. Rather than simply phase out the two mechanisms abruptly, NTIA asked that the community express its opinions. The community took the opportunity to express a wide variety of concerns. It took two and a half years and considerable expenditures, much of it in legal fees, to complete the process.

A significant result of the deliberations by the community was the creation of yet another layer of governance around ICANN called the Empowered Community. The Supporting Organizations and Advisory Committees were given additional roles including the power to recall either individual board members or the whole board, and the power to approve or disapprove bylaw changes.

An important but subtle issue debated during the creation of this Empowered Community was whether the Empowered Community would have broad general powers comparable to the shareholders in a corporation or more limited powers. Many people involved in the debate expected the result would be the former. The counter argument, which prevailed, is that ICANN serves the entire Internet community, not just the constituencies represented by the Supporting Organizations and Advisory Committees.

How Effective is ICANN?

ICANN is structurally composed of constituencies representing vested interests. It has a technical and managerial mission, but the dominant mode of interaction is negotiation based on its structure. Adherence to policy processes is the primary determinant of what it does and how it does it. There are no well-defined metrics for measuring ICANN's actual effectiveness. Perhaps with the Transition completed three years ago, it's time for ICANN and the ICANN community to develop effectiveness and efficiency metrics in addition to adherence to multi-stakeholder processes.

And as the Internet community creates additional organizations to address various aspects of Internet governance, the community might consider such organizations can be effective and efficient in addition to inclusive.

Source

[111] The Arpanet was the first heterogenous, general-purpose computer network. It was in operation beginning in 1969. Multiple network projects both within the U.S. Government and around the world followed, and the interconnection of these networks became the Internet.

A Question of Will or Resources?

Lynn St. Amour

Much has been written about possible frameworks, and the title of this book is “Towards a Global Framework for Cyber Peace and Digital Cooperation: An Agenda for the 2020s“; and while frameworks are necessary and important, they have not been nearly enough. To help what I hope will be a real turning point in these discussions, I would like to comment on some pragmatic aspects, focusing on impact and support – participatory and financial.

The Internet Governance Forum (IGF) is an outcome of the World Summit on the Information Society (WSIS), which invited the UN Secretary-General to convene a new forum for multi-stakeholder policy dialogue. The IGF was created specifically as a platform to help address cross-cutting international public policy issues pertaining to the Internet, bringing different viewpoints and different expertise to bear – not only to discuss but to offer guidance, frame issues, identify key partners, and, yes, make recommendations. At the time, UN SG Kofi Annan made a bold move establishing the **IGF as a multistakeholder Forum where all participants participate on an equal footing,** and where an empowered globally diverse multi-stakeholder community had significant say over the agenda.

This was very important at the time to ensure an appropriate breadth of issues, diversity in participation, and that as many voices as possible would be heard. The report from the UN Secretary General’s High Level Panel on Digital Cooperation “A Declaration for Digital Interdependence“ showcases some interesting opportunities. In particular, the IGF Plus model suggests a future IGF should comprise an (updated) Advisory Group, a Cooperation Accelerator, a Policy Incubator and an Observatory and Help Desk. I believe most of these are useful ideas AND strongly believe they can be supported or evolved from existing activities within the IGF ecosystem. Importantly, the IGF already has the necessary values and principles. IGF has many of the structures needed and has the right DNA to question progress and evolve as necessary. The report also says that this model “aims to address the IMF‘s current shortcomings.

For example, **the lack of actionable outcomes can be addressed by working on policies and norms of direct interest to stakeholder communities.** The limited participation of government and business representatives, especially from small and developing countries, can be addressed by introducing discussion tracks in which governments, the private sector and civil society address their specific concerns. What the IGF has not had is the level of support – participatory or financial - needed to implement its mandate. This needs to be addressed for any model to succeed. Nearly every individual in the world, most organizations or businesses, and every government in the world has benefited from the Internet – directly or indirectly. Society has benefited (which is not to say that only good has come from digital developments as society has always had exploitative elements); yet broad and real support for engaging deeply around international public policy issues has been seriously lacking. Unless we understand the reasons for such an unambiguous lack of support, future frameworks will also falter.

As the IGF is an extra-budgetary programme of the UN, its secretariat and programme support comes only from voluntary contributions. In 14 years of the IGF, less than 25 countries have contributed financially (most only once or twice) and less than 30 organizations or businesses have contributed to the IGF Trust Fund. We should talk about improvements or new frameworks, but I fear they will come with the same lack of support, which in itself could fuel a return to less inclusive, less open processes, or will re-trench behind closed or more traditional multi-lateral processes. To be clear, multi-stakeholder processes are not easy, precisely because they encourage different viewpoints, and work to incorporate varying frames of reference; and when the issues are so intertwined this is even more complex, but this is something we all need to lean into rather than lean away from. So, what is needed going forward? I believe it is quite straight-forward as so many of the basic building blocks are already in place.

Needs across the IGF ecosystem include:

- Participation and strong vocal and/or financial support from:
    - the UN: all relevant agencies/committees/councils
    - the private sector
    - policy makers – governmental and non-governmental
    - international civil society organizations

Without additional funds and increased participation from key sectors, no framework will be truly successful. With increased participation and increased funding, for example:

- additional outreach and engagement opportunities would be possible for small and developing countries, and for marginalized communities,
- outputs from current IGF ecosystem activities would be more robust and distribution efforts improved,
- IGF ecosystem activities themselves would be strengthened,
- the IGF secretariat could be staffed to its full requirement

New efforts are needed to pull in policy makers, private sector participants, additional and multi-disciplinary partners. A global forum for deliberation is necessary given the interconnectedness, and combining this with purpose-built community/stakeholder meetings as well as full multi-stakeholder sessions could be helpful. With respect to impact, IGF intersessional activities have grown over the years and include major policy programmes such as the "Policy Options for Connecting and Enabling the Next Billions" which ran from 2014 – 2018, or the Best Practice Forums (4) which have been running for the last 6 years, focused on Cybersecurity, IoT, Big Data and AI, Gender and Access, etc.

These joined Dynamic Coalitions (18) which emerged at the IGF's inaugural meeting in 2006, and are open, multi-stakeholder groups dedicated to an Internet governance issue. There are now over 115 National, Sub-Regional, Regional and Youth IGF initiatives (NRIs), and these are Internet Governance Forums organized on a national, regional or sub-regional level based on specific local needs. The NRIs enrich and benefit the IGF at the global level and conversely the global IGF enriches and benefits the NRIs at local levels. All these activities in concert with the global IGF help concretely advance issues at global and local levels.

I strongly believe that the IGF has much of what it needs to make an even more beneficial contribution to digital cooperation and to society at large. What is lacking is real, broad support – financial and participatory. If we are all concerned with advancing a people-centered, inclusive, development-oriented and non-discriminatory Information Society, this should be easy for all of us to fix.

The High Level Panel on Digital Cooperation - Yet another UN panel and report?

Jörg Schweiger

The High-Level Panel links digital cooperation with the Sustainable Development Goals (SDGs) and then answers the question what digital cooperation must be like in order to meet the SDGs. It makes sure to meticulously list all governance fields and all stakeholders. Interesting is that the ideological dispute between multi-stakeholderism and multilateralism is resolved by proposing an informed coexistence of the two. Like numerous other respectively specific UN working groups and reports, challenges to be faced are reviewed across all areas of societal and economic life, with a particular focus on the UN's typical point of view of human rights and equality.

So, nothing but "old ideas in new boxes"?

Not quite! The report lists exemplary global projects to explain its requirements and ideas of digital cooperation as it should be.

It further addresses "contemporary" challenges, such as AI or social media, and offers equally contemporary solutions, such as agile methods and processes, but also unconventional approaches. The latter, in particular, for one of the issues that has been identified to be among the most urgent today: permissionless innovation will create de facto standards set by dominating market players, with regulations or the consideration of human rights aspects often lagging far behind. Instead of cumbersome (global) regulations, the report advocates "soft governance", i.e. values, principles, standards and certification processes that can be tested in regional pilot zones.

A value-based approach was already proposed by the NETmundial Initiative and backed broadly, particularly by governments. But it was not followed up on. A promising approach needs to build on those values as the basis of all action and has to achieve a buy-in not only by civil society and governments but also by the private sector. This will avoid the emergence of ever new working groups, accords and calls that suffer from a lack of broad, global acceptance and therefore remain playing fields of specific interest groups or present redundant approaches.

How will urgent problems be identified and how are appropriate solutions created?

The Panel presents three potential solutions. The most tangible one is the IGF Plus, which is based on the comprehensive understanding of the shortcomings of today's IGF.

Building on the authority of UN Secretary-General António Guterres, who convened the Panel, and on the broad global experience of the high-calibre experts, the High-Level Panel on Digital Cooperation has the capacity to give an impetus and stimulate first active steps towards tackling the known problems and challenges. A mandatory requirement, however, is that the proposals it makes are accepted, pursued and implemented – a task that could be assumed by a potential Envoy, who unites the whole range of stakeholders in a single value-based initiative and is accountable to all of them, not only to the UN.

DENIC is the manager of one of the largest Top-Level Domains (TLD) worldwide: Germany's country code TLD ".de". Constituted as a not-for-profit cooperative DENIC is part of the Internet's infrastructural core responsible for the German namespace on the Internet.

Hence, as a technical operator, DENIC calls for a single rooted, resilient Internet based on transparent, unambiguous technical standards and policies. Socio-politically we strive towards an open, free and secure Internet. Both to be achieved by a value-based "soft governance" approach.

New Deal, New Peal

Leonid Todorov

For a non-Westerner, it is amusing to note it's easily discernible spirit of Enlightenment and rationalism, which optimistically suggests a linear, progressive, and ascensional advancement of the Internet and the major stakeholders' exposure to, and eagerness to apply, good Internet Governance practices. The reality, however, appears radically opposite: the rise of the new social conservatism and nationalism across the Atlantic and much of the world, and the return of the Big State, coupled with irrationality in policy making, rather suggests fundamental policy setbacks, which are yet to mount to the further prejudice of the Internet's nature and, subsequently, Internet Governance.

New Deal, New Wheal?

I would also defy the notion of global common interest which the paper interprets as the upholding of the Internet's integrity. Notwithstanding ritual statements, in reality some leading Internet nations seek quite the opposite. In a similar vein "shared responsibility to provide open and resilient Internet services to all and to protect the rule of law and human rights" has become infamous for its quite opportunistic interpretations in pursuit of fiercely contesting geopolitical interests. Looking ahead, such a rivalry is unlikely to cease any time soon, thereby affecting the Internet's fundamentals. Plus, there is no body or institution capable of effectively reconciling nation-states' parochial interests and cure their irrational fears, and it would hardly emerge any time soon.

A significant part of the blame should also be laid on the global community behind the IG/IGF movement for the failure to propone a global consensus on the common interest over past decades. Too busy assembling in lovely places to celebrate a purported global universal IG agenda and kowtowing to government and business celebrities it has ignored a hardly gratifying job of turning the agenda into a main-street narrative.

The Internet business was lulled by the original laissez-faire environment and, ultimately, was caught unaware by a drastic change in the institutional environment. Understandably, it has opted for petty opportunism as the only credible survival strategy.

The technical community seems to have been living in a bubble of its own and being ignorant of the-then looming socio-political challenges. The payday

is yet to come as Governments have become far more technically versed, coopted renegade techies and are now far more capable of shaping tech policies to serve what they conceive of as a national, rather than common interest.

Last but not least, the biggest nation on the Internet offers what seems to some a simple yet effective alternative to the multistakeholder-based governance. Few nations would bother to test it for universality, yet many are tempted to replicate it, apparently adding to detrimental effects on the Internet's integrity.

New Deal, New Heal

The authors' attempt to table a new, hybrid model to revitalize the dialogue on the IG agenda seems too late and quite naïve. As some of them would admit, by its existence the Internet has challenged traditional societal fundamentals, and sensing the time has come for them to strike back, Governments will stick to the "winner-takes-it-all" approach, meaning an assault on and/or crawling revision of the multistakeholder-based IG principles. With their polarized approaches, little doubt that the Internet is going to split, at least, in terms of both parameters and policies, in 2 or even more loosely interconnected bubbles (e.g. the Golden Billion plus a handful of other nations vs. the rest of the world).

The good news, however, is that whilst the multistakeholder-based governance is now facing a conceptual and existential crisis, there have already emerged signs that the opposing stance is prone to a similar crisis, too. Plus, the hope remains today's institutions and socio-economic and societal fundamentals would evolve over time into more mature and relevant ones (albeit not granted and not necessarily in a linear and progressive way).

At the end of the day, once the stakeholders realize, each in its own way, the gravity of the loss, perhaps the time would come to hammer the very new deal suggested by the authors or a different but effective one, as the Internet still keeps a lot of surprises.

Intersection of Privacy with Security and Stability: Balancing Competing Interests

Ram Mohan, Philipp Grabensee

The Challenge

There is broad agreement in the internet governance debate that the protection of privacy as well as the security and stability of cyberspace are both essential parts of any global, future-proof internet governance regime. As stewards responsible for the security and stability of over 200 gTLDs, we observe that these recognized objectives of privacy as well as security and stability may not always go hand in hand.

The WHOIS[112] protocol is the most widely known and deployed Registration Data Directory Service (RDDS). It is being replaced by the Registration Data Access Protocol (RDAP)[113]. In both cases, the simplest operation is the presentation of a domain name to the appropriate server, which will respond with all the contact information associated with the domain name. This contact information would typically include the name, postal address, email address, and telephone number of the owner of the domain name (the registrant) and, if present, similar details for administrative and technical contacts for the domain name.

Domain ownership information has been used by security practitioners and by law enforcement as part of a larger set of information sources to investigate alleged or actual malfeasance that involve domain names, e.g., malware, phishing, pharming, and botnets.

Major developments in data privacy and data protection regulations have contributed to a new reality as far as registration data display and storage is concerned. Perhaps the most significant change was the global adoption of the General Data Protection Regulation (GDPR) in 2018. The application of GDPR and other privacy policies has meant that previously available contact information is now PII, and as a result may no longer be made available to the public. Registries and registrars who hold this information in registration data have dramatically curtailed the information displayed publicly, often dropping an iron curtain over all registration data.

To address the requirements of GDPR with respect to gTLD practices, the ICANN Board of Directors adopted by resolution the Temporary Specification for gTLD Registration Data[114] in May 2018. The Temporary Specification provided a single, unified interim model to ensure a common framework for gTLD operators to handle registration data, including RDDS. The

Temporary Specification also directed the creation of a gTLD RDAP profile as a prerequisite to launching the RDAP service across the gTLD space. To move beyond the interim solution, a Draft Framework for a Possible Unified Access Model[115] was created. This could serve as a possible starting point for conversations with European data protection authorities, including the European Data Protection Board.

The availability of contact information has often been important for the investigation of abusive activities. In addition to the basic task of identifying the owner of a specific domain name, it has been routinely used to identify portfolios of domain names belonging to alleged and known malefactors. With this information, when a single domain name was found to be abusive, additional potentially abusive domain names could be quickly identified and mitigation applied immediately, sometimes before the additional domains could be deployed in an abusive way. The loss of ready access to registration data may have a negative effect on the ability to detect and fight cybercrime.

The Technical Study Group on Access to Non-Public Registration Data[116] (TSG) has proposed a credential management infrastructure that allows authenticated requests for contact information. TSG01, Technical Model for Access to Non-Public Registration Data[117], provides the technical underpinnings on how to lift the curtain on providing third parties with a legitimate purpose with access to non-public registration data. The implementation of such a model might be a step in the right direction in balancing the competing and legitimate interests of privacy and security.

Additional steps being taken by the technical community may improve both privacy and security. Several recent protocols focus on increasing the privacy of Internet users by minimizing or encrypting DNS queries and responses. For example, QNAME Minimization[118] aims to increase the privacy of users by minimizing DNS queries to only contain the information needed to answer the immediate next question. In addition, DNS-over-TLS[119] (DoT) and DNS-over-HTTPS[120] (DoH) encrypt DNS queries and responses on the wire.

Balancing Privacy with Security and Stability

The DNS and the Internet depend upon a “shared faith” model. In this model, each of the parts of the Internet have an unwritten agreement to conform to open standards and interoperability in return for accessibility and reach. The discussion about the governance of the Internet and the creation of norms needs to balance the demands of privacy and human rights with the practical realities of security and stability. The usability and trustworthiness of the DNS depends upon a sustained shared faith system; if the trustworthiness declines as a result of an impaired ability to counter cybercrime or to resolve names predictably, the long-term viability of the Internet comes into question.

We believe that the IGF Berlin 2019 can provide an effective forum to deliberate over the apparently competing interests of privacy and security and stability. Both components form critical pillars in the ongoing debate over effective internet governance. The future of a trustworthy and interoperable Internet requires the reconciliation of the recognized right for the protection of user privacy with the legitimate needs of authenticated requestors of registration data to mitigate cybercrime.

Source

[112] Daigle, L.:WHOIS Protocol Specification. RFC 3912, DOI 10.17487/RFC3912, September 2004, https://www.rfc-editor.org/info/rfc3912
[113] Newton, A., Ellacott, B., and N. Kong:HTTP Usage in the Registration Data Access Protocol (RDAP). RFC 7480, DOI 10.17487/RFC7480, March 2015 https://www.rfc-editor.org/info/rfc7480
[114] https://www.icann.org/resources/pages/gtld-registration-data-specs-en
[115] https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-18jun18-en.pdf
[116] Marby, G.: Technical Study Group: November 2018 https://www.icann.org/tsg
[117] Mohan, R., et al.. TSG01: Technical Model for Access to Non-Public Registration Data: TSG01, April 2019, https://www.icann.org/en/system/files/files/technical-model-access-non-public-registration-data-30apr19-en.pdf
[118] Bortzmeyer, S.. DNS Query Name Minimisation to Improve Privacy. RFC 7816, March 2016, https://tools.ietf.org/html/rfc7816
[119] Hu, Z., et al.. Specification for DNS over Transport Layer Security (TLS). RFC 7858, May 2016, https://tools.ietf.org/html/rfc7858
[120] Hoffman, P., et al.. DNS Queries over HTTPS (DoH). RFC 8484, October 2018, https://tools.ietf.org/html/rfc8484

Internet Governance from a technical perspective

Hans-Peter Dittler

The Internet is the major medium for communication in our days. Without the Internet most modern life and business would not work. The Internet was developed by people who think along technical lines and believe in standards and conventions that are developed in several groups with different grades of openness and public documentation. The Internet is run and maintained by companies with technically minded people using a lot of conventions and mutual agreements without any real central power or institution which could enforce rules.

That is true for the basic Internet but on top of the basic network of networks a whole range of services and products is existing – search engines, social media platforms, video streaming any many more. They are run by companies which are mostly driven by commercial and financial interests. These interests are often quite different from the rules used in the Internet based on mutual agreement and conventions agreed upon in open discussions with final – often raw – consensus between all interested parties.

To make things even more complicated, a whole industry of unlawful groups are using the Internet and the layers on top of it to run their special businesses ranging from blackmailing, offering of weapons, drugs and other forbidden goods and services up to stealing and selling of private data.

We also see governments interfere with the Internet often under the premises of protecting their people. But any attempt to protect people by blocking the Internet or spying on people will in the end fall back on the people who should be protected. There is no technique – and there never will be one – which only breaks the encryption of bad people. Everything which is developed for good intention can also be misused with bad intention by other people.

Taking all of this into account the question is: can the Internet be made a better Internet by good or at least better governance of the Internet?

In the technical Internet world approaches which invite and include all interested parties like the IETF (Internet Engineering Task Force) seem to give better results than local or closed efforts for creating technical standards. If we try to use those principles also in the area of governance of the Internet we would build and create principles and rules for governance and control of the Internet acting along the same lines. Starting with an open and inclusive discussion of the problems and areas of work a set of principles could be identified and refined over time using open discussions. During this development process all interested parties should be invited and be involved. There should be no special role for neither governments nor civil society, all should be part of the development and discussion cycles. It might be very hard to fit the diverging interests of privacy and anonymity versus trust and interest to identify bad users of the system. There will be a need for compromises and only a rough consensus might be reachable without fulfilling everybody's wishes in full extent.

If there is consensus about the governance rules between all involved parties as a next step at least the vast majority of all players must signal acceptance of the basic set and adhere to them. When reaching this goal a large part of the problem is solved. In addition to the non-binding acceptance some of the rules and best practices could be used to define local laws, international law and treaties. Only rules which are widely accepted should be enforced globally. Development of rules for the Internet as a global medium must be done globally even if laws might only be defined and enforced locally.

One step on this path was the discussion of governance principles and problems at the IGF (Internet Governance Forum). After several years of open, fruitful and multi-sided discussions the next step of development should be taken. A more result-oriented platform delivering at least some basic deliverables should be initiated. This might be an evolution of the IGF or a new follow-on kind of platform. The great achievements of the IGF by including all parties and the openness of discussions with all on equal setting must be kept as crucial for success and acceptance. An even more inviting and more encompassing structure might help that parties which were not yet used so much to this kind of development would also find their place in the discussion and the acceptance of the results. This work should be based on recommendations like the report from the UN Secretary-General's High-level Panel on Digital Cooperation from June 2019, the UN 2030 Agenda for Sustainable Development and respect the principle from the framework of the Human Rights Council.

The condition for success is the openness and inclusiveness of the overall process. Only if all parties ranging from end users and civil societies to big companies, from governments to non-governmental-organizations are involved in the development process results which change the global acceptance and global commitment can be expected.

PART 2: ISSUES

CYBERSECURITY

Taking Responsibility for a Trusted Cyberspace

Wolfgang Ischinger

Our ever-growing digital connectivity has in many ways contributed to the empowerment of the individual, just as optimists imagined it 20 years ago when the Internet was still in its infancy. From the perspective of foreign and security policy, the empowerment of individuals through cyberspace tends to undermine state's monopoly on the use of force. And it is doing so in a way that we don't yet fully comprehend. That is why we must abandon the idea that the state can ever universally guarantee safety in cyberspace. Our digital lines of defense are increasingly drawn at the level of each individual company or each individual user.

As a consequence, the large private companies whose services and hardware make up the infrastructure of cyberspace are acquiring not just economic but also geopolitical relevance. It is no coincidence that the heads of technology companies like Facebook, Twitter and others now regularly meet one-on-one and at eye level with world leaders. And with power comes (or should come) responsibility – including the responsibility to contribute to adequate standards for cybersecurity, not only at the national but also at the international level.

Some of the private sector partners of the Munich Security Conference (MSC) are among the companies who have stepped up: At the Munich Security Conference 2017, Microsoft presented its ambitious proposal for a "Digital Geneva Convention". Just as the existing Geneva Convention of 1949 commits states to protect civilians from harm in the event of war, a Digital Geneva Convention would oblige them to protect individuals from the dangers of cyber warfare. It would ban states from launching cyberattacks on private sector targets, critical infrastructure, or intellectual property. And it envisions the tech sector as a neutral "Digital Switzerland" that never assists in offensive cyber activities and wins users' trust by protecting them impartially no matter where they are.

One year later, at the Munich Security Conference 2018, we convened a number of industry giants who, led by Siemens, signed the "Charter of Trust" (CoT). Since then, over a dozen major companies have joined this initiative. The CoT commits members to transparency about cybersecurity incidents and promotes the inclusion of cybersecurity rules in free trade agreements. The CoT demonstrates what meaningful common standard setting can look like. In the case of products, for example, it means standardizing access authorization, data encryption, and continuous security updates. By next year, the number of connected devices in use worldwide is supposed to reach 20 billion. Imagine if none of those connected products had come onto the market without meeting certain standard cybersecurity requirements. Standard setting also has the important confidence-building effect of empowering citizens and users to better protect themselves by knowing what standards the products they use had to meet or did not meet.

Now, it is incumbent upon states to step up. If governments continue to leave it to the private sector to self-regulate, citizens might lose trust in politics to manage the pressing issues of technology. That is precisely why multistakeholderism is the right approach to cyber governance. It is encouraging to see, for instance, Emmanuel Macron personally championing an initiative that brings together governments, businesses and civil society: the Paris Call for Trust and Security in Cyberspace, which draws on principles of the Digital Geneva Convention and the Charter of Trust.

When we established the MSC Cyber Security Summit in 2012 as our first regular thematic format outside the main conference in Munich, there were two messages I wanted to put on the agenda: First, that cyber security needs to be "Chefsache", as we say in Germany – it has to be dealt with by decision makers at the very highest levels. That means by CEOs and by heads of government. And second, we need to provide adequate "translation" between those top-level decision makers and the cyber security experts in companies and think tanks who deal with the technology every day. The Charter of Trust and the Paris Call show that there is progress on both counts.

It is important that these trust-building initiatives succeed. Trust is the cornerstone for cyber diplomacy, as it is for diplomacy in general. Without mutual trust, binding norms cannot develop, much less succeed. And we still have a long way to go towards states, companies and individual users having full confidence in the cyber sphere and in each other.

Bridging Stakeholder Gaps in the Governance of Cyberspace

Chris Painter

In the nearly thirty years that I have been involved in cyber and Internet issues, much has changed for both better and worse. The technical and policy threats to cyberspace have grown in number and sophistication and have had far greater impact because we are all increasingly dependent on computer networks for our everyday lives. A wide range of state and nonstate actors are penetrating and attacking computer systems leading to greater instability and some states wish to fundamentally change the way the Internet is run risking fragmentation of a technology that aspires to be unified and global. On the positive side, we are paying more attention to combating threats in cyberspace and seizing the many opportunities it offers. Not so many years ago, if you raised a cyber issue with a Cabinet Secretary, Minister or other very senior government official, they would treat it as a niche technical issue and relegate it to a lower level. This lack of understanding and priority was also the norm in the C-Suite of many businesses. Today, largely because of the threats we are seeing, that has slowly but surely changed. Though much more needs to be done to mainstream cyber and Internet policy, increasingly governments are seeing it as not just a technical issue but a core issue of national security, economic prosperity, human rights and, ultimately foreign policy. The private sector at the C-Suite level is also beginning to treat the issue as more than a technical cost issue but one on which the future of their businesses may depend.

While slow but steady progress in prioritizing cyber issues is foundational, one enduring challenge is bringing the right stakeholders into important conversations and decisions regarding cyberspace and bridging the gaps between various stakeholder communities. Even traditional stakeholder groups are not monolithic. Within government, for example, there are vast differences in perspective and expertise between the security, economic and human rights communities. While I was at the White House and we were beginning to write the first International Strategy for Cyberspace, I convened many different agencies in a room for an entire day and the result can best be described as "creative cacophony." Even the language each community used was different – the security community used "cyber policy" and the economic community used "Internet policy." Of course, there is vast differentiation in other traditional groups such as "the private sector", "civil society", "the academic community" or the "technical community" as well, so the challenge is not only to promote meaningful interaction both between and within these groups.

When my then office was created at the US State Department in 2011 – the Office of the Coordinator for Cyber Issues – it was the first high-level diplomatic office in the world devoted to the full scope of cyber and Internet issues. Now there are over thirty cyber offices in foreign ministries around the world – a testament to the priority of these issues as a matter of foreign policy. In establishing the office at State, we recognized that cyber and Internet issues could not be adequately addressed in stovepipes, that many cyber issues were cross cutting and it was important to make sure that our policies reflected all of our national priorities across security, economic and human rights dimensions. That meant working with seemingly diverse stakeholders across our own and other governments and with many and diverse nongovernmental stakeholders in recognition that no one group has all the answers and that our policies are stronger and more complete when they are informed by a number of different perspectives.

For example, the US Government consulted private sector and civil society groups in formulating its International Strategy for Cyberspace and conducted many bilats with other countries that included a private sector and civil society component. In addition, many countries are working with nongovernmental stakeholders in writing their national cyber strategies and incident response plans.

The idea of a "multi-stakeholder" approach is a flexible one, with different stakeholders having different roles depending on the issue at hand. In some areas, like the governance of the technical aspects of the Internet, governments are only one stakeholder among many. In others, like law enforcement and international peace and security, governments have a more dominant role. But even with respect to these later issues, there is an important role for nongovernmental stakeholders and governments do not have an absolute monopoly. I once had representatives of another government who was, at the time, skeptical of the multi-stakeholder approach, ask if it meant that they had to consult all the other stakeholders before defending themselves from an ongoing severe cyberattack. Clearly not – but building a response plan and policies with other stakeholders in advance could make any defense or response stronger. Similarly, only states can prosecute and arrest the perpetrators of cybercrime – but the private sector and others can help trace the perpetrators and provide critical evidence of the wrongdoing.

In the area of international stability, only states can agree to restrain certain destructive state actions, decide whether to obey particular agreed upon norms of state behavior or employ a range of state tools such as diplomacy, economic sanctions or force to respond to a norm violation. But here too other stakeholders have an important role. Among other things, they can help

inform the discussion of what the rules of the road should be or how best to implement them given their technical or other experience. For example, the Forum of Incident Response and Security Teams ("FIRST") – a group composed of Computer Incident Response Teams – can play a vital role in raising awareness of the UNGGE agreed norm protecting CSIRTS from state cyberattack. The Global Commission on the Stability of Cyberspace, comprised of former government representatives and members of the private sector, academia and civil society with expertise on issues ranging from hard security to human rights, has been working to help inform and supplement that government debate on these issues as have a number of other initiatives including the Paris Call and a number of industry led efforts. Other stakeholders can also agree on norms involving their own conduct and help call out violations of agreed norms by both states and nonstate actors leading to greater accountability. In addition, other stakeholders, working with governments, play a critical role in capacity building – including capacity building aimed at more widespread adoption of international law and norms. For example, the Global Forum for Cyber Expertise -- a collection of governments, private sector, academic and other organizations – has made capacity building on international security issues a priority.

Although, ultimately, governments will negotiate the conclusions of these processes, the newly formed UN Open Ended Working Group and Group of Governmental Experts on cyber stability both offer a unique opportunity for engagement with nongovernmental stakeholders. Although the focus should be firmly on international cyber stability issues, such engagement would benefit from a wide range of private sector and civil society members and any final report will be better informed by such engagement. Of course, the conversation on these issues should happen in other global and regional venues as well to both help inform the UN processes and make sustained progress more generally.

The IGF offers one important, though non-exclusive, forum for discussions around growing peace and security issues. There has been discussion on international security issues before in the IGF and it offers a forum comprised of many stakeholders who do not regularly deal with peace and stability issues. Its strength is that it can expose these stakeholders, many from the technical and Internet Governance communities, to the debates that are being held by those in governments and others who are steeped in hard security issues, helping raise awareness and helping both groups appreciate the potential effects those negotiations will have on the larger cyber ecosystem. The IGF's weakness, however, is that members of the international peace and security community often don't attend the IGF, particularly at a high level.

For example, though many ICT Ministers and senior officials attend at least part of the meeting, they are seldom attended by foreign, defense or interior ministers who are focused on security and stability issues. For the IGF to be a more effective venue for these kinds of discussions, more attendance from the traditional security community should be sought and prioritized.

India, cyber-peace and digital cooperation

Latha Reddy

When I look back over the previous decade, how do I see progress having been made on Cyber Peace and Digital Cooperation? I see greater awareness on the threats emanating from cyberspace, if it is left totally unregulated. It is clear that positions have shifted – countries that earlier argued against the need for universal norms and rules of the road, and for the need for a free and innovative ecosystem in cyberspace, today have come to the belated realization that the use of this medium by terrorist groups, motivated disinformation campaigners, and cyber criminals has made some form of state and non-state cooperation inevitable if cyberspace is to continue to be the preferred means of communication.

I also believe that there is a more widespread understanding that viable norms can only be developed by a multistakeholder model within a multilateral process. By this I mean that there has to be first a process of each government going through consultations within all stakeholders which includes not just government departments, but industry, academia, civil society, technical and technology experts, legal advisers, and general users. Then all governments need to consult with each other to coordinate their national positions into a common international position. This could lead to a "lowest common denominator" result, but I do believe certain dangers are becoming so alarmingly common and widespread that there will be a universal recognition that some globally acceptable norms and regulations are indeed required.

I have often spoken on the fact that today the countries with the largest number of users of the internet are China, India and the USA – in that order. Therefore in the 2020s there will have to be some modification of the traditional postures of the USA, Europe and their allies on the question of internet Governance and its leadership. The different sectors which have been identified as the four main baskets of the global internet Governance Ecosystem (cybersecurity, digital economy, human rights and technology may not be prioritized in the same order by all countries. Developing countries – such as China, India and others – have emphasized other issues too, such as inclusion, development, access and affordability, which may not figure as high in the calculations of developed and affluent nations.

It is for this reason that I would argue for all dialogues to continue - whether at the United Nations, within regional groups and alliances, within individual countries. But there also has to be better cooperation between these dialogues, processes, and at some stage a combining of their recommendations and norms for universal acceptance. Holding comforting consultations among the like-minded is easy, having the difficult conversations with those perceived as adversaries is the harder process. But if we wish to avoid fragmentation and splintering the internet and cyberspace, there is no alternative.

And finally, we have to preserve and cherish this amazing medium that has connected us in ways we never dreamt of. Unless we agree on the means to use this technology, and future (and possibly more disruptive) technologies in a responsible manner, we, the Cyber Peace Warriors, would have failed. So, let us soldier on, overcome our geopolitical rivalries, create universal standards and norms and usher in the Cyber Peace and the Digital Cooperation that we need.

The next decade of Digital Governance: Practice will make it perfect

Amandeep Gill

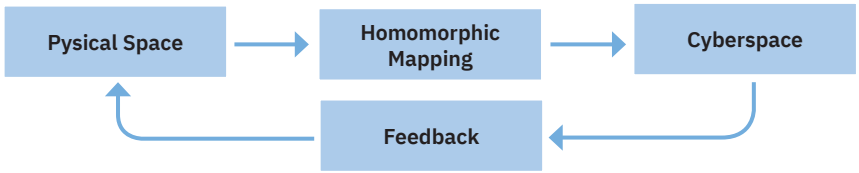
In 2020, the international community will mark 75 years of the founding of the United Nations. It is a somber moment because multilateral cooperation is still embarrassingly difficult despite seven plus decades of experience, and because key organs of global governance continue to reflect a world of old privileges. Can we make a new start with governance of digital technologies, particularly their latest manifestation which promises to extend human intelligence in new directions?

The Report of the UN Secretary-General's independent High-level Panel on Digital Cooperation, the most diverse ever in UN history and the first to be chaired by non-government representatives, makes a case for a three-step approach. First, a recognition of shared human values such as inclusiveness, respect, human-centredness, human flourishing, transparency, collaboration, accessibility, sustainability and harmony to shape the development and deployment of technologies. Second, a Global Commitment for Digital Cooperation to "enshrine shared values, principles, understandings and objectives for an improved global digital cooperation architecture". Third, the elaboration of a new digital governance architecture for which three models are offered as inspiration: Internet Governance Forum Plus, Distributed Co-Governance Architecture, and a Digital Commons Architecture.

The task, which given the nature of these technologies has to embrace a wider circle of actors than the traditional UN inter-governmental machinery, is formidable and brooks no delay. There are also risks on the way. First, there is a risk that these steps are seen excessively in terms of a grand design for peace and cooperation, which internationally minded idealists have passionately advocated since Jean-Jacques Rousseau, instead of a distributed 'architecture' for digital governance which allows for context-specific flexibility and innovation.

Indeed, one could argue that the three-step approach prescribed by the Panel for global digital governance could even be applied at the level of the firm – the founders or the employees discover through a process of dialogue a set of common values in their social and political context, commit to cooperate within and across the firm's boundaries with relevant stakeholders, and then put in place mechanisms and capacities to implement the good governance of digital technologies. Similarly, at the level of a State, the

Figure 1: Interaction between Cyberspace and Physical Space



Source: Compiled by the Dr. Zhou Hongren.

government, the private sector and civil society – the sarkar, bazaar and samaaj of India's digital cooperation enthusiasts - should get together to put in place digital governance principles and mechanisms keeping in view the top international tier of guiding values, principles and possible norms.

Another risk on the digital governance path is exclusion: of dynamic youthful geographies in Africa, Asia and Latin America, of startups and SMEs, of women, of the non-initiated - those who are not technologists or those who do not speak the special vocabulary of digital governance. Losing diverse perspectives and inclusiveness is not only immoral but it also enhances risk and diminishes the long-term economic opportunity coming from digitalisation and the AI/data revolution.

Then, **we could get digital governance wrong by being divorced from practice, governing without doing, regulating for abstraction.** In Brazil, China, India and Kenya, to take a few examples from emerging economies, **digital technologies are seen as a leap-frogging opportunity.** The success of indigenous programmes for digitally-driven financial inclusion, e-governance and e-commerce platforms, and the rise of a new elite of tech entrepreneurs has given many countries of the Global South the confidence to go their own way on digital technologies. Over-emphasising 'misuse' at the expense of 'missed' use will drive them away from the global governance of digital technologies.

A practice-rich approach governance should not be misunderstood as accepting the status quo or passively accepting what tech developers and companies roll out in the future. Instead, **it is about creating smart learning loops between policy and practice. That is the only way policy can keep pace with the rapid shift in the technology landscape, and practice can respect the intent behind policy.** It is about creating 'common rails' and 'guard rails', the former to level the playing field, promote inclusive demand and scale innovation, and the latter to prevent misuse and exclusion.

It could be argued that it is not the job of multilateral organisations to promote the use of digital technologies. They are better off setting norms and standards for use as well as tackling select cases of misuse such as development of lethal autonomous weapons. But if we do not bend the direction of private sector investments and national efforts with successful examples of 'good' use, misuse cannot be avoided. You do not get someone to stop thinking about a fish riding a bicycle by asking them to stop doing so. You have to give the mind something better to focus on.

It is particularly urgent to shift minds away from world dominance through Artificial Intelligence to solving the world's most urgent challenges through AI. **We need 'moonshots' to nudge thinking on data, algorithms and computing capacity away from scarcity to abundance and from conflict to cooperation.** In line with the UNSG Panel's recommended approach to digital public goods, these moonshots can be prepared in multi-stakeholder platforms involving the UN and related agencies but not necessarily owned or mandated by them. The excitement around them can attract a younger generation of digital natives, the practical idealists who are seizing the initiative on climate change for example, and channel their energy and talent into making digital technologies work for everyone.

The governance that comes out of these platforms of practice in areas such as health and financial inclusion (Recommendation 1a of the Panel's report) can extend to other areas. Its benefits would be more obvious to communities of practice in civic, private and public sectors. Such an approach will not only be more meaningful for diverse countries and populations, making digital governance more broad-based but also more sustainable in the long run.

Maintaining Strategic Stability in Cyberspace becomes the priority of cyberspace governance

Chuanying Lu

Cyberspace stability is already a prioritized topic in global governance agenda. There are already some initiatives starting to focus on the cyber stability issues, including Global commission on the stability of cyberspace, who defined"stability of cyberspace is the condition where individuals and institutions can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services in cyberspace is generally assured, where change is managed in relative peace, and where tensions are resolved in a peaceful manner."International Security Advisory Board, believes Cyber Stability would enhance continuity of relations between nations in the face of attack or exploitation through cyber means. Another initiative made by MIT and SIIS discussed the Military Cyber Stability, which refers to the condition under which interactions in the cyber dimension do not unduly destabilize traditional security architectures and force postures.

We are entering into an age of maintaining strategic stability of cyberspace. Cyberspace is disruptive, it is changing the nature of global strategic stability. Not just because The Internet was born from preventing the Nuclear attack. DARPA designed the original internet in order to maintain command and control over its missiles and bombers after a nuclear attack. Unfortunately, after over 50 years development of the internet, all nuclear state worries about their nuclear r command and control systems under the threat of cyberattack right now. This caused people nervous about the traditional strategic stability will be broken. More importantly. Cyberspace is already a strategic domain, which covers such diverse areas as from nuclear command and control systems up to personal cell phones. Equipment of a total amount of 200 billion will be connected in the future.

To understand strategic stability, we need to better understand the cyberspace. In social sciences, cyberspace is usually seen as the mapping of physical space into the digital world. In addition to related technologies, cyberspace also covers such dimensions in physical space as actors, behavior, as well as rules and norms, transcending the traditional "international norm dynamics." To be more specific, political, economic, social, cultural, military, scientific and technological activities of mankind in physical space are mapped into cyberspace by the process of informatization.

From this definition, we can define four basic characteristics of cyberspace related to strategic stability.

Basic Characteristics of Cyberspace

Disruptive is the impact of cyber to existing international system.

- Strategic describes the nature of state competition in cyberspace.
- Integrated means cyberspace should not be balkanized.
- Holistic applies to the construction of rules, norms, laws in cyberspace.

According to maintain the four basic characteristics cannot be changed by state behaviors, the goals of strategic stability in cyberspace are:

- Keep state strategic competition in check.
- Manage constraints to use cyber technology (e.g. adapt the international system accordingly).
- Consider the integrity of cyberspace in policy-making.
- Use holistic approaches for global governance of cyberspace.

According to the previous studies, here we can define the strategic stability in cyberspace as that the responsible state behavior should ensure the continuing evolvement of the global internet, avoid balkanization of cyberspace, protect the critical infrastructure from cyber military operations, exclude nuclear command and control systems as military targets. Also we need international cooperation to maintain the strategic stability in cyberspace. The international society should first Build a common understanding of strategic stability in cyberspace, raise the awareness of the importance of the strategic stability issues. Then we need more strategic coordination among big powers, in order to regulate their behavior in cyberspace, as well as avoid the cyber conflicts. Then, the international society also should develop governance mechanisms for cyber technology, to share knowledge and experiences like we did in other areas, which will be helpful to promote discourse in expert communities.

Finally, to establish institutions to maintain strategic stability in cyberspace, which the UN may need to convene the state top leaders to discuss how to design the institutions for peace in cyberspace.

DIGITAL ECONOMY

OECD: Embracing Multistakeholderism at a Multilateral Organization

Andrew Wyckoff

The UN High-level Panel Report on Digital Cooperation represents a welcome effort to improve the network of organisations and entities that contribute to Internet governance. It is well timed, as it comes as the world recognises that the digital transformation is fundamentally shaping every sector of the economy and many dimensions of society. Improving our understanding of this transformation has been the focus of OECD's "Going Digital" project since 2017[121].

In this sense, the OECD welcomes being a partner in this effort and being recognised as an organisation that can advance the measurement agenda and fill in some of the identified gaps where we need a sound evidence base. Experience shows that policies are more effective when developed based on facts and not anecdotes, the passion of the moment or competition between countries. The OECD takes prides in improving and using statistics and our most recent milestone, "Measuring the Digital Transformation"[122] is the latest step in this policy space. It sets out a forward road map of work that needs to be pursued to develop better measures of connectivity, human capacity, autonomous intelligent systems and trust – topics identified as priority actions in the UN Panel report.

However, the OECD is more than just a number crunching organisation. We can also contribute to advancing the policy agenda in a variety of areas. In fact, some of our experiences may provide a useful guide to the future of Internet governance and how to move from political aspirations to outcomes that are more concrete. The OECD engages with a variable geometry of countries, ranging from our committee meetings where about about a quarter of the delegates are not formal members to our Global Forums that now cover the world: the Global Forum on Transparency and Exchange of Information for Tax Purposes has 157 members participating. In addition, our active involvement with the G20 on digital policy issues since the 2016 Chinese Presidency broadens the number of countries we support in this space. A recent example of this, is the 2019 G20 Summit under the Japanese Presidency that agreed to support a set of G20 AI principles[123] that were drawn from the OECD AI Principles[124] that our Council adopted a month earlier.

Embracing Multistakeholderism at a Multilateral Organisation

Our smaller set of countries, many of whom have been pioneers in digital policymaking, may represent a configuration that is able to forge a consensus and has the flexibility to adapt to new working methods. One example of this is our early embrace of the multistakeholder approach to policy making that was formally enshrined in 2008 at the Seoul Ministerial Meeting after which the stakeholders at the Committee on Digital Economy Policy expanded from business and labour to include the technical community and civil society. These stakeholders are not window-dressing: they sit at the table next to government officials, they have access to the substantive documents in advance of the meeting, and they are encouraged to provide comments on the documents. The importance of a multi-stakeholder approach was further advanced when the OECD adopted in 2011 the OECD Internet Policy-making Principles[125] as a Council Recommendation of "soft law" which specifically recommend that countries include stakeholders in their policymaking.

This multi-stakeholder approach was used to constitute the Expert Group on Artificial Intelligence (AIGO[126]) in 2018-19 to explore the development of AI principles to "further the development of and trust in AI." Consisting of more than 50 experts including from each of the stakeholder groups, AIGO produced a draft proposal that was instrumental in the development of the OECD's AI Principles from which the G20 AI Principles are drawn. These principles embrace many of the aspirations of the UN HL Panel report such as human-centered values, transparency, robustness and accountability. These AI principles represent a prototype of how multilateralism and multistakeholderism can work to produce outcomes that advance digital governance.

In parallel, work is underway at the OECD that seeks to update our methods of taxation for the digital era. It also embraces a similar multi-stakeholder approach but one that includes a large set of countries. Its work will go beyond "soft law" and rather establish the basis for new tax regulations. This work has been underway for several years and is expected to reach fruition next year for the G20 under the Saudi Arabian Presidency.

A future architecture for Internet Governance

The UN Panel report is refreshing in its recognition that there is no single approach to digital cooperation. Chapter 4's list of five challenges and gaps provides a succinct list of the problems that need to be addressed by any new approach. The first two – the low political status of digital policy issues and making technical bodies more inclusive – will be relatively easy to fix.

The remaining three – the considerable overlap among mechanisms covering digital policy, the fact that digital issues now permeate a wide range of siloed-policy area (e.g. health, trade) and the lack of reliable data – are more intractable. Respectively, the overlap reflects to some degree the natural tendency of countries to seek coalitions with like-minded partners with similar economic and social contexts, and it will be hard to stop especially in the current environment; the awakening of various bodies to the digital transformation is to be welcomed, but they need to join the party, not operate in isolation; and as for data, one critical action is to put our money where our mouth is and fund our statistical agencies which includes paying higher salaries for public sector data scientists.

From where I sit, option 3, a "Digital Commons Architecture" is the most practical and pragmatic option and best respects the organic nature of the Internet. Clearly, it will not be easy to herd all the actors into various work streams, but the ethos of this community has always been shaped by a shared vision of a global commons.

Source

[121] https://www.oecd.org/going-digital/
[122] https://www.oecd.org/going-digital/measurement-roadmap.pdf#targetText=Measuring%20the%20Digital%20Transformation%3A%20A,%3A%20Shaping%20Policies%2C%20Improving%20Lives.
[123] https://www.mofa.go.jp/files/000486596.pdf#targetText=a)%20AI%20actors%20should%20respect,and%20internationally%20recognized%20labor%20rights.
[124] https://www.oecd.org/going-digital/ai/principles/
[125] https://www.oecd.org/internet/ieconomy/oecd-principles-for-internet-policy-making.pdf
[126] http://www.oecd.org/innovation/oecd-creates-expert-group-to-foster-trust-in-artificial-intelligence.htm

Distributed Co-Governance Architecture: Construction in Progress

Richard Samans

The internet and a number of emerging technologies of the Fourth Industrial Revolution present a particular challenge for international governance and cooperation. Unlike other policy domains, there is no institutional focal point for technology governance in the international system, just as there tends not to be an integrated focal point for such policy in national governments. In addition, because the technologies are developing rapidly and being applied in constantly evolving and intersecting ways, traditional, formal rule-setting processes often may not be the most appropriate or effective approach to strengthening cooperation and governance in the public interest.

Yet the economic, social and security stakes are enormous. This is perhaps nowhere better illustrated than in Japan's "Society 5.0"[127] integrated technology vision in which people, things, and systems are connected in cyberspace with the resulting data analysed by AI and fed back into physical space in ways that bring extraordinary new value to industry and society.

One study estimates that artificial intelligence (AI) could generate an additional $15.7 trillion[128] (US) in economic value by 2030, slightly more than the current annual economic output of China and India combined, with 40% of this value likely to accrue to China and the US alone. The EU estimates[129] its digital market "could contribute €415 billion [$472 billion] per year" to the economy, while projections for ASEAN[130] digital integration are around $1 trillion (US) in gains by 2025. Meanwhile, genome-editing technology CRISPR may develop a market of over $10 billion by 2027[131], and cryptocurrency markets already register gains and losses[132] in the billions, sometimes within a single day.

But while AI is likely to generate new wealth, some analysis[133] suggests it could make inequality worse[134] and even increase the risk of nuclear war[135]. There are also potential environmental and social costs of the technology revolution. Bitcoin, for example, requires a network with energy consumption[136] roughly equal to Singapore,66 producing 262 kg of CO2 for each of its more than 250,000 transactions per day, and the recent concern over "fake news" has been connected to the proliferation of "bots"[137], automated accounts driven by algorithms. As emphasized by the Stewardship Board of the World Economic Forum's Digital Economy and Society System Initiative in its recent report, Our Shared Digital Future[138], greater cooperation among all stakeholders is necessary to bolster trust in technology.

The report of the UN Secretary General's High-Level Panel on Digital Cooperation[139] has rightly suggested that digital cooperative governance should take the form of a "distributed co-governance" approach, encompassing various purpose-built configurations that involve governments, the private sector, civil society, international organizations, academia, the technical community and other relevant stakeholders. A new and quite variable geometry of international digital cooperation remains at an early stage but is developing (some might say proliferating) very rapidly. Following are a number of illustrative examples, both multidisciplinary and issue-specific:

On the multidisciplinary plurilateral front, the Digital 9[140] group of leading digital nations have been gathering in different configurations since its launch in the UK in 2014. Canada convened the group, which shares world-class digital practices, collaborates to solve common problems, and identifies how digital government can provide the most benefit to citizens, in December 2018 as part of the follow up activities related to its G7 presidency.

On the multidisciplinary multi-stakeholder front, the World Economic Forum launched the Centre for the Fourth Industrial Revolution Network[141] (C4IR) in 2017 to serve as a public-private platform for the collaborative development and refinement of governance frameworks and protocols that more fully anticipate the risks and accelerate the benefits for societies of advanced technologies. It brings together governments, business organizations, dynamic start-ups, civil society, academia and international organizations to co-design human-centred governance protocols and policy frameworks, and pilot them with government and industry partners. The Centre Network is headquartered in San Francisco and is establishing operations in Japan, India, China and several other countries in cooperation with their governments at the highest level along with leading business, civil society and academic figures. Its programme of multi-stakeholder policy development and piloting is active in nine technology domains. With nearly 30 government partners now engaged, the C4IR established leader-level global councils in six domains in 2019, composed of ministers and heads of regulatory agencies, chief executive officers and leading technical and civil society experts to cross-pollinate international policy experience sharing and public-private cooperation. The aim is to help shape the global technology policy and corporate governance agenda by providing a unique place in the international system where policy dialogue, practical learning and international agenda setting can take place across stakeholders and regions on an ongoing basis.

Artificial intelligence and machine learning

As part of the 2018 G7 process, Canada and France announced the creation of a multistakeholder International Panel on Artificial Intelligence (IPAI)[142] that could become a global point of reference for understanding and sharing research results on AI issues and methodologies as well as convening international AI initiatives. The stated mission of the panel is to support and guide the responsible adoption of AI that is human-centric and grounded in human rights, inclusion, diversity, innovation and economic growth. It aims to facilitate international collaboration among the scientific community, industry, civil society, related international organizations and governments. By relying on the expertise of important stakeholders and providing a mechanism for sharing multidisciplinary analysis, foresight and coordination capabilities, the panel plans to conduct analysis intended to guide policy development and the responsible adoption of AI.

The Institute of Electrical and Electronic Engineers' (IEEE) Global Initiative on Ethics of Autonomous and Intelligent Systems (A/IS)[143] was launched in April 2016 to incorporate ethical aspects of human well-being that may not automatically be considered in the current design and manufacture of A/IS technologies, and to reframe the notion of success so that human progress can include the intentional prioritization of individual, community and societal ethical values. The initiative seeks to ensure that every stakeholder involved in the design and development of autonomous and intelligent systems is educated, trained and allowed to prioritize ethical considerations so that these technologies are advanced for the benefit of humanity. It has two primary outputs: the creation and iteration of a body of work known as Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems; and the identification and recommendation of ideas for standards projects focused on prioritizing ethical considerations in A/IS. The Global Initiative has recently increased from 100 AI/ethics experts to more than 250 individuals, including new members from China, Japan, South Korea, India and Brazil.

The OECD Principles on Artificial Intelligence promote artificial intelligence (AI) that is innovative and trustworthy and that respects human rights and democratic values. They were adopted in May 2019 by OECD member countries when they approved the OECD Council Recommendation on Artificial Intelligence[144]. The OECD AI Principles are the first such principles signed up to by governments. Beyond OECD members, other countries including Argentina, Brazil, Colombia, Costa Rica, Peru and Romania have already adhered to the AI Principles, with further adherents welcomed. The OECD AI Principles complement existing OECD standards in areas such as privacy, digital security risk management and responsible business conduct. In June 2019, the G20 adopted human-centred AI Principles[146] that draw from the OECD AI Principles.

The Forum's Centre for the Fourth Industrial Revolution AI and Machine Learning Platform has begun work on several artificial intelligence governance projects. The first is developing a governance framework or toolkit for boards of directors to aid them in asking the right questions, understanding the key trade-offs and meeting the needs of diverse stakeholders, including how to consider approaches such as appointing a chief value officer, chief AI officer or AI ethics advisory board. It is being designed around four pillars: technical, brand, governance and organizational impacts of AI, each providing an ethical lens for creating, marketing and sustaining AI in the long term. The second is drafting a framework to guide government procurement of AI products and services. Government procurement rules and purchasing practices often have a strong influence on markets, particularly in their early stages of development. The third project is designing best practice guidelines and policy measures for the protection of children in cooperation with UNICEF. In the absence of clear guidelines, parents and caregivers are left to make decisions about toys and other AI-enabled products with incomplete information about the implications for their children's well-being and privacy. As these devices come onto the market, mechanisms will be needed to protect children while enabling the benefits of "precision education".

The Partnership on AI (PAI)[147] is a multistakeholder organization that brings together academics, researchers, civil society organizations, companies building and using AI technology, and other groups working to better understand AI's impacts. The partnership was established to study and formulate methodologies on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discussion and engagement about AI and its influences on people and society.

Data

The data intensity of the Fourth Industrial Revolution is posing multiple policy challenges relating to privacy, security, bias, accountability, abuse of personal data, antitrust, international trade, access to public services, etc. Most governments are still in the early stages of developing policy frameworks, and international coordination is similarly nascent but greatly needed.

There are over 120 different data protection and privacy laws in effect around the world, raising concerns about the compliance and transaction costs for firms navigating this patchwork quilt of regulation. A particular concern is the

burden compliance may place on small and medium-sized enterprises (SMEs), which do not have the large legal departments and budgets of multinational firms.

China, the US and Europe have fundamentally different regulatory approaches to data protection and enforcement. The US and China tend to take a light regulatory approach unless or until a specific harm is identified. In addition, the US regulates data by sector and type. There is no uniform omnibus privacy law in the US, although the recent passage of the California Consumer Privacy Law has sparked renewed interest in the passage of such a law to pre-empt 50 different state laws and potentially countless local laws. While the US appears to have a less protective privacy model than Europe, comparisons of enforcement practices seem to indicate that privacy outcomes are not dramatically different.

Europe's General Data Protection Regulation (GDPR) went into effect in late May 2018. In creating a strict regulatory framework for data, Europe has set a high bar. It hopes to encourage countries to coalesce around its model, thereby setting a de facto global standard. Many countries are indeed working to achieve GDPR "adequacy", and several new laws have been adopted in countries such as China and Brazil that look very similar to GDPR. But the distinguishing feature of GDPR is the potential cost of non-compliance, which can run up to 4% of global revenue. Prior regulations included fines that had little to no deterrent effect on companies with market values in the tens and hundreds of billions of dollars.

China has adopted a security law that requires all foreign companies to localize data about Chinese consumers within China's borders. Other rules accompanying the new security law include requirements that look very similar to GDPR, but it remains to be seen how enforcement will be carried out, including whether foreign companies will be treated differently from domestic entities.

Between the differing data localization requirements, data protection rules and approaches to data ownership and online content and expression around the world, there is a growing risk that the internet will fragment into separate, parallel systems. There is also rising concern that the centrality of data to value creation in the Fourth Industrial Revolution will serve to widen the already large digital divide in the world, particularly between the US and China (which host all 20 of the world's largest technology companies by market valuation) and other countries.

Indeed, growing appreciation of the value of open data has led municipalities and nations to begin mandating open data laws. For example, France's Digital Republic Act[148] requires government agencies to move to an open data orientation and to set quality standards for such data. Barcelona's Open Data BCN[149] is just one example of a municipality administrative initiative that prioritizes the availability of public-sector data for free use by interested parties and includes statistical and public-service data. At the international level, a multistakeholder set of good governance principles, A Contract for the Web[150], is gathering support from companies, governments and civil society groups. These principles establish a set of commitments on the part of governments, companies and citizens that aim to increase the agency of citizens over their data and protect the open web as a public good and basic right for everyone.

Blockchain and distributed ledgers

Blockchain, an early-stage technology that enables the decentralized and secure storage and transfer of information, has the potential to be a powerful tool for tracking and transactions that can minimize friction, reduce corruption, increase trust and support users. Cryptocurrencies built on distributed ledger technologies (DLT) have emerged as potential gateways to new wealth creation and disruptors across financial markets. Other revolutionary use-cases are being explored in almost every sector, ranging from energy and shipping to media. Blockchain has the potential to upend current models of data ownership, giving users greater control over their data, granting access at a more granular level and enabling micropayments for data usage. In addition, the digital representation of real-world assets on a blockchain, as well as the emergence of new categories of crypto assets, offer new financial opportunities for stakeholders. New economic models could enhance privacy, security, inclusion and individual rights, potentially shifting control of user data from shareholders to consumers while providing access to new funding flows. In sum, DLT has the potential to upend entire systems, but it also faces important policy and cooperation challenges, including lack of interoperability, security threats and potential environmental and financial system impacts. Innovative policy mechanisms are needed to unlock this potential and manage the unforeseen consequences of these new paradigms.

The C4IR Global Network is co-designing and piloting governance protocols to ensure the interoperability and inclusivity of the myriad blockchain experiments attempting to track and manage supply chains. And it is developing approaches to balancing transparency and anonymity on blockchains as well as supporting the creation of a collaborative framework

within which Central Banks can responsibly explore and experiment with blockchain given its important potential financial services applications, including digital currencies.

Internet of Things and Connected Devices

There are more connected devices in the world today than humans. These devices, commonly known as the internet of things (IoT), come in infinite forms, from smart building technologies that monitor and manage energy usage to connected vehicles that help anticipate and avoid potential collisions. By 2020, the number of IoT devices is projected to exceed 20 billion, and as they spread to all aspects of day-to-day life, and even become embedded in the human body, questions about data ownership, accuracy and privacy protection take on greater importance. Similarly, in an interconnected world where electric grids, public infrastructure, vehicles, homes and workplaces are capable of being accessed and controlled remotely, the vulnerability to cyber-attacks and the potential for these security breaches to cause serious harm are unprecedented. The C4IR Global Network has co-design an Industrial IOT Security protocol with diverse stakeholders that is now being piloting in various industries. And as new voice-enabled speakers, smart home systems and wearables enter the consumer market, the C4IR Global Network is exploring the possibility of standardized labels or disclosures about public safety risks. Efforts are needed to align the private sector, government and civil society on common approaches to inform, educate and build trust among consumers on topics such as privacy and security. Finally, a very small amount of data (less than 1% according to some studies) is actually used to drive decisions and add value. To unlock data silos and unleash the full potential of the IoT, the C4IR Global Network is developing new models of data sharing within and across the public and private sectors that will be critical to enable cities and rural communities to maximize the cross-cutting value of IoT data and enable more sustainable business models.

Conclusion

This recent profusion of cooperative innovation on digital cooperation shows great promise and is in line with the UN High-Level Panel's vision of distributed co-governance. However, it does pose a number of specific cross-cutting issues. For example, agility and flexibility in technology governance is one thing, but how and where will broader efforts to strengthen inclusion be advanced and coordinated? This includes not only the digital infrastructure, human and institutional capacity and human rights imperatives emphasized by the UN High-Level Panel Report but also the fundamental question of how economic policy more generally must structurally adapt to the labor and community dislocation and opportunity- and income-dispersing effects of digital disruption.

It also raises an overall question about systemic coherence: how and where will the dots be connected among initiatives and norms being created in this bottom-up fashion within each technology governance domain, not to mention among them? The IGF is an obvious candidate, as an inclusive multistakeholder forum for dialogue anchored in the United Nations. However, to perform this function well going forward, its official scope will need to expand beyond "internet governance" to digital cooperation and governance more broadly, reflecting the major additional aspects of digital or Fourth Industrial Revolution governance this chapter has surveyed and beyond.

Source

[127] *https://www8.cao.go.jp/cstp/english/society5_0/index.html*
[128] *https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf*
[129] *https://ec.europa.eu/commission/priorities/digital-single-market_en*
[130] *https://www.bain.com/contentassets/37a730c1f0494b7b8dac3002fde0a900/report_advancing_towards_asean_digital_integration.pdf*
[131] *https://www.prnewswire.com/news-releases/global-crispr-technology-market-2018-2027-market-is-expected-to-reach-10-55-billion-300636272.html*
[132] *https://www.blockchain.com/en/charts*
[133] *https://www.nber.org/papers/w24174*
[134] *https://www.nber.org/papers/w24174*
[135] *https://www.rand.org/blog/articles/2018/04/how-artificial-intelligence-could-increase-the-risk.html*
[136] *https://digiconomist.net/bitcoin-energy-consumption*
[137] *https://www.sciencenews.org/article/twitter-bots-fake-news-2016-election*
[138] *http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf*
[139] *https://digitalcooperation.org/*
[140] *https://www.canada.ca/en/treasury-board-secretariat/news/2018/11/canada-welcomes-leading-digital-nations-into-the-digital-9.html*
[141] *https://www.weforum.org/centre-for-the-fourth-industrial-revolution*
[142] *https://pm.gc.ca/eng/news/2018/12/06/mandate-international-panel-artificial-intelligence*
[143] *https://standards.ieee.org/industry-connections/ec/autonomous-systems.html*
[144] *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449*
[145] *https://www.mofa.go.jp/files/000486596.pdf*
[146] *https://www.weforum.org/communities/artificial-intelligence-and-machine-learning*
[147] *https://www.partnershiponai.org/*
[148] *https://www.republique-numerique.fr/pages/in-english*
[149] *http://opendata-ajuntament.barcelona.cat/en/*
[150] *https://contractfortheweb.org/*
[151] *http://www3.weforum.org/docs/WEF_Advancing_Human_Centred_Economic_Progress_WP_2017.pdf*

Amazon and Internet Governance - The Future of Internet Governance Is Now

Brian Huseman

Amazon has long appreciated the dynamic nature of the internet and its impact on citizens globally. Indeed, Amazon's growth and history hews closely to the maturation of the commercial Internet as we know it today. And as a company that relies heavily on an open, free, secure, and interconnected internet, Amazon has long supported multi-stakeholder policies and practices that further the internet's growth for all.

To be sure, the internet governance and policy landscape has changed significantly over recent history. Matters such as online content moderation, privacy and data flows, cybersecurity, digital rights, and others have dominated policy discussions and headlines. As these complicated policy matters continue to, rightfully, garner attention, the need increases for more coordinated and collective transnational efforts to deal with internet policy issues of concern.

But in the face of certain countries moving away from "one internet," it is imperative that we double-down on multi-stakeholder solutions to difficult transnational policy concerns. As tempting as it may be to seek provincial legislative or regulatory fixes, voluntary multi-stakeholder solutions can and must remain a tool towards solving fast-moving and challenging transnational internet problems.

Nobody should take the cross-border internet for granted. It is the seamless and cross-border nature of the internet that allows Amazon to strive to be the Earth's most customer-centric company. Ensuring an open internet where anyone can innovate and trade is critical to the continued success of the digital economy.

The need to move data across borders is a necessary aspect of e-commerce. Policies that limit cross-border data flows drive up transaction costs and produce additional frictions for consumers.

Amazon has long supported various multi-stakeholder initiatives and entities, including the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet & Jurisdiction Policy Network, and the Internet Governance Forum (IGF). All of these, and others, contribute towards creating understanding, mechanisms, and, ultimately, policies that facilitate a robust internet ecosystem.

Of course, despite the relative success of the multi-stakeholder model of internet governance, this is no time to rest on laurels. Amazon recognizes that further enhancement and improvement of the multi-stakeholder model is necessary. To this end, for example, Amazon is actively engaged in a variety of stakeholder groups and constituencies within ICANN and works closely with all stakeholders, including governments, towards enhancing ICANN's accountability and an improved policy development process. With respect to the IGF, Amazon supports making the IGF a more vibrant platform for concrete discussions involving all necessary entities. Amazon is sensitive to the concerns raised by some who believe the IGF is no longer fit for purpose. In this regard, Amazon appreciates the general concept of an enhanced IGF, as explored by the U.N. High-Level Panel on Digital Cooperation. Further discussions about how best to improve the IGF should occur and Amazon looks forward to actively participating in those discussions.

The commercial internet is not yet 25 years old. Amazon launched in 1995. Multi-stakeholder internet governance as we know it today is younger still. The multi-stakeholder experiment continues, but it requires a redoubling of efforts and commitment from all interested stakeholders to work together to ensure the commercial internet serves the global public for at least another 25 years and beyond.

At Amazon, we always refer to each day as "Day 1." This means that we must always think about our customers with renewed focus and seek to innovate on their behalf every day. It must also remain Day 1 for internet governance – stasis is not an option. The future of the internet depends on a holistic, multi-stakeholder engagement – the policy issues are too complex and the stakes are too high to do otherwise. The future of internet governance is now.

African Perspective on Global Internet Policy Making

Daniel Nanghaka

According to the Draft Declaration on Internet Governance[152] it was acknowledged that Africa's voice in global Internet Governance is critical to the stable development of the global economy that is intertwined with Africa's economy and needs to be significantly elevated.

A new global governance approach that flows through various administrative structure continues to be a gospel that is preached across the globe in which a team of corporate executives, leaders of civil society organizations, officials from governments, academics and other players take on the governance of a specific international challenge defining Multi Stakeholderism.[153]

AU in collaboration with the United Nations Economic Commission for Africa (ECA) and civil society organizations continue to strengthen African participation in global Internet governance and related public policy discussions. The AfrIGF[154] remains a center of discussion of issues related to Internet Governance in Africa but have limited actionable items which are to be implemented. After Fora, follow-up items implementation mechanisms are minimal. This brings an agenda to review the mandate and implementation procedures of policy development process in relation to review outcomes or recommendations that come from biggest consortium of multistakeholderism in Africa.

The Internet is often cited as not only one of the prime examples of multi stakeholder participation in governance but sometimes described as inherently 'multistakeholder'. The Internet is defined by open, distributed, interconnected, participatory, and bottom-up processes – features that match multi stakeholder participation in specific regard to its governance. Vint Cerf, one of the authors of the Internet Protocol (IP), has similarly noted that.

The biggest challenge of Multistakeholderism is driving consensus or agreement. With African disintegration in administration which affects policy development, it is difficult to achieve a unique value proposition of the approach. With the challenges faced in connectivity – less than 20% of Africans are online[155], the majority of those not connected are women and the rural poor, and that the average cost of fixed line and mobile internet exceeds 50% of average per capita income poses a paradigm shift in the representation of the regional voices in the global internet policy making process.

This shows a need to enhance internet development in the region. The business models that drive connectivity are linked to where there is a return on investment in Infrastructure. Where the returns are low and cannot match the operational expenses limit the growth[156]. Will policy solve the challenge? This becomes a question that drives the collaboration between corporate companies and government legislatures as majority of the African economies are driven by the Non-Government companies and nonprofit organisations. Nonprofits in Africa are more of Humanitarian which drive the needs of livelihood enhancement contributing less to the Multistakeholder models of internet governance.

What is the future of Multi-Stakeholderism in Africa?

The biggest challenge to the present Internet governance models are related to accountability, which is affected by weaknesses of transparency with respect to deliberations of the decision making bodies in Internet governance.[157]

Multi-stakeholder contribution to global policies is influenced by super countries who contribute to the development of Internet infrastructure in Africa with low cost solutions deployed.[158] These solutions are also subject to surveillance and remote monitoring.[159]

"Most policymakers and politicians in Africa don't really care. Africa is a pawn on the global chessboard in the ongoing geopolitical context. Everybody spies on Africa," Emeka Umejei (journalism Lecturer, American University of Nigeria.)[160]

Although secrecy clauses are legitimate, there should be more transparency on how decisions are made, i.e. on what grounds, with which objectives. In Africa there is a still a challenge of judicial review given in Internet governance matters; governance rules are therefore not accountable to judges. Though there is still a claim that the Multistakeholder model of Internet governance remains a key drive to appropriate policies and internet governance.

There are up to 16 national[161], sub-regional and regional[162] IGFs in Africa. These numbers continue to grow. Of the African countries that hosted[163] forums during 2016, most were civil society led with some support from government reported – for instance in Ghana, Nigeria and Uganda. However, there was limited participation by the judiciary and law enforcement, youth and the private sector.[164] This portrays the need to drive participation from the judiciary and law enforcement agencies. Of late the African youth started the Africa Youth Internet Governance forum[165], contributing to the Internet Governance in Africa which has contributed to the Youth Coalition on Internet Governance.[166]

Speaking at the African Union (AU) session[167] at the IGF, Olugbile stated that bringing more stakeholders to the table on internet governance in Africa requires "embracing" policy documents from the continent, such as the African Union Convention on Cyber Security[168] and the African Declaration on Internet Rights[169] – less so international instruments – so as to ensure contextual understanding of key concerns. This would contribute to a demonstration of value in participation for the stakeholders currently not participating. Furthermore, it would ensure that agendas for debate are localized to suit African needs and follow ups on recommendations are directly linked to the mandate of the relevant stakeholders. This portrays an African framework that could be implemented which creates a link between the IGF and the regional IGFs.

Recommendations

Internet Governance discussions in Africa should be further developed in the next decade through feedback and response to the bottom up process; and policy registries shared to various stakeholders which include the Ministerial meeting that are held to include strongly the agenda of Internet Governance and how to effectively regulate internet governance principles and practices.

Multistakeholderism is the dominating mode of governance that has been shown in various fora[170]. There is a need for a holistic approach to Internet Governance, taking into account the interdependence of stakeholders (governments, business, civil society, technical community) and the interdependence of sectors (cybersecurity, digital economy, human rights, technology as the main four baskets of the global Internet Governance Ecosystem) remains a key drive for making African voices be heard.

Appropriate jurisdictions and community deliberations are important in the drive of better and enhanced internet policies in Africa. With unified model for eccentric development of internet policies which stream across various boundaries, clear and open standards are pertinent in the drive of these models. These call for collaborations between various stakeholders, legal entities and key drivers on a common round table based on their respective strengths.

Conclusion

In conclusion, the idea of enhancing existing or creating new global mechanisms to frame the future development of digital cooperation remains a key issue when it comes to global engagement of African opinion and position in global issues of internet governance.

Various (multi-stakeholder) institutions that have contributed to the Internet's global growth and while advocating for their continued role as the core of the global Internet governance ecosystem are not global in their operations and processes. There is a need of institutional transformations to be more inclusive and represent African citizens, taking into account the regional concerns and needs.

Source

[152] https://au.int/sites/default/files/newsevents/workingdocuments/31357-wd-au_declaration_on_internet_governance_draft_v21072015_21.pdf
[153] https://www.passblue.com/2019/09/02/they-call-it-multistakeholderism-where-does-that-leave-the-un/
[154] https://www.afigf.africa/
[155] https://www.passblue.com/2019/09/02/they-call-it-multistakeholderism-where-does-that-leave-the-un/
[156] Investments are driven by growth and investors target Return on Investment in a particular infrastructure. Following the Uganda IGF it is quoted that where there is limited returns, the cost of infrastructure growth tends not to match the returns hence limiting the growth or internet penetration is some regions.
[157] Discussion paper on Mapping Multistakeholderism in Internet Governance: Implications for Africa by Enrico Calandro, Alison Gillwald & Nicolo Zingales
[158] In January 2018, the French newspaper Le Monde reported that Beijing had bugged the headquarters of the African Union—whose construction was paid for and built by China. Every night for five years the entire contents of the building's computer systems—which were installed by Huawei—were reportedly transferred to China. Microphones were found embedded in the desks and walls, according to the report. Both China and the African Union dismissed the allegations.
[159] https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html
[160] https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/
[161] http://www.intgovforum.org/multilingual/content/national-igf-initiatives
[162] http://www.intgovforum.org/multilingual/content/regional-igf-initiatives
[163] https://igf2016.sched.com/event/8ht6/national-and-regional-igfs-nris?iframe=no&w=100%25&sidebar=yes&bg=no
[164] https://cipesa.org/2016/12/how-applicable-is-the-multi-stakeholder-approach-to-internet-governance-in-africa/
[165] https://yigf.africa/
[166] https://www.intgovforum.org/multilingual/content/youth-coalition-on-internet-governance-ycig
[167] https://igf2016.intgovforum.org/
[168] https://cipesa.org/2014/01/civil-societys-proposals-on-the-african-cybersecurity-convention/
[169] http://africaninternetrights.org/
[170] These For an include and are not limited to Africa IGF, AFRINIC Meeting, AfPIF, Community Network summit, etc as some of the events that have brought together various multi-stakeholders to discuss a common goal related to the Internet and its respective policies in Africa region

How UNESCO's ROAM can reinvigorate Internet governance

Guy Berger[171]

UNESCO is an intergovernmental body, and at the same time it is also one that enjoys strong ties with non-state actors. This flows from the mandate of the organisation in covering education, science, culture and communication, which necessitates deep engagements and partnerships with diverse civil society groups and, where possible, with private sector actors as well.

This insight is key to understanding how it came about that UNESCO, as a multilateral institution, nevertheless adopted a position on the Internet in 2015 after an explicitly multistakeholder process.

That process was a consultative study, launched in November 2013 at the initiative of UNESCO Member States. The initiative responded to the call from some states for the Organisation to adopt an instrument on safeguarding privacy, in the wake of the Snowden revelations. A two-year research process, canvassing a very wide range of actors around the world and with 200 formal submissions, culminated in the multistakeholder "CONNECTing-the-dots" conference in 2015.[172]

The outcome statement of the conference chartered a path between the idea of a UNESCO instrument on privacy and no action at all. It offered a midway option in the form of a powerful concept titled "Internet Universality". Endorsed unanimously some months later by 195 states at the UNESCO General Conference, the concept has significant normative value in signalling a single Internet as well as an Internet for everyone. Such universality is seen as the combined effect of four key principles which are summarised under the memorable acronym of ROAM.[173] These are: human Rights, Openness, Accessibility to all, and Multi-stakeholder participation

ROAM designates distinct but interdependent ideals that guide us as to how the Internet should be shaped, and it also serves as a prism for assessing change. The holistic thinking here is that having respect for Rights online, but lacking universal Access, is a recipe for exclusivity, rather than for inclusivity and universality. Conversely, Accessibility to an Internet that falls short in regard to rights, is not normatively desirable.

This kind of interdependence is to be further understood in terms of the uniqueness of the Internet in that this communications facility has come about through Openness – of technology, standards and markets. Hence, this principle is critical to sustaining the digital whole.

Lastly, the integrated package of Rights, Openness and Accessibility can, in the Internet Universality perspective, only be assured through participative governance – the M of ROAM. The foundation of the Internet in multistakeholder practice serves to draw in different interests and insights, at the same time as also fending off capture by any single dominant actor or single stakeholder sector.

The ROAM perspective is not exhaustive for the Internet. Indeed UNESCO's 2018 indicators to assess ROAM at country-level, expand the notion into ROAM-X in order to reference several cross-cutting issues, such as economic issues and network security, which are also obviously important for shaping the Internet.[174] Nevertheless, it can be affirmed that the UNESCO focus puts a finger on four key dimensions which no one should ignore. Indeed, ROAM is recognised in the report of the UN Secretary-General's panel High Level Panel on Digital Cooperation[175].

Further, the UN Human Rights Council adopted Resolution (A/HRC/38/L.10/Rev.1 on the promotion, protection and enjoyment of human rights on the Internet, which references UNESCO's process of developing Internet Universality indicators as a means to contribute to advancing online human rights and achieving Sustainable Development Goals.

With its background, ROAM now stands as an approach with substantial legitimacy. As such, it opens doors for dialogue between different, even opposing, entities. Further, as a framework with indicators for measurement, the world now has a handy instrument that carries the stamp of the UN. In this way, ROAM is a meaningful contribution to norms for shaping the Internet going ahead – including for the evolution of technologies like Artificial Intelligence which have grown within the interconnected global ecosystem.

The achievement represented in "ROAM" and its potential can be additionally unpacked in terms of the classic conceptualisation of Internet Governance which recognises the patchwork of "shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet".[176]

Through its UNESCO status, the package of ROAM principles is directly relevant to elaborating the norms to underpin rules and decision-making. For example, the package points stakeholders to keep in mind human Rights implications in regard to digital developments, as well as to avoid treating these in isolation of Openness and Accessibility – and vice versa.

Internet governance includes the classic nuance that provides for involvement by "Governments, the private sector and civil society, in their respective roles".[177] There are indeed different roles for different stakeholders, but what the Multistakeholder insistence in ROAM highlights is the principle of shared interest in consultation about formulating of rules, procedures and programmes, as well as in implementation or evaluation processes at the operational level.

The M in ROAM reminds us that involvement by different interest groups produces well-informed decisions in a field that is characterised by enormous complexity, interdependence and unforeseen effects, as well as a reality where there is decision-making under uncertainty and ignorance.[178] What this means, is that all stakeholders – and just state entities (eg. parliaments, regulators) – are seen to do well to practice multi-stakeholder governance. This principle applies also to companies in the formulation of their codes of conduct, academics in regard to their research ethics, technologists in their experiments, etc ... .

How does Internet Universality thus become meaningful and have real impact? At global level, UNESCO is promoting the concept and its indicators widely, including in their relevance to the subject of ethics and artificial intelligence.

At country level, actors in 11 countries in 2019 are already applying the ROAM-X indicators in order to diagnose the health of the Internet as experienced in their national space. Research based on these indicators, guided by a Multistakeholder Advisory Board, will culminate in recommendations for improvement and related dialogues. The resulting momentum is expected to improve the Internet for everyone in the country.

In such a way, this type of digital co-operation at national level could in some cases even lead to institutionalised or constitutionalised governance modalities. And the national engagement with ROAM can in turn feed into enriching the character of various distributed global processes that are grappling with digital problems and opportunities.

If indeed, the Internet is to help amplify progress towards the Sustainable Development Goals, UNESCO Internet Universality offering merits increased attention going forward.

Source

[171] This chapter is written as part of the author's work as Director for Freedom of Expression and Media Development, UNESCO. However, the ideas and opinions expressed are not necessarily those of UNESCO and do not commit the Organization.
[172] http://www.unesco.org/new/en/internetstudy
[173] http://www.unesco.org/new/en/communication-and-information/crosscutting-priorities/unesco-internet-study/internet-universality/
[174] https://en.unesco.org/themes/internet-universality-indicators
[175] https://www.un.org/en/digital-cooperation-panel/
[176] https://www.wgig.org/docs/WGIGREPORT.pdf
[177] https://publicadministration.un.org/en/internetgovernance
[178] Van der Spuy, A. 2018: What if we all governed the Internet? Paris, UNESCO.

Because I am involved!

Nnenna Nwakanma

My name is Nnenna. I come from the Internet. I followed the High-Level Panel's work very closely. I participated in Consultations in Europe and in Africa, Community Consultations, Online Consultations, even a one-on-one consultation. Having been around since WSIS, the Digital Solidarity Fund, Netmundial and the global, regional, subregional, and some national IG Forums. I hold stakes here.

I was a bit underwhelmed by the report. I had expected a more indepth document, of more than 30 pages! What effort the panel must have made in deciding what to keep, how to keep it and what not to put in the main report! I loved the title, **The Age of Digital Interdependence.** For one, it captures the vision of the pioneers of the Internet: community, commons, co-creation, multi-stakeholders, embracing the future and like Sir Tim Berners-Lee, the inventor of the world wide web puts it "**For Everyone**".

For me, "Digital" is not the problem. Technology in itself, has not been our major issue. Our challenge is with "Cooperation"... in other words, with people, humans. One question keeps running on my mind: If Digital Solidarity Fund died, and NetMundial went cold, what guarantee do we have that Digital Cooperation will live? How do we engage, going forward, to make it sustainable. Maybe by 2020 we will have a way forward... The introduction of the term "multilateralism" and "holding each other accountable, along with multistakeholderism, for me is a good indication that we may finally be able to have governments get "passionate" over this.

Either for political correctness or just lack of space, I did not see an acknowledgement of the geo-political tensions that exist in our real world. Are the forces that hold sway in global warming, global arms (war and peace), global financial flows (licit and illicit), international air and sea movements, world trade and commerce (tariffs and trade wars), not be the same in Digital Cooperation? What will be the difference between this "Digital Cooperation" and the existing development landscape as we know it today? Virtual collaboration is great but real world (geographic and political) forces (push and pull) are here with us. Will something new happen?

The proposed architectural models for coordination made me smile. The IGF is so much like the United Nations: no rapid response team (army), not enough budget, not much teeth to bite, and not able to take decisions and implement them. The IGF is not what we want it to be. But we do not have a better option. We all wish to be happy, but since we cannot all be happy in our own ways, we settle for collective dissatisfaction.

Here is what I see:

There is the pessimism of processes that came and went, but also the optimism of a renewed global concern.

We need to acknowledge the pessimism of long tortuous UN processes but also the optimism of a large global digital community.

There is the pessimism of the connected 50% who may not care, but also the optimism of the unconnected 50% who are to come online.

It is time to balance the pessimistic drive of some actors to control and dominate others with the strong optimism of multiple others who seek to use digital tools for human development, poverty reduction and job creation.

The age of digital interdependence is the ripe age to challenge the strength of digital pessimism with the power of resolute, concerted digital cooperation.

NETmundial's experiments should be recovered

Raúl Echeberría

In 2004, while working as part of the Working Group on Internet Governance (WGIG) created by Kofi Annan, I proposed an argument which I believe is still very relevant fifteen years later.

At the time, I argued that behind the discussions on the various multi-stakeholder models was the question if the statement "governments are the only legitimate representatives of the interests of their peoples" was valid. Back then, this gave rise to a very interesting discussion.

This discussion remains relevant and I am absolutely convinced that this statement is not valid and that, even if it had been valid at some point in time, this is no longer the case.

People have access to an abundance of information, even if they are connected, that allows them to shape their own views on various issues, in some cases practical and everyday issues, in others, issues of a more strategic and political nature.

There is no originality in saying that the world has changed dramatically since the widespread use of ICTs, and this is one of the consequences brought about by these changes. Citizens no longer need to delegate 100% of the issues to a single group of representatives and, in many cases, they prefer to choose different participation and representation channels for different topics.

An individual is not defined by a single aspect, is defined by many (citizenship, place of residence, profession, and so on). Each of these aspects involves specific interests that can be represented in each case by different organizations, or even by the person themself. The governance models have to fit this reality.

The emergence of the Internet and the subsequent need to develop the necessary governance mechanisms gave us the unprecedented opportunity to create a new model from scratch. This allowed us to observe the characteristics of this new model instead of having to wait for traditional models to evolve naturally.

Internet governance was built on new paradigms and resulted in mechanisms based on the search for consensus, transparency/accountability and equal participation of all stakeholders.

It is a model that in many ways is at odds with traditional models.

Never before has it been so clear that wisdom and experience are highly distributed. While this became very visible with regard to the Internet, that concept applies to all areas of human activity.

Governance models will surely continue evolving in that direction, and in the future we will see models in which power will be increasingly distributed.

This is a world where things that were once considered set in stone are no longer valid, one where paradigms are being destroyed. In all probability, we do not need to find new paradigms but instead accept that there will be no more paradigms.

Organizations based on participatory models will be best positioned to build strategies that will allow them to respond successfully to the changing environment. Stability lies in the distribution of power among the various stakeholders.

This is why any solution to address current and future challenges should be built on the innovative governance instruments we have created and avoid the temptation of going back to previous models. Openness, transparency, the search for consensus and equal participation of the various actors are governance features that should be protected and maintained.

So far, what best represents these concepts, is the Internet Governance Forum, the IGF. However, as already noted, the world continues to change constantly and rapidly, and the IGF must adapt to this reality.

The IGF was conceived as a place to hold central multistakeholder discussions on almost every Internet governance topic. Today, however, these topics crosscut every policy issue, so they cannot be discussed in a single place and must instead be present at every forum, on almost ay issue. We need mechanisms with different level of formality, focus and type of stakeholders involved.

The report prepared by the High-Level Panel on Digital Cooperation includes three possible cooperation models. In fact, it is not a question of adopting one or the other; what we need is a bit of each: an improved IGF plus additional, more flexible collective construction mechanisms.

The role of the IGF should evolve to a forum that synthesizes the different points of view, documents differences and coincidences, and that, without forcing agreements, produces consensus where possible. These consensuses should be in the form of principles, general guidelines and/or directions in which to advance. Other global, regional and national forums will then take these general agreements and design ways to implement them.

The IGF must obviously evolve to fulfill this new mission. The IGF has already made much progress and must continue to improve. Addressing these specific practical aspects is not the purpose of this article, but broadly speaking some of these improvements should include enhancing intersessional work, an agenda that combines a space for general reflection with the increasingly focused discussions on the most cyclical topics, and instances for high-level validation of the Forum's conclusions.

In 2014, Netmundial allowed us to experiment with practices that produced good results. It was the first time that a multistakeholder process with no formal negotiation mechanism managed to produce outcomes. Those practices should be recovered.

I envision an IGF that works throughout the year, that advance the production of conclusions, that interacts with other forums following up on global discussions on the most relevant topics; an IGF that holds its annual meeting having first produced solid foundations that will allow us to identify disagreements and also to achieve high-level consensus that can be validated with a NetMundial-type high level meeting to be held on the final day of the Forum.

Those conclusions should be brought later to other forums so that they can continue the work in cycles, nourishing others and producing local policies that will once again serve as inputs for regional and global discussions.

The world is in our hands. Driven by the challenges posed by constant change, the future presents us with incredible opportunities that we must seize.

Does the Internet run a risk of becoming a victim of its own success?

Yrjö Länsipuro

In a few decades, the Internet grew from an obscure byproduct of military research into a worldwide network of networks, connecting more than half of mankind, and becoming the operating system of most human activities. Unfettered by regulation and based on voluntary cooperation among autonomous networks, it defied the established world communications order and threw a gauntlet at governments, 'weary giants of flesh and steel', from whom John Perry Barlow proclaimed the independence of cyberspace in 1996. At that time, the Internet was a community of 150 million early adopters, its expansion was only starting and its future seemed bright.

Today, about four billion people are not only using the Internet but critically dependent on it. It used to be 'nice to have', now it is a 'must have', because the tools it replaced are no more. Climbing the ladder of technology, we destroyed the rungs we left below us. Regrettably, as users we thought of ourselves as customers but realized we were often just raw material for advertisers and cannon fodder for political campaigns. Liberated from the tutelage of media gatekeepers, we found ourselves confronted with hate speech, disinformation and alternative realities. No wonder that on the verge of new technological leaps into artificial intelligence, the fifth generation of mobile connections and the Internet of Things, our discussions about the future focus more on looming threats than on new exciting opportunities.

Not quite a quarter of a century after the independence manifesto of cyberspace, it is indeed time for a Declaration of Digital Interdependence, issued by the UN Secretary-General's High-Level Panel on Digital Cooperation. The Internet and it's users are not marooned in some separate space. Online and offline worlds are inextricably intertwined. There is a need for a holistic view.

The report of the panel is an authoritative effort to update some of the outcomes of the World Summit on Information Society (2003 and 2005) to cope with current realities. Back then, WSIS was still seen by many as just one in the series of UN sectoral summits. It is now understood that as a critical resource, the Internet is underpinning most other critical resources for the world, and its governance must be seen in that light.

Multi-stakeholder approach has been a household word in internet governance discussions since the WSIS, but the concept has not been widely understood, let alone endorsed, in the wider world. In that respect, the

panel's unequivocal support of multistakeholderism as an indispensable complement to multilateralism is very important. But this makes it even more urgent to develop practical modalities of cooperation between governments, international organizations, private sector, technical and academic communities and civil society. All stakeholders should contribute to turning the multistakeholder approach from a mantra into a method. It will be the language of the future, but it still lacks a grammar.

In addition to principles and norms, the panel also presents three alternative paths for mechanisms for global digital cooperation. At the WSIS and in its follow-up discussions, the m-word tended to raise red flags lest somebody somewhere was conspiring to "take over" the internet. Maybe we are already beyond that. Of the three options, at least at first sight, the safest bet seems to be to give more teeth to the Internet Governance Forum, which has a proven track record since 2006 and has spawned dozens of regional and national internet forums around the world.

Recognizing the interdependence among all stakeholders, we may, in the end, reach the very goal that, in its flowery language, the 1996 manifesto described as a "civilization of the Mind in Cyberspace". In the words of the co-chairs of the 2019 UN panel: "No one knows how technology will evolve, but we know that our path forward must be built through cooperation and illuminated by shared human values".

ANNEX

From the WSIS Tunis Agenda (2005) to the UN High Level Panel on Digital Cooperation (2019)

Wolfgang Kleinwächter

Since more than two decades "Internet Governance" is a controversial issue on the global political agenda. During the first phase of the UN World Summit on the Information Society (2002 – 2003) the controversy circled around the question, whether the Internet should be managed by governments (China) or by the private sector (USA). The UN Working Group on Internet Governance (WGIG), which was established by UN Secretary General Kofi Annan in 2004 with the mandate, to bridge this conflict, rejected the concept of "single stakeholder leadership". It concluded that the Internet is too big to be managed by one stakeholder-group or one organisation alone and proposed a "multistakeholder approach".

The WGIG-Definition

The working definition, which was adopted by the Heads of States in the WSIS Tunis Agenda in November 2005, states that "Internet Governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[179]

This WGIG-definition was a "broad definition" which included both the management of the so-called critical (technical) Internet resources as well as the management of the Internet related public policy issues.

The WGIG-definition was reaffirmed ten years later by the High Level Meeting of the 70th UN General Assembly on the overall review of the implementation of the WSIS outcomes which also stated in UN-Resolution 70/125 (2015): "We reaffirm, moreover, the value and principles of multi-stakeholder cooperation and engagement that have characterized the World Summit on the Information Society process since its inception, recognizing that effective participation, partnership and cooperation of Governments, the private sector, civil society, international organizations, the technical and academic communities and all other relevant stakeholders, within their respective roles and responsibilities, especially with balanced representation from developing countries, has been and continues to be vital in developing the information society."[180]

At the time of the WSIS in 2005, Internet Governance was seen primarily as a technical issue with political implications. 15 years later the Internet has penetrated all spheres of policy, economy and society. Today Internet Governance is a political issue with a technical component.

Some people have compared the Internet Governance Ecosystem with a "virtual rainforest", where an endless and growing diversity of networks, services, applications, regimes and other properties co-exist in a mutual interdependent mechanism of communication, coordination, and collaboration. Many players with very different legal status operate on many different layers — on local, national, regional and international levels — driven by technical innovation, user needs, market opportunities and political interests. This has led to a broad variety of different regulatory, co-regulatory or self-regulatory regimes which co-exist, complement or conflict each other. The system as a whole is decentralized, diversified and has no central authority. However, within the various subsystems there is an incredible broad variety of different sub-mechanisms which range from hierarchical structures under single or inter-governmental control to non-hierarchical networks based on self-regulatory mechanisms by non-governmental groups with a wide range of co-regulatory arrangements in between where affected and concerned stakeholders from governments, private sector, civil society and technical community are working hand in hand.

There is no "one size fits all"

There is no "one size fits all" solution. The specific form of each sub-system has to be designed according to the very specific needs and nature of the individual issue. In such a mechanism, traditional national legislation and intergovernmental agreements continue to play a role but have to be embedded into the broader multistakeholder environment while new emerging mechanisms have to take note and recognize existing frameworks and regulations on various levels. The "do-not-harm" principle becomes more important than ever. It means that whatever a governmental or non-governmental player will do on the Internet has to take into consideration its direct or indirect consequences for not involved third parties as well as the unintended side-effects for the system as a whole.

Such a competitive coexistence of rather different regimes and mechanisms creates opportunities but has also risks. There are incredible opportunities for new mechanisms, platforms, and services to bring more dynamic into political strategies, social actions and market developments. This competitive coexistence can stimulate innovation, promote job creation, enlarge all kinds of cultural activities and broaden the use of individual freedoms by the public at large both in developed and developing nations. But there is also a risk that differences between regimes and systems create controversies and produce heavy conflicts which include the threat to turn down innovation, hamper sustainable development, militarize cyberspace, reduce individual freedoms and pollute the Internet Governance Eco-System in a way that parts of it will be damaged or destroyed.

However, for many years the global Internet discussions were overshadowed by the question whether Internet related issues could be better solved by multilateral treaties or by multistakeholder arrangements. "Multistakeholderism" is not yet defined. There is no single "multistakeholder model". The reference in the WGIG-definition to the "respective roles" of stakeholders give policy makers a certain flexibility in finding individual solutions for concrete issues. Nevertheless, the multistakholder approach got step by step universal acceptance on the highest political level .

G7, G20 & BRICS

Already in 2011 the G8 summit meeting In Deauville (which included the Russian president Dimitrij Medwedew) made a clear statement in support of the multistakeholder approach. The "G8 Declaration: Renewed Commitment for Freedom and Democracy" stated in Chapter II.17ff. "As we support the multi-stakeholder model of Internet governance, we call upon all stakeholders to contribute to enhanced cooperation within and between all international fora dealing with the governance of the Internet.... The security of networks and services on the Internet is a multi-stakeholder issue. It requires coordination between governments, regional and international organizations, the private sector, civil society und the technical community." The G8 recognized also the role of governments "informed by a full range of stakeholders, in helping to develop norms of behaviour and common approaches in the use of cyberspace."[181]

Five years later, in 2016, the G20 summit meeting in the Chinese city of Hangzhou reiterated the commitment to the multistakeholder approach. The "G20 Digital Economy Development and Cooperation Initiative" stated in Chapter II, 5b: "Internet governance should continue to follow the provisions set forth in outcomes of World Summit on the Information Society (WSIS). In particular, we affirm our commitment to a multistakeholder approach to Internet governance, which includes full and active participation by governments, private sector, civil society, the technical community, and

international organizations, in their respective roles and responsibilities. We support multistakeholder processes and initiatives which are inclusive, transparent and accountable to all stakeholders in achieving the digitally connected world."[182]

Also the five leaders of the BRICS countries committed themselves to the multistakeholder approach. The "BRICS Leaders Xiamen Declaration" (2017) stated in paragraph 57: "We believe that all states should participate on an equal footing in the evolution and functioning of the Internet and its governance, bearing in mind the need to involve relevant stakeholders in their respective roles and responsibilities."[183]

As said above, there is no single multistakehoder model. This flexible language of the WGIG-definition has helped to develop a broad variety of different "multistakeholder practices" in dealing with Internet related technical and public policy issues.

It was the "Global Multistakeholder Meeting on the Future of Internet Governance", also known as NETmundial, in Sao Paulo, April 2016 which defined a number of characteristics for a multistakeholder process. The Sao Paulo Statement said "that Internet governance should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users. The respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the issue under discussion." And it referred to characteristics as openness, transparency, accountability, inclusiveness, equitability, decentralization, collaboration, meaningful participation, agility, access and low entry barriers.[184]

Multilateralism & Multistakeholderism

Based on those characteristics, we have now a broad variety of different approaches which reach form sharing policy development and decision making on equal footing among all stakeholders until a more differentiated system of open consultations between state and non-state actors.

In Internet related technical issues – as the development of Internet protocols, the management of the domain name system and IP addresses as well as the operation of the root server system – it is mainly the technical community and the private sector, which take the lead in policy development and decision making. However, governments are involved, as in ICANN via the Governmental Advisory Committee (GAC).

In Internet related public policy issues – as cybersecurity, digital trade or human rights – it is mainly the governments which negotiate treaties. But intergovernmental organisations of the UN system have broaden their consultations with non-state actors from the private sector, civil society and the technical community. One recent example is UN resolution 73/27 (2018), which established an Open Ended Working Group (OEWG) on cybersecurity under the 1st Committee of the UNGA. The resolution included a paragraph which provides the possibility of holding intersessional consultative meetings with industry, non-governmental organizations and academia. Also the UN Human Rights Council has regular consultations with non-state actors. Another example are the two UNCSTD Working Groups on Enhanced Cooperation (WGEC/2013 – 2018) where state and non-state actors participated on equal footing.[185] The UNCSTD is the intergovernmental UN body which oversees the implementation of the WSIS decisions.

A number of other intergovernmental organisations - as the OECD – have in recent years introduced subsidiary bodies where representatives from business, civil society and the technical community have an opportunity to contribute to Internet related policy development.

Various expert groups , as the Global Commission on Internet Governance (2015 – 2016) and the Global Commission on Stability in Cyberspace (2017b – 2019) have further elaborated the concept of a multistakeholder approach to Internet Governance.

Furthermore, a number of private sector companies – as Microsoft and Siemens – have started their own political initiatives and have produced documents like the "Tech Accord" (April 2018) and the Charter of Trust (February 2018). The Paris Peace Forum, which remembered the 100th anniversary of the end of World War One in November 2018, produced with the "Paris Call for Trust and Security in Cyberspace" a new type of document which includes commitments both for state and non-state actors. The Paris Call, which was signed by nearly more than 50 governments and hundreds of non-state actors, including big Internet corporations, defined nine norms fort the good behaviour of state and non.-state actors in cyberspace, including the norm to protect "the general availability or integrity of the public core of the Internet." [186]

The UN High Level Panel on Digital Cooperation discussed at length the relationship between "Multilateralism" and "Multistakeholderism" and concluded in its final report in June 2019 that "reinvigorating multilateralism alone will not be sufficient. Effective digital cooperation requires that multilateralism be complemented by multistakeholderism – cooperation that

involves governments and a diverse spectrum of other stakeholders such as civil society, technologists, academics, and the private sector (ranging from small enterprises to large technology companies).” And it continued: “While only governments can make laws, all these stakeholders are needed to contribute to effective governance by cooperating to assess the complex and dynamic impacts of digital technologies and developing shared norms, standards and practices. We need to bring far more diverse voices to the table, particularly from developing countries and traditionally marginalised populations. Important digital issues have often been decided behind closed doors, without the involvement of those who are most affected by the decisions.” [187]

Source

[179] Tunis Agenda for the Information Society, November 18, 2005, see: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
[180] UN Resolution 70/125, December 15, 2015, Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society, see: https://publicadministration.un.org/wsis10/
[181] G8 Declaration: Renewed Commitment for Freedom and Democracy“, Deauville, May 27, 2011, see: http://www.g7.utoronto.ca/summit/2011deauville/2011-declaration-en.html
[182] G20 Digital Economy Development and Cooperation Initiative, Hangzhou, September 5, 2016, see: http://www.g7.utoronto.ca/g20/2016/160905-digital.html
[183] BRICS Leaders Xiamen Declaration, September 4, 2017, see: http://www.brics.utoronto.ca/docs/170904-xiamen.html
[184] NetMundial Multistakeholder Statement, Sao Paulo, April 23, 2014, see: http://netmundial.br/netmundial-multistakeholder-statement/
[185] UNCSTD Working Group on Enhanced Cooperation (WGEC), see: https://unctad.org/en/Pages/CSTD/WGEC-2016-to-2018.aspx
[186] Paris Call for Trust and Security in Cyberspace, Paris, November 11, 2018: https://www.diplomacy.edu/blog/table-paris-call-trust-and-security-cyberspace
[187] The Age of Digital Interdependence, Final Report oft he UN High Level Panel on Digital Cooperation, New York, June, 10, 2019, see: https://digitalcooperation.org/

Internet Governance Documents (Excerpts)

1. WSIS Tunis Agenda on the Information Society (Tunis, November 18, 2005)

[...] 29. We reaffirm the principles enunciated in the Geneva phase of the WSIS, in December 2003, that the Internet has evolved into a global facility available to the public and its governance should constitute a core issue of the Information Society agenda. The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism.

[...] 31. We recognize that Internet governance, carried out according to the Geneva principles, is an essential element for a people-centred, inclusive, development-oriented and non-discriminatory Information Society. Furthermore, we commit ourselves to the stability and security of the Internet as a global facility and to ensuring the requisite legitimacy of its governance, based on the full participation of all stakeholders, from both developed and developing countries, within their respective roles and responsibilities.

[...] 34. A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.

35. We reaffirm that the management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect it is recognized that: Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues. The private sector has had, and should continue to have, an important role in the development of the Internet, both in the technical and economic fields. Civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role. Intergovernmental organizations have had, and should continue to have, a facilitating role in the coordination of Internet-related public policy issues. International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.

36. We recognize the valuable contribution by the academic and technical communities within those stakeholder groups mentioned in paragraph 35 to the evolution, functioning and development of the Internet.

37. We seek to improve the coordination of the activities of international and intergovernmental organizations and other institutions concerned with Internet governance and the exchange of information among themselves. A multi-stakeholder approach should be adopted, as far as possible, at all levels.

[...] 39. We seek to build confidence and security in the use of ICTs by strengthening the trust framework. We reaffirm the necessity to further promote, develop and implement in cooperation with all stakeholders a global culture of cybersecurity, as outlined in UNGA Resolution 57/239 and other relevant regional frameworks. This culture requires national action and increased international cooperation to strengthen security while enhancing the protection of personal information, privacy and data. Continued development of the culture of cybersecurity should enhance access and trade and must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.

[...] 42. We reaffirm our commitment to the freedom to seek, receive, impart and use information, in particular, for the creation, accumulation and dissemination of knowledge. We affirm that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.

[...] 46. We call upon all stakeholders to ensure respect for privacy and the protection of personal information and data, whether via adoption of legislation, the implementation of collaborative frameworks, best practices and self-regulatory and technological measures by business and users. We encourage all stakeholders, in particular governments, to reaffirm the right of individuals to access information according to the Geneva Declaration of Principles and other mutually agreed relevant international instruments, and to coordinate internationally as appropriate.

[...] 49. We reaffirm our commitment to turning the digital divide into digital opportunity, and we commit to ensuring harmonious and equitable development for all. We commit to foster and provide guidance on development areas in the broader Internet governance arrangements, and to include, amongst other issues, international interconnection costs, capacity building and technology/know-how transfer. We encourage the realization of multilingualism in the Internet development environment, and we support

the development of software that renders itself easily to localization, and enables users to choose appropriate solutions from different software models including open-source, free and proprietary software.

51. We encourage governments and other stakeholders, through partnerships where appropriate, to promote ICT education and training in developing countries, by establishing national strategies for ICT integration in education and workforce development and dedicating appropriate resources. Furthermore, international cooperation would be extended, on a voluntary basis, for capacity building in areas relevant to Internet governance. This may include, in particular, building centres of expertise and other institutions to facilitate know-how transfer and exchange of best practices, in order to enhance the participation of developing countries and all stakeholders in Internet governance mechanisms.

52. In order to ensure effective participation in global Internet governance, we urge international organizations, including intergovernmental organizations, where relevant, to ensure that all stakeholders, particularly from developing countries, have the opportunity to participate in policy decision-making relating to Internet governance, and to promote and facilitate such participation.

[...] 55. We recognize that the existing arrangements for Internet governance have worked effectively to make the Internet the highly robust, dynamic and geographically diverse medium that it is today, with the private sector taking the lead in day-to-day operations, and with innovation and value creation at the edges.

[...] 58. We recognize that Internet governance includes more than Internet naming and addressing. It also includes other significant public policy issues such as, inter alia, critical Internet resources, the security and safety of the Internet, and developmental aspects and issues pertaining to the use of the Internet.

59. We recognize that Internet governance includes social, economic and technical issues including affordability, reliability and quality of service.

60. We further recognize that there are many cross-cutting international public policy issues that require attention and are not adequately addressed by the current mechanisms.

[...] 63. Countries should not be involved in decisions regarding another country's country-code Top-Level Domain (ccTLD). Their legitimate interests, as expressed and defined by each country, in diverse ways, regarding decisions affecting their ccTLDs, need to be respected, upheld and addressed via a flexible and improved framework and mechanisms.

64. We recognize the need for further development of, and strengthened cooperation among, stakeholders for public policies for generic Top-Level Domain names (gTLDs).

65. We underline the need to maximize the participation of developing countries in decisions regarding Internet governance, which should reflect their interests, as well as in development and capacity building.

[...] 68. We recognize that all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the Internet. We also recognize the need for development of public policy by governments in consultation with all stakeholders.

69. We further recognize the need for enhanced cooperation in the future, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters, that do not impact on international public policy issues.

70. Using relevant international organizations, such cooperation should include the development of globally-applicable principles on public policy issues associated with the coordination and management of critical Internet resources. In this regard, we call upon the organizations responsible for essential tasks associated with the Internet to contribute to creating an environment that facilitates this development of public policy principles.

71. The process towards enhanced cooperation, to be started by the UN Secretary-General, involving all relevant organizations by the end of the first quarter of 2006, will involve all stakeholders in their respective roles, will proceed as quickly as possible consistent with legal process, and will be responsive to innovation. Relevant organizations should commence a process towards enhanced cooperation involving all stakeholders, proceeding as quickly as possible and responsive to innovation. The same relevant organizations shall be requested to provide annual performance reports.

72. We ask the UN Secretary-General, in an open and inclusive process, to convene, by the second quarter of 2006, a meeting of the new forum for multi-stakeholder policy dialogue – called the Internet Governance Forum (IGF). The mandate of the Forum is to:

1. Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.
2. Facilitate discourse between bodies dealing with different cross-cutting international public policies regarding the Internet and discuss issues that do not fall within the scope of any existing body.
3. Interface with appropriate intergovernmental organizations and other institutions on matters under their purview.
4. Facilitate the exchange of information and best practices, and in this regard make full use of the expertise of the academic, scientific and technical communities.
5. Advise all stakeholders in proposing ways and means to accelerate the availability and affordability of the Internet in the developing world.
6. Strengthen and enhance the engagement of stakeholders in existing and/or future Internet governance mechanisms, particularly those from developing countries.
7. Identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations.
8. Contribute to capacity building for Internet governance in developing countries, drawing fully on local sources of knowledge and expertise.
9. Promote and assess, on an ongoing basis, the embodiment of WSIS principles in Internet governance processes.
10. Discuss, inter alia, issues relating to critical Internet resources.
11. Help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users.
12. Publish its proceedings.

73. The Internet Governance Forum, in its working and function, will be multilateral, multi-stakeholder, democratic and transparent.

2. RECOMMENDATION OF THE OECD COUNCIL ON PRINCIPLES FOR INTERNET POLICY MAKING (Paris, December 13, 2011)

THE COUNCIL...RECOMMENDS that, in developing or revising their policies for the Internet Economy, Members, in co-operation with all stakeholders, take account of the following high level principles as explained in the Communiqué:

1. Promote and protect the global free flow of information;
2. Promote the open, distributed and interconnected nature of the Internet;
3. Promote investment and competition in high speed networks and services;
4. Promote and enable the cross-border delivery of services;
5. Encourage multi-stakeholder co-operation in policy development processes;
6. Foster voluntarily developed codes of conduct;
7. Develop capacities to bring publicly available, reliable data into the policy-making process;
8. Ensure transparency, fair process, and accountability;
9. Strengthen consistency and effectiveness in privacy protection at a global level;
10. Maximise individual empowerment;
11. Promote creativity and innovation;
12. Limit Internet intermediary liability;
13. Encourage co-operation to promote Internet security;
14. Give appropriate priority to enforcement efforts.

3. Declaration by the Committee of Minister of the Council of Europe on Internet Governance Principles (Strasbourg, September 21, 2011)

In order to ensure a sustainable, people-centred and rights-based approach to the Internet, it is necessary to affirm the principles of Internet governance which acknowledge human rights and fundamental freedoms, democracy and the rule of law, as well as the basic tenets of Internet communities as they have been developed in the processes mentioned above. As a contribution to this ongoing, inclusive, collaborative and open process, the Committee of Ministers of the Council of Europe: a. affirms the principles set out below, which build on Internet governance principles progressively developed by stakeholders and Internet communities; b. declares its firm commitment to these principles and underlines that they should be upheld by all member states in the context of developing national and international Internet-related policies; c. encourages other stakeholders to embrace them in the exercise of their own responsibilities.

1. Human rights, democracy and the rule of law

Internet governance arrangements must ensure the protection of all fundamental rights and freedoms and affirm their universality, indivisibility, interdependence and interrelation in accordance with international human rights law. They must also ensure full respect for democracy and the rule of law and should promote sustainable development. All public and private actors should recognise and uphold human rights and fundamental freedoms in their operations and activities, as well as in the design of new technologies, services and applications. They should be aware of developments leading to the enhancement of, as well as threats to, fundamental rights and freedoms, and fully participate in efforts aimed at recognising newly emerging rights.

2. Multi-stakeholder governance

The development and implementation of Internet governance arrangements should ensure, in an open, transparent and accountable manner, the full participation of governments, the private sector, civil society, the technical community and users, taking into account their specific roles and responsibilities. The development of international Internet-related public policies and Internet governance arrangements should enable full and equal participation of all stakeholders from all countries.

3. Responsibilities of states

States have rights and responsibilities with regard to international Internet-related public policy issues. In the exercise of their sovereignty rights, states should, subject to international law, refrain from any action that would directly or indirectly harm persons or entities outside of their territorial jurisdiction. Furthermore, any national decision or action amounting to a restriction of fundamental rights should comply with international obligations and in particular be based on law, be necessary in a democratic society and fully respect the principles of proportionality and the right of independent appeal, surrounded by appropriate legal and due process safeguards.

4. Empowerment of Internet users

Users should be fully empowered to exercise their fundamental rights and freedoms, make informed decisions and participate in Internet governance arrangements, in particular in governance mechanisms and in the development of Internet-related public policy, in full confidence and freedom.

5. Universality of the Internet

Internet-related policies should recognise the global nature of the Internet and the objective of universal access. They should not adversely affect the unimpeded flow of transboundary Internet traffic.

6. Integrity of the Internet

The security, stability, robustness and resilience of the Internet as well as its ability to evolve should be the key objectives of Internet governance. In order to preserve the integrity and ongoing functioning of the Internet infrastructure, as well as users' trust and reliance on the Internet, it is necessary to promote national and international multi-stakeholder co-operation.

7. Decentralised management

The decentralised nature of the responsibility for the day-to-day management of the Internet should be preserved. The bodies responsible for the technical and management aspects of the Internet, as well as the private sector should retain their leading role in technical and operational matters while ensuring transparency and being accountable to the global community for those actions which have an impact on public policy.

8. Architectural principles

The open standards and the interoperability of the Internet as well as its end-to-end nature should be preserved. These principles should guide all stakeholders in their decisions related to Internet governance. There should be no unreasonable barriers to entry for new users or legitimate uses of the Internet, or unnecessary burdens which could affect the potential for innovation in respect of technologies and services.

9. Open network

Users should have the greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice. Traffic management measures which have an impact on the enjoyment of fundamental rights and freedoms, in particular the right to freedom of expression and to impart and receive information regardless of frontiers, as well as the right to respect for private life, must meet the requirements of international law on the protection of freedom of expression and access to information, and the right to respect for private life.

10. Cultural and linguistic diversity

Preserving cultural and linguistic diversity and fostering the development of local content, regardless of language or script, should be key objectives of Internet-related policy and international co-operation, as well as in the development of new technologies.

4. NetMundial Multistakeholder Statement (Sao Paulo, April 24, 2014)

This is the non-binding outcome of a bottom-up, open, and participatory process involving thousands of people from governments, private sector, civil society,technical community, and academia from around the world. The NETmundial conference was the first of its kind. It hopefully contributes to the evolution of the Internet governance ecosystem.

Internet governance principles

NETmundial identified a set of common principles and important values that contribute for an inclusive, multistakeholder, effective, legitimate, and evolving Internet governance framework and recognized that the Internet is a global resource which should be managed in the public interest.

Human rights and shared values

Human rights are universal as reflected in the Universal Declaration of Human Rights and that should underpin Internet governance principles. Rights that people have offline must also be protected online, in accordance with international human rights legal obligations, including the International Covenants on Civil and Political Rights and Economic, Social and Cultural Rights, and the Convention on the Rights of Persons with Disabilities. Those rights include, but are not limited to:

Freedom of expression: Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Freedom of association: Everyone has the right to peaceful assembly and association online, including through social networks and platforms.

Privacy: The right to privacy must be protected. This includes not being subject to arbitrary or unlawful surveillance, collection, treatment and use of personal data. The right to the protection of the law against such interference should be ensured.

Procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including mass surveillance, interception and collection, should be reviewed, with a view to upholding the right to privacy by ensuring the full and effective implementation of all obligations under international human rights law.

Accessibility: persons with disabilities should enjoy full access to online resources Promote the design, development, production and distribution of accessible information, technologies and systems on the internet.

Freedom of information and access to information: Everyone should have the right to access, share, create and distribute information on the Internet, consistent with the rights of authors and creators as established in law.

Development: all people have a right to development and the Internet has a vital role to play in helping to achieve the full realization of internationally agreed sustainable development goals. It is a vital tool for giving people living in poverty the means to participate in development processes.

Protection of intermediaries

Intermediary liability limitations should be implemented in a way that respects and promotes economic growth, innovation, creativity and free flow of information. In this regard, cooperation among all stakeholders should be encouraged to address and deter illegal activity, consistent with fair process.

Culture and linguistic diversity

Internet governance must respect, protect and promote cultural and linguistic diversity in all its forms.

Unified and unfragmented space

Internet should continue to be a globally coherent, interconnected, stable, unfragmented, scalable and accessible network-of-networks, based on a common set of unique identifiers and that allows data packets/information to flow freely endto-end regardless of the lawful content.

Security, stability and resilience of the internet

Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance. As a universal global resource, the Internet should be a secure, stable, resilient, reliable and trustworthy network. Effectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation among different stakeholders.

Open and distributed architecture

The Internet should be preserved as a fertile and innovative environment based on an open system architecture, with voluntary collaboration, collective stewardship and participation, and upholds the end-to-end nature of the open Internet, and seeks for technical experts to resolve technical issues in the appropriate venue in a manner consistent with this open, collaborative approach.

Enabling environment for sustainable innovation and creativity

The ability to innovate and create has been at the heart of the remarkable growth of the Internet and it has brought great value to the global society. For the preservation of its dynamism, Internet governance must continue to allow permissionless innovation through an enabling Internet environment, consistent with other principles in this document. Enterprise and investment in infrastructure are essential components of an enabling environment.

Internet governance process principles

Multistakeholder: Internet governance should be built on democratic, multi-stakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users. The respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the issue under discussion.

Open, participative, consensus driven governance: The development of international Internet-related public policies and Internet governance arrangements should enable the full and balanced participation of all stake-holders from around the globe, and made by consensus, to the extent possible.

Transparent: Decisions made must be easy to understand, processes must be clearly documented and follow agreed procedures, and procedures must be developed and agreed upon through multistakeholder processes.

Accountable: Mechanisms for independent checks and balances as well as for review and redress should exist. Governments have primary, legal and political accountability for the protection of human rights

Inclusive and equitable: Internet governance institutions and processes should be inclusive and open to all interested stakeholders. Processes,

including decision making, should be bottom-up, enabling the full involvement of all stakeholders, in a way that does not disadvantage any category of stakeholder.

Distributed: Internet Governance should be carried out through a distributed, decentralized and multistakeholder ecosystem.

Collaborative: Internet governance should be based on and encourage collaborative and cooperative approaches that reflect the inputs and interests of stakeholders.

Enabling meaningful participation: Anyone affected by an Internet governance process should be able to participate in that process. Particularly, Internet governance institutions and processes should support capacity building for newcomers, especially stakeholders from developing countries and underrepresented groups.

Access and low barriers: Internet governance should promote universal, equal opportunity, affordable and high quality Internet access so it can be an effective tool for enabling human development and social inclusion. There should be no unreasonable or discriminatory barriers to entry for new users. Public access is a powerful tool for providing access to the Internet.

Agility: Policies for access to Internet services should be future oriented and technology neutral, so that they are able to accommodate rapidly developing technologies and different types of use.

Open standards

Internet governance should promote open standards, informed by individual and collective expertise and decisions made by rough consensus, that allow for a global, interoperable, resilient, stable, decentralized, secure, and interconnected network, available to all. Standards must be consistent with human rights and allow development and innovation.

5. Report of the UN Group of Governmental Experts on Development in the field of Information and Telecommunications in the Context of Information Security (New York, July 22, 2015)

Taking into account existing and emerging threats, risks and vulnerabilities, and building upon the assessments and recommendations contained in the 2010 and 2013 reports of the previous Groups, the present Group offers the following recommendations for consideration by States for voluntary, non-

binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment:

(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

(d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

(f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

(h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

6. Tech Accord (Redmond, April 17, 2018)

The online world has become a cornerstone of global society, important to virtually every aspect of our public infrastructure and private lives. As we look to the future, new online technologies will do even more to help address important societal challenges, from improving education and healthcare to advancing agriculture, business growth, job creation, and addressing environmental sustainability. Recent events, however, have put online security at risk. Malicious actors, with motives ranging from criminal to geopolitical, have inflicted economic harm, put human lives at risk, and undermined the trust that is essential to an open, free, and secure internet. Attacks on the availability, confidentiality, and integrity of data, products, services, and networks have demonstrated the need for constant vigilance, collective action, and a renewed commitment to cybersecurity.

Protecting our online environment is in everyone's interest. Therefore we – as enterprises that create and operate online technologies – promise to defend and advance its benefits for society. Moreover, we commit to act responsibly, to protect and empower our users and customers, and thereby to improve the security, stability, and resilience of cyberspace.

To this end, we are adopting this Accord and the principles below:

1. WE WILL PROTECT ALL OF OUR USERS AND CUSTOMERS EVERYWHERE.

- We will strive to protect all our users and customers from cyberattacks – whether an individual, organization or government – irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical.
- We will design, develop, and deliver products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability, and severity of vulnerabilities.

2. WE WILL OPPOSE CYBERATTACKS ON INNOCENT CITIZENS AND ENTERPRISES FROM ANYWHERE.

- We will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use.
- We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere.

3. WE WILL HELP EMPOWER USERS, CUSTOMERS AND DEVELOPERS TO STRENGTHEN CYBERSECURITY PROTECTION.

- We will provide our users, customers and the wider developer ecosystem with information and tools that enable them to understand current and future threats and protect themselves against them.
- We will support civil society, governments and international organizations in their efforts to advance security in cyberspace and to build cybersecurity capacity in developed and emerging economies alike.

4. WE WILL PARTNER WITH EACH OTHER AND WITH LIKEMINDED GROUPS TO ENHANCE CYBERSECURITY.

- We will work with each other and will establish formal and informal partnerships with industry, civil society, and security researchers, across proprietary and open source technologies to improve technical collaboration, coordinated vulnerability disclosure, and threat sharing, as well as to minimize the levels of malicious code being introduced into cyberspace.
- We will encourage global information sharing and civilian efforts to identify, prevent, detect, respond to, and recover from cyberattacks and ensure flexible responses to security of the wider global technology ecosystem.

To ensure a meaningful partnership is established through the implementation of the Tech Accord, we, the undersigned companies, will continue to define

collaborative activities we will undertake to further this Accord. We will also report publicly on our progress in achieving these goals.

7. Charter of Trust: For a Secure Digital World (Munich, February 19, 2018)

The digital world is changing everything. Artificial intelligence and big data analytics are revolutionizing our decision-making while billions of devices are being connected by the Internet of Things and interacting on an entirely new level and scale. As much as these advances are improving our lives and economies, the risk of exposure to malicious cyberattacks is also growing dramatically. Failure to protect the systems that control our homes, hospitals, factories, grids and virtually all of our infrastructure could have devastating consequences. Democratic and economic values need to be protected from cyber and hybrid threats.

Cybersecurity is and has to be more than a seatbelt or an airbag here; it's a factor that's crucial to the success of the digital economy. People and organizations need to trust that their digital technologies are safe and secure; otherwise, they won't embrace the digital transformation. Digitalization and cybersecurity must evolve hand-in-hand.

To keep pace with continuous advances in the market as well as threats from the criminal world, companies and governments must join forces and take decisive action. This means making every effort to protect the data and assets of both individuals and businesses, prevent damage to people, businesses, and infrastructures and build a reliable basis for trust in a connected and digital world.

In other words, it's a matter of building trust in cybersecurity, advancing it on all ist various levels and thereby paving the way for digitalization. And that's not something that any company can do all by itself. It has to be approached through a close collaboration of all the parties involved. In this document, the undersigned outline the key principles for a secure digital world – principles that they're actively pursuing in collaboration with civil society, government, business partners and customers. Cybersecurity is critical for everyone

1. Keep your hardware and antivirus software up to date. Be cautious when dealing with unknown apps. Internet-capable equipment should always be up to date. Install updates as soon as they become available. Don't install unknown apps.
2. Use different passwords and two-factor authentication for your accounts. Long, cryptic passwords incorporating numbers, symbols and both capital and small letters are more secure. Avoid simple sequences of numbers or characters, names in normal text, and complete words. Don't let others know your passwords, and don't write them down in places like note pads. Use two-factor authentication with additional identification, such as an SMS code.
3. Be able to recognize spam (fake email) and be cautious when dealing with attachments and links. Be mistrustful of emails with unrequested information or attachments, or messages from a known name accompanied by an unknown email address. Don't click on links embedded in emails from unfamiliar sources. You can use your mouse pointer to compare the pop-up text with the link without clicking it. Don't open executable files (.exe, .scr, .cpl, zip files) or Office documents that contain macros. Delete emails from services you don't use or that you don't normally receive email from, such as delivery services, banks, telephone providers and hotels. Ignore requests to install software from an unknown source
4. Don't accept every "friend" request on social media. Check to see if you know the person and whether the request is really from that person. If you're in doubt, ignore the request.
5. Provide access only to certain limited data and information. Don't release your personal data carelessly.

8. Paris Call for Trust and Security in Cyberspace (Paris, November 12, 2018)

Cyberspace now plays a crucial role in every aspect of our lives and it is the shared responsibility of a wide variety of actors, in their respective roles, to improve trust, security and stability in cyberspace.

We reaffirm our support to an open, secure, stable, accessible and peaceful cyberspace, which has become an integral component of life in all its social, economic, cultural and political aspects.

We also reaffirm that international law, including the United Nations Charter in its entirety, international humanitarian law and customary international law is applicable to the use of information and communication technologies (ICT) by States.

We reaffirm that the same rights that people have offline must also be protected online, and also reaffirm the applicability of international human rights law in cyberspace.

We reaffirm that international law, together with the voluntary norms of responsible State behavior during peacetime and associated confidence and capacity-building measures developed within the United Nations, is the foundation for international peace and security in cyberspace.

We condemn malicious cyber activities in peacetime, notably the ones threatening or resulting in significant, indiscriminate or systemic harm to individuals and critical infrastructure and welcome calls for their improved protection.

We also welcome efforts by States and non-state actors to provide support to victims of malicious use of ICTs on an impartial and independent basis, whenever it occurs, whether during or outside of armed conflict.

We recognize that the threat of cyber criminality requires more effort to improve the security of the products we use, to strengthen our defenses against criminals and to promote cooperation among all stakeholders, within and across national borders, and that the Budapest Convention on Cybercrime is a key tool in this regard.

We recognize the responsibilities of key private sector actors in improving trust, security and stability in cyberspace and encourage initiatives aimed at strengthening the security of digital processes, products and services.

We welcome collaboration among governments, the private sector and civil society to create new cybersecurity standards that enable infrastructures and organizations to improve cyber protections.

We recognize all actors can support a peaceful cyberspace by encouraging the responsible and coordinated disclosure of vulnerabilities.

We underline the need to enhance broad digital cooperation and increase capacity-building efforts by all actors and encourage initiatives that build user resilience and capabilities;

We recognize the necessity of a strengthened multistakeholder approach and of additional efforts to reduce risks to the stability of cyberspace and to build-up confidence, capacity and trust.

To that end, we affirm our willingness to work together, in the existing fora and through the relevant organizations, institutions, mechanisms and processes to assist one another and implement cooperative measures, notably in order to:

– Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure;

– Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet;

– Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities;

– Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector;

– Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm;

– Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain;

– Support efforts to strengthen an advanced cyber hygiene for all actors;

– Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors ;

– Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.

In order to follow-up on the progress made to advance these issues in the appropriate existing fora and processes, we agree on reconvening at the Paris Peace Forum in 2019 and at the Internet Governance Forum in Berlin in 2019.

9. Final Report High Level UN Panel on Digital Cooperation (New York, June 10, 2019)

Recommendations:

1. An inclusive digital economy and society

1A: We recommend that by 2030, every adult should have affordable access to digital networks, as well as digitally-enabled financial and health services, as a means to make a substantial contribution to achieving the SDGs. Provision of these services should guard against abuse by building on emerging principles and best practices, one example of which is providing the ability to opt in and opt out, and by encouraging informed public discourse.

1B: We recommend that a broad, multi-stakeholder alliance, involving the UN, create a platform for sharing digital public goods, engaging talent and pooling data sets, in a manner that respects privacy, in areas related to attaining the SDGs.

1C: We call on the private sector, civil society, national governments, multilateral banks and the UN to adopt specific policies to support full digital inclusion and digital equality for women and traditionally marginalised groups. International organisations such as the World Bank and the UN should strengthen research and promote action on barriers women and marginalised groups face to digital inclusion and digital equality.

1D: We believe that a set of metrics for digital inclusiveness should be urgently agreed, measured worldwide and detailed with sex disaggregated data in the annual reports of institutions such as the UN, the International Monetary Fund, the World Bank, other multilateral development banks and the OECD. From this, strategies and plans of action could be developed.

2. Human and institutional capacity

2: We recommend the establishment of regional and global digital help desks to help governments, civil society and the private sector to understand digital issues and develop capacity to steer cooperation related to social and economic impacts of digital technologies.

3. Human rights and human agency

3A: Given that human rights apply fully in the digital world, we urge the UN Secretary-General to institute an agencies-wide review of how existing international human rights accords and standards apply to new and emerging digital technologies. Civil society, governments, the private sector and the public should be invited to submit their views on how to apply existing human rights instruments in the digital age in a proactive and transparent process.

3B: In the face of growing threats to human rights and safety, including those of children, we call on social media enterprises to work with governments, international and local civil society organisations and human rights experts around the world to fully understand and respond to concerns about existing or potential human rights violations.

3C: We believe that autonomous intelligent systems should be designed in ways that enable their decisions to be explained and humans to be accountable for their use. Audits and certification schemes should monitor compliance of artificial intelligence (AI) systems with engineering and ethical standards, which should be developed using multi-stakeholder and multilateral approaches. Life and death decisions should not be delegated to machines. We call for enhanced digital cooperation with multiple stakeholders to think through the design and application of these standards and principles such as transparency and non-bias in autonomous intelligent systems in different social settings.

4. Trust, security and stability

4: We recommend the development of a Global Commitment on Digital Trust and Security to shape a shared vision, identify attributes of digital stability, elucidate and strengthen the implementation of norms for responsible uses of technology, and propose priorities for action.

5. Global digital cooperation

5A: We recommend that, as a matter of urgency, the UN Secretary-General facilitate an agile and open consultation process to develop updated mechanisms for global digital cooperation, with the options discussed in Chapter 4 as a starting point. We suggest an initial goal of marking the UN's 75th anniversary in 2020 with a "Global Commitment for Digital Cooperation" to enshrine shared values, principles, understandings and objectives for an improved global digital cooperation architecture. As part of this process, we understand that the UN Secretary-General may appoint a Technology Envoy.

5B: We support a multi-stakeholder "systems" approach for cooperation and regulation that is adaptive, agile, inclusive and fit for purpose for the fast-changing digital age.

LAYERS & PLAYERS

In the 1990s, there was a clear distinction between the technical layer and the political layer. With less than 100 million Internet users worldwide (out of the total world population of seven billion) Internet problems were seen as „sectoral problems“ and did not really play a role in the discussion of global political issues as international security, economic development, trade, environment, human rights etc. This has changed. Today we have around 4 billion Internet users and nearly all traditional“ public policy issues have an Internet related component. Internet experts are now included into public policy-making and governments pay closer attention to the discussion about technical issues. This has led to parallel and partly competitive negotiation structures and a clash of cultures.

Parallel institutional structures:

i. The established intergovernmental system of the United Nations emerging after WWII is based on intergovernmental treaties that give organizations a special limited mandate for a clearly defined area. The issues are negotiated by governments alone and the outcomes are legally binding treaties. There is very little to no inter-institutional coordination or cooperation across the various sectors.

ii. Over the last three decades, a complementary system of non-governmental Constituencies have emerged where non-state actors from the private sector, civil society and the technical community have built institutions that develop specific policies. The outcomes are technical code, industry self-regulation or legally non-binding commitments. These platforms are highly interconnected.

iii. As a result, issues such as cybersecurity, eCommerce, privacy, Internet protocols or the DNS are negotiated by different state and non-state groups, which can lead to confusing and contradicting regulations.

Clash of cultures:

i. Negotiations among constituencies are iterative processes that include public consultation. They are open, transparent, bottom up, inclusive, and based on the philosophy of “rough consensus and running code”.

ii. Negotiations among governments are very mainly behind closed doors, they are not inclusive, not transparent and are based on majority voting or full consensus.

Global intergovernmental negotiations on disarmament, environment, trade or development are not interconnected. They are managed by different ministries within national governments. There is little to no coordination among the various negotiators. In the Internet, everything is connected with everything. A new technical protocol, as DOH, can have major implications for cybersecurity, affect business models, and strengthen or weaken human rights. The same goes for political decisions. The new European General Data Protection Regulation (GDPR), which intends to strengthen the individual right to privacy, affects the business of many Internet companies, digital trade as well as policing cyberspace and the work of law enforcement agencies.

Issues

There is nearly no public policy issue anymore which is not Internet related. In 2015 the Correspondence Group of the UNCSTD Working Group of Enhanced Cooperation (WGEC) tried to identify Internet related public policy issues and ended up with a list of more than 600 issues. All those issues can be packed into four baskets:

a. Cybersecurity
b. Digital Economy;
c. Human Rights;
d. Technology.

For the majority of the 600+ issues there are existing platforms where either governments or non-state actors are negotiating norms and regulations. This has led to a very diversified and unconnected tableau of Internet related negotiations and discussions where different constituencies and stakeholders are constrained to their silos – often ignoring what is happening in other silos. There are only a limited number of platforms, as the IGF that enable and stimulate cross-sectoral and cross-constituency multistakeholder discussions and a more holistic approach.

Basket 1: Cybersecurity

Cybersecurity is discussed by the United Nations mainly in the 1st Committee of the UN General Assembly, UNGGE, OEWG, GGECCW, UN Security Council Counter Terrorism Committee, ITU, Council of Europe, European Union, African Union, Interpol/Europol, Wassenaar Arrangement, Global Commission on the Stability of Cyberspace (GCSC), Global Conference on Cyberspace (GCCS),

Munich Security Conference (MSC), Global Forum on Cyber Expertise (GFCE), NATO, WSIS, IGF, OSCE, G7, BRICS, and others. For a number of specific issues there are special negotiation and discussion platforms, such as:

a. Norms of behavior of state and non-state actors in cyberspace: UNGGE, OEWH, GGECCW, OSCE, G7, BRICS, GCSC, GCCS, WEF;

b. Confidence building measures in cyberspace (CBMs): UNGGE, OEWG, OSCE, ASEAN, G7, BRICS, GCSC, GCCS;

c. Protection of the public core of the Internet and critical infrastructure as electricity, financial transactions, transportation services and electoral systems: UN, G7, ICANN/PIT, GCSC, GCCS, MSC, NATO;

d. Lethal autonomous weapon systems (LAWS) and other Internet based offensive cyber weapons: GGECCW, GCCS;

e. Dual-use technologies: Wassenaar Arrangement, GCSC, GCCS

f. Fight against cybercrime: Council of Europe, Interpol/Europol, GFCE, GCSC, GCCS, WEF, EU, AU

g. Fight against the terrorist use of ICTs: UN Security Council Counter Terrorism Committee, Interpol/Europol, GCCS, GCSC, WEF.

Basket 2: Digital Economy

Digital economy is discussed by the G20, the G7, WTO, UNCTAD, UNDP, WIPO, UNCITRAL, OECD, the World Economic Forum (WEF), UNCSTD, WSIS, IGF, the International Trademark Association (INTA), ICANN, Trademark Clearinghouse etc. For a number of specific issues there are special negotiation platforms, such as:

a. Digital Trade: G7, G20, WTO, UNCTAD, OECD, WEF, IGF;

b. eCommerce: WTO, UNCTAD, UNDP, UNCITRAL, OECD, WEF;

c. Infrastructure development: UN Regional Commissions, ITU, UNCTAD, IGF, WSIS

d. Industry 4.0: G20, G7, WEF, IGF, OECD

e. Internet of Things : G20, G7, ITU-T, IGF, WEF, OECD

f. Artificial Intelligence : G20, G7, IGF, WEF, OECD

g. Protection of Intellectual Property: WIPO, WSIS, IGF, INTA, OECD, ICANN/Trademark Clearinghouse

Basket 3: Human Rights

Human Rights are discussed by the 3rd Committee of the UN General Assembly, the UN Human Rights Council (HRC Special Rapporteurs for Freedom of Expression and Privacy in the Digital Age), UNESCO, ILO, Council of Europe, OSCE, WSIS, IGF, UNDP, UNCSTD, Freedom Online Coalition (FOC), Reporter without Borders (RWB), APC, Human Rights Watch (HRW), the Global Commission on the Future of Work and others. For a number of specific issues, there are special negotiation and discussion platforms, such as:

a. Access to the Internet: UNESCO, ITU, WSIS, IGF, APC;

b. Freedom of expression: HRC, UNESCO, Council of Europe, OSCE, WSIS, IGF, FOC, RWB, HRW;

c. Privacy in the digital age: HRC, UNESCO, Council of Europe, WSIS, IGF, FOC, ICANN/Whois;

d. Freedom of Association, HRC, UN

e. Right to education: HRC, UNESCO

f. Right to culture: HRC, UNESCO

g. Online Media: HRC, UNESCO, Council of Europe, OSCE

h. Future of work: HRC, ILO, Global Commission on the Future of Work

Basket 4: Technology

Technical issues are discussed by the so-called I*Organizations such as ICANN, IETF, IAB, ISOC, W3C, RIRs and the IGF but also by intergovernmental organizations including WSIS, ITU and ETSI. For a number of specific issues there are special negotiations and discussion platforms, such as:

a. IP addresses: RIRs, IETF, IGF, WSIS, ITU;

b. Domain Name System: ICANN, OETF, IGF, WSIS, ITU;

c. Root server system: ICANN/PIT, IGF;

d. Internet protocols: IETF, W3C, IEEE, 3GPPP, ITU, ETSI, IGF;

e. IOT: ITU-T, IGF, WSIS;

f. OTT: ITU-T, IGF.

ABOUT THE AUTHORS

Carlos A. Afonso

Master in Economics, York University, Toronto, Canada, with doctoral studies in Social and Political Thought at the same university. Works in human development fields since the early 1970s. Co-founder of the APC (1990). Coordinator of the Eco ,92 Internet project with APC and the UN. Member of the UN's Working Group on Internet Governance (WGIG) - 2004-2005. Special advisor, Internet Governance Forum (IGF), 2007. Member of the UNCTAD Expert Group on ICT and Poverty Alleviation (2009-2011). Member of the UNCSTD Working Group on Enhanced Cooperation (WGEC, 2013-2018). Co-founder and board member of the Brazilian Internet Steering Committee (CGI.br, 1995-1997 and 2003-2017). Co-founder and chair of the Brazilian chapter of Internet Society (2012-2017). Member of the IGF MAG (2019-2021). Executive director of Instituto Nupef, Rio de Janeiro.

Byrganym Aitimova

Byrganym Aitimova was born 26 February 1953 in Kazakh Soviet Republic. In 1974 Mrs. Aitimova graduated Uralsk pedagogical university, National Al-Farabi university in 1994. Ambassador extraordinary and plenipotentiary. Minister of sport, tourism and youth of the Republic of Kazakhstan (1993-1996); Member of the Senate of the Parliament of the Republic of Kazakhstan (01.1996-10.1996); Ambassador to Israel (1196-2002, Ambassador to Italy (10.1996); Vice - Premier-Minister of the Republic of Kazakhstan (14.05.2004-13.12.2005); Minister of science and education of the Republic of Kazakhstan (13.12.2005-10.01.2007); Ambassador of Kazakhstan to the UN (12.02.2007-08.2013); Ambassador to Cuba (05.2007-08.2013); Ambassador to Solomon Islands (08.2012-08.2013) Member of the Senate of the Parliament of the Republic of Kazakhstan (08.2013-12.08.2019); Chairman of social and culture Committee of the Senate of the Parliament of the Republic of Kazakhstan (09.2017-12.08.2019)

Abdul-Hakeem Ajijola

Abdul-Hakeem Ajijola (AhA), a global Cybersecurity resource is ranked #13 in the IFSEC Global Cybersecurity professionals influencers and thought leaders list; he is concurrently a Commissioner, Global Commission on the Stability of Cyberspace (#theGCSC); Chair, Working Group on Cyber Incident Management and Critical Information Protection of Global Forum on Cyber Expertise #theGFCE; Listed on the United Nations Office for Disarmament Affairs (UNODA) Roster of Experts supporting the development of an online training course in "Cyberdiplomacy;" Member, Group of Experts for the Nigerian Senate Committee on Cybersecurity and ICT. He is a founding member Organisation of Islamic Cooperation – Computer Emergency Response Team (OIC-CERT). AhA's day time job is Chairman, Consultancy Support Services (CS2) Ltd., www.cs2.com.ng a Cyber Security, e-Library and Information Communication Technology (ICT) Policy Consultancy Firm, based in Abuja, Nigeria. He is working to kick-start the development of an Africa CyberSecurity Economic sub sector employing thousands of knowledge workers, below 35 years of age, who will profitably drive CyberSecurity solutions value chains to solve problems, many of which don't yet exist.

Natasha Aduloju-Ajijola

Natasha Aduloju-Ajijola, PhD, MPH works with Consultancy Support Services as a research consultant and data analyst. Her research has focused primarily on health inequalities, sexual and reproductive health, and the impact of stress on health behaviors. She is a research fellow with the Global Institute of Sustainable Prosperity and was a Post Doctoral Fellow supported by the Clinical and Translational Science Award grant from National Center for Advancing Translational Science awarded to the University of Kansas for Frontiers: University of Kansas Clinical and Translational Science Institute.

Fiona Alexander

Fiona Alexander is Distinguished Policy Strategist in Residence in the School of International Service and Distinguished Fellow in the Internet Governance Lab at American University.

Virgilio Almeida

Virgilio A.F. Almeida is a professor in the Computer Science at the Federal University of Minas Gerais (UFMG), Brazil, and a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University. Virgilio was the National Secretary for Information Technology Policies of the Brazilian Government from 2011 to 2015. He was the chair of the Brazilian Internet Steering Committee (CGI.br) and chairman of NETmundial, the Global Multistakeholder Conference on the Future of Internet Governance (2014). He is currently one of the commissioners of the Global Commission for the Stability of Cyberspace.

Guy Berger

Guy Berger is UNESCO's director for Freedom of Expression and Media Development, based in Paris. He oversees the Organisation's programmes that promote press freedom and freedom of information, safety of journalists, media development, and media and information literacy. These activities cover media online and offline, and include UNESCO's Internet Freedom Series and UNESCO's indicator framework for assessing Internet Universality. Berger previously headed the School of Journalism and Media Studies at Rhodes University, South Africa.

Roland Busch

Dr. Roland Busch is Deputy CEO and CTO of Siemens AG. As head of Corporate Development, he is responsible for driving digital transformation and IoT, R&D and emerging technologies. Roland is also responsible for Next47, a global venture firm of Siemens, which focuses on deep tech startups working in areas like artificial intelligence, cybersecurity, IoT and robotics. He leads the company's sustainability and carbon neutral initiatives. In addition, he is responsible for Siemens Mobility GmbH, a leader in intelligent mobility solutions.

Pilar del Castillo

Pilar del Castillo, Former Minister of Education and Culture from 2000 to 2004, del Castillo was elected to the European Parliament for the first time in 2004. She is a member of the European People's Party (EPP). She has been, among others, the European Parliament's rapporteur on the European Electronic Communications Code; the Telecoms Single Market Regulation; the Directive on Security of Networks and Information Systems for the ITRE committee; the Regulation on the Body of European Regulators in Electronic Communications' (BEREC); the report on Cloud Computing Strategy for Europe and the Report "A Digital Agenda for Europe: 2015.eu. Del Castillo is the Chair of the European Internet Forum (EIF)".

Olga Cavalli

Olga Cavalli is an Internet leader whose work has been fundamental for enhancing a relevant participation of Latin America and the Caribbean in Internet Governance.

Olga is a Member of the ISOC Board of Trustees and Co-founder of ARGENSIG the Argentine School on Internet Governance, SSIG School on Internet Governance and Dominios Latinoamerica.

She has recently co-edited the book “Internet Governance and regulations in Latin America” available free for the community in Spanish, Portuguese and English. She is vice chair of the GAC of ICANN and during 2007- 2014 she was a member of the MAG. She is also a university teacher at the University of Buenos Aires. Her education includes a PhD in Business Direction, an MBA, a Master degree in Telecommunications Regulation, and Electronic and Electric Engineer. She is Fluent in Spanish, English, Portuguese and German, and can understand French and Italian. Olga lives in Buenos Aires and is the mother of Juana and Federico.

Vinton G. Cerf

Vinton G. Cerf is vice president and Chief Internet Evangelist for Google. Cerf is the co-designer of the TCP/IP protocols and the architecture of the Internet. He has served in executive positions at ICANN, the Internet Society, MCI, the Corporation for National Research Initiatives and the Defense Advanced Research Projects Agency. A former member of the US National Science Board, he is the past President of the Association for Computing Machinery and serves in advisory capacities at NIST and NASA.

Steve Crocker

Stephen (Steve) D. Crocker has been involved in the Arpanet and Internet from the beginning, including the creation of the Request for Comments series of notes and chairing of the Network Working Group 1968-71. Crocker was the first area director for security in the Internet Engineering Task Force (IETF) 1989-94, founding chair of ICANN’s Security and Stability Committee (SSAC) 2002-2010, and ICANN board member 2003-2017, including chair 2011-2017. Crocker holds a B.A. in mathematics and a Ph.D. in computer science, both from UCLA.

Bertrand de la Chapelle

Bertrand de La Chapelle is, since 2012, the Executive Director and Co-founder of the Internet & Jurisdiction Policy Network, building on more than 15 years of experience in internet governance processes. He was previously a Director on the ICANN Board (2010-2013), France‘s Thematic Ambassador and Special Envoy for the Information Society (2006-2010) and an active participant in the World Summit on the Information Society (2002-2005). Bertrand de La Chapelle is a graduate of Ecole Polytechnique (1978), Sciences Po Paris (1983), and Ecole Nationale d‘Administration (1986).

Hans-Peter Dittler

Hans Peter Dittler started his working career in 1977 as a research assistant at the University of Karlsruhe after graduating there in computer science. Since 1995 he is president and owner of BRAINTEC Netzwerk-Consulting GmbH in Karlsruhe; since 1992 he is active at the IETF (Internet Engineering Task Force); since 1997, he is a member of the board of the German chapter of the Internet Society (ISOC.DE); since 2014 is a member of the Board of Trustees of the Internet Society.

Eileen Donahoe

Eileen Donahoe is Executive Director of the Global Digital Policy Incubator (GDPI) at Stanford University. GDPI is a global multi-stakeholder collaboration hub for development of digital policies that reinforce human rights.She served as the first US Ambassador to the United Nations Human Rights Council in Geneva during the Obama administration, and later as Director of Global Affairs at Human Rights Watch.

Raul Echeberria

Raúl Echeberría is a broadly recognized expert in the fields of Internet Policy, Development and Governance field. He currently works as an independent consultant. Raúl served as Vicepresident for Global Engagement and Relations at Internet Society (ISOC) between 2014 and 2019, he was a member of the Board of Trustees of ISOC between 2008 and 2014, and Chair of the Board between 2009 and 2012. Echeberrría was one of the founders of LACNIC (The Internet Addresses Regsitry for Latinamerica and the Caribbean) and CEO of the organizations between 2002 and 2014. Along his career, Raúl has also served in other important positions like: Member of the Working Group on Internet Governance (WGIG) formed in 2004 by the United Nations Secretary General, member of the Uruguayan delegation to the World Information Society Summit (WSIS) in 2005, member of the Multistakeholder Advisory Group of the Internet Govenance Forum (IGF MAG) between 2006 and 2014, and Co-chair of the Executive Committee of NetMundial in 2014.

Echeberría has been awarded in 2014 with the “Ing. Julio Granato Award” for his contribution to the digital inclusion in Uruguay and in 2015 with the “Trayectoria Award” for his “continued contribution to an Open, Stable and Secure Internet for the development of Latinamerica and the Caribberan”.

Anriette Esterhuysen

Anriette Esterhuysen was the executive director of the Association for Progressive Communications - the largest ICT-focused civil society network in the world - from 2000 to 2016. She continues to work with APC as a consultant and coordinates the annual African School on Internet Governance (AfriSIG). Anriette was a member of the IGF‘s Multistakeholder Advisory Group (MAG) from 2012 to 2014. Currently she serves as a Commissioner on the Global Commission on the Stability of Cyberspace. She has published extensively on ICTs for development and social justice. She is based in Johannesburg, South Africa.

Melinda Gates

Philanthropist Melinda Gates has dedicated her life to achieving transformational improvements in the health and prosperity of families, communities and societies. Core to her work is empowering women and girls to help them realize their full potential. As co-chair of the Bill & Melinda Gates Foundation, Melinda shapes and approves strategies, reviews results, and sets the overall direction of the world’s largest private foundation. In 2015, Melinda created Pivotal Ventures, an investment and incubation company that enables her to bring together other new and emerging strands of her advocacy and philanthropic work focused in the US. Melinda received a bachelor’s degree from Duke and an MBA from Duke’s Fuqua School. After joining Microsoft Corp. in 1987, she helped develop many of the company’s multimedia products. In 1996, Melinda left Microsoft to focus on her philanthropic work and family.

(c) WEF swiss-image.ch/Remy Steinegger

Amandeep Gill

Amandeep Gill is the former Executive Director & Co-Lead of the Secretariat of the UN Secretary-General’s High-level Panel on Digital Cooperation and former Chair of the Group of Governmental Experts on Lethal Autonomous Weapons Systems. In follow-up to the Panel’s report, he is currently leading a new multi-stakeholder initiative for establishing an international collaborative on Digital Health and AI research.

António Guterres

António Guterres, the ninth Secretary-General of the United Nations, took office on 1st January 2017.

Having witnessed the suffering of the most vulnerable people on earth, in refugee camps and in war zones, the Secretary-General is determined to make human dignity the core of his work, and to serve as a peace broker, a bridge-builder and a promoter of reform and innovation.

Prior to his appointment as Secretary-General, Mr. Guterres served as United Nations High Commissioner for Refugees from June 2005 to December 2015, heading one of the world's foremost humanitarian organizations during some of the most serious displacement crises in decades. The conflicts in Syria and Iraq, and the crises in South Sudan, the Central African Republic and Yemen, led to a huge rise in UNHCR's activities as the number of people displaced by conflict and persecution rose from 38 million in 2005 to over 60 million in 2015.

Before joining UNHCR, Mr. Guterres spent more than 20 years in government and public service. He served as prime minister of Portugal from 1995 to 2002, during which time he was heavily involved in the international effort to resolve the crisis in East Timor.

As president of the European Council in early 2000, he led the adoption of the Lisbon Agenda for growth and jobs, and co-chaired the first European Union-Africa summit. He was a member of the Portuguese Council of State from 1991 to 2002.

Mr. Guterres was elected to the Portuguese Parliament in 1976 where he served as a member for 17 years. During that time, he chaired the Parliamentary Committee for Economy, Finance and Planning, and later the Parliamentary Committee for Territorial Administration, Municipalities and Environment. He was also leader of his party's parliamentary group.

From 1981 to 1983, Mr. Guterres was a member of the Parliamentary Assembly of the Council of Europe, where he chaired the Committee on Demography, Migration and Refugees.

For many years Mr. Guterres was active in the Socialist International, a worldwide organization of social democratic political parties. He was the group's vice-president from 1992 to 1999, co-chairing the African Committee and later the Development Committee. He served as President from 1999 until mid-2005. In addition, he founded the Portuguese Refugee Council as well as the Portuguese Consumers Association DECO, and served as president of the Centro de Acção Social Universitário, an association carrying out social development projects in poor neighbourhoods of Lisbon, in the early 1970s.

Mr. Guterres is a member of the Club of Madrid, a leadership alliance of democratic former presidents and prime ministers from around the world.

Mr. Guterres was born in Lisbon in 1949 and graduated from the Instituto Superior Técnico with a degree in engineering. He is fluent in Portuguese, English, French and Spanish. He is married to Catarina de Almeida Vaz Pinto, Deputy Mayor for Culture of Lisbon, and has two children, a stepson and three grandchildren.

Philipp Grabensee

Philipp Grabensee is a co-founder and Deputy Chairman at Afilias. He has extensive experience in DNS, Domain Names and leads Afilias' worldwide government relations team. Philipp is a practicing criminal defense attorney and partner of the law firm SHSG, Rechtsanwälte und Fachanwälte für Strafrecht, Düsseldorf. He represents Afilias on the board of the Global Commission on the Stabilty of Cyberspace, was previously a member of the Names Council in the ICANN Domain Name Supporting Organization. He served as Chairman of the Afilias board from 2003 to 2014.

Brian Huseman

Brian Huseman is Vice President, Public Policy at Amazon. He joined Amazon in 2012 from Intel Corporation. Prior to Intel, Brian worked at the U.S. Federal Trade Commission as Chief of Staff to the Chairman. Brian is Co-Chair of the U.S. Chamber of Commerce's Global Connect Committee and is Vice-Chair of the Executive Committee of the Information Technology Industry Council. Additionally, Brian serves on the High-Level Advisory Group of the Internet & Jurisdiction Policy Network. A highly respected public policy professional, Brian has contributed significantly to the development of the multi-stakeholder model of internet governance and remains actively engaged with related organizations, including ICANN and the Internet Governance Forum. He has a law degree and a B.A. in political science.

Wolfgang Ischinger

Ambassador Wolfgang Ischinger has been Chairman of the Munich Security Conference (MSC) since 2008. A German career diplomat, he was State Secretary (Deputy Foreign Minister) from 1998 to 2001. From 2001 to 2006, he was the Federal Republic of Germany‘s Ambassador to the US, and from 2006 to 2008, to the Court of St James‘s. He is a Senior Professor at the Hertie

School of Governance, Berlin, and serves on the boards of numerous companies as well as non-profit-institutions, including Atlantik-Brücke/Berlin, AICGS/Washington D. C., the American Academy/Berlin, and the Atlantic Council of the United States/Washington D.C.

Manal Ismail

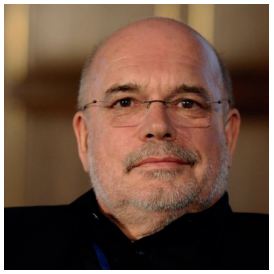
Ms. Manal Ismail is Executive Director for International Technical Coordination at the National Telecom Regulatory Authority of Egypt and Chair of the Governmental Advisory Committee of ICANN. She is a member of the Internet and Jurisdiction Domains Contact Group, was a member of the NETmundial Executive Multistakeholder Committee, and founding member of ISOC-EG and AfriNIC. She participates to the IGF, Arab IGF, and League of Arab States.

Marina Kaljurand

Marina Kaljurand was elected to the European Parliament in 2019. She was a member of the UN Secretary General's High Level Panel on Digital Cooperation (2018-2019) and was twice appointed to the UN GGEs (2014-2017). Kaljurand had a long career in Estonian Foreign Service. She served as Estonian Ambassador to Russia, USA, Israel, Kazakhstan, Mexico and Canada. Kaljurand was Estonian Foreign Minister in 2015-2016. She is currently member of the Global Commission of the Stability of Cyberspace (GCSC).

Matthias C. Kettemann

PD Mag. Dr. Matthias C. Kettemann, LL.M. (Harvard), is Head of the Research Program Regulatory Structures and the Emergence of Rules in Online Spaces at the Leibniz Institute for Media Research | Hans-Bredow-Institut (HBI), Hamburg, Chair ad interim for Public Law, International Law and Human Rights - Hengstberger Professor for the Foundations and Future of the Rule of Law, University of Heidelberg, and associated researcher at the Alexander von Humboldt Institute for Internet and Society, Berlin. His research focuses on how rules develop in online spaces, how individual spheres of freedom are protected, and how societal values and the common interest is insured in sociotechnical constellations. He studied international law in Graz, Geneva and Harvard Law School and completed his postdoctoral work at the Cluster of Excellence "The Emergence of Normative Orders" at Goethe University Frankfurt am Main. Matthias has provided expertise for the German Bundestag, several DAX companies, foundations and international organizations, on Internet regulation, cybersecurity and human rights.



Wolfgang Kleinwächter

Prof. Dr. Wolfgang Kleinwächter, Professor Emeritus at the University of Aarhus, is a member of the Global Commission on Stability in Cyberspace, was a member of the ICANN Board (2013-2015) and served as Special Ambassador for the NetMundial Initiative (2014-2016).

Alexander Klimburg

Dr. Alexander Klimburg is Director of the Cyber Policy and Resilience Program and of the Global Commission on the Stability of Cyberspace Initiative. He is also a nonresident senior fellow with the Atlantic Council, and associate and former fellow of Harvard University. His most recent book "The Darkening Web: The War for Cyberspace" was published by Penguin Press and described in The New York Review of Books as "an important and prescient book."

Jovan Kurbalija

Jovan Kurbalija is Founding Director of DiploFoundation and Head of the Geneva Internet Platform. In 2018 - 2019, he served as co-Executive Director of the UN Secretary General's High Level Panel on Digital Cooperation. Previously, he was Special Advisor to the Chairman of the UN Internet Governance Forum. His book, An Introduction to Internet Governance, has been translated into 9 languages and is used as a textbook for academic courses worldwide.

Yrjö Länsipuro

With a background in journalism and public diplomacy, Yrjö Länsipuro is a member of the Board and past president of the Finnish chapter of Internet Society. While working for the foreign service, he represented Finland at the WSIS and in the Governmental Advisory Committee (GAC) of ICANN. He is now the Liaison of ICANN's At-Large Advisory Committee to the GAC.

Chuanying Lu

Dr. Lu, Chuanying is senior fellow and director of the Research Center for Cyberspace Governance (RCGCG), Shanghai Institutes for International Studies. He has experienced working for the foreign ministry of China and China cyberspace administration. He was a visiting fellow of the Center for Strategic and International Studies, Oxford University (U.K.). Dr. Lu specializes on cyberspace governance and cyber security. He is the co-founder of Roundtable of Military Cyber Stability, and the Editor Chief of Information Security and Communication Privacy. He has published a couple of articles on the issues of cyberspace on journals and newspapers including Cyberspace Governance, Cyber Security.

Jack Ma

Jack Ma founded Alibaba Group in 1999. He has served as Alibaba's executive chairman since May 2013, and previously as chairman and chief executive officer. Jack is also the founder of the Zhejiang-based Jack Ma Foundation. Jack founded Alibaba based on the belief that the Internet could democratize the playing field for all types of businesses, particularly small businesses. This tenet continues to underpin his vision for Alibaba, both in China and around the world.

In September 2016, Jack was named special adviser of the United Nations Conference on Trade and Development (UNCTAD) for Youth Entrepreneurship and Small Business. He also served as chair of the 2016 B20 Small and Medium-Sized Enterprises Development Taskforce, where he called for the establishment of an Electronic World Trade Platform (eWTP), an internet-based trading platform to help bring small businesses into the global economy and make it easier for them to expand trading capabilities worldwide.

Jack currently serves on the Board of SoftBank Group Corp., a Japanese corporation listed on the Tokyo Stock Exchange. He is also a member of the Foundation Board of the World Economic Forum, a member of the Board of the Breakthrough Energy Ventures, chairman of the Zhejiang Chamber of Commerce, and chairman of the China Entrepreneur Club. In January 2016, he was named a Sustainable Development Goals (SDGS) advocate by the United Nations.

Jack graduated from Hangzhou Teacher's Institute with a major in English language education.

(c) World Economic Forum / Ciaran McCrickard

Peter Major

Peter Major is vice-chair of the UN Commission on Science and Technology for Development (CSTD). He actively participated in international forums for more than 30 years. Peter chaired the CSTD Working Group on the Improvements of the IGF. Subsequently he chaired the CSTD Working Group on Enhanced Cooperation. Peter was a member of the IGF MAG and he is alternate representative of

Hungary of CANN GAC.

Robin Mansell

Robin Mansell is Professor in the Department of Media and Communications, London School of Economics and Political Science, Board member of TPRC (Research Conference on Communications, Information and Internet Policy), past President, International Association for Media and Communication Research (IAMCR), and author of Imagining the Internet: Communication, Innovation and Governance, OUP.

Ram Mohan

Ram Mohan, Chief Operating Officer at Afilias Inc., chaired the Technical Study Group on Access to Non-Public Registration Data, is a Board member of the Global Commission on Stability in Cyberspace, was a member of the ICANN Board (2008-2018), and a founding member of the ICANN Security and Stability Advisory Committee (SSAC). A recognized expert on cybersecurity and internationalization, he is a columnist and an inventor of several technology patents.

Katharina Mosene

Katharina Mosene, Political Scientist (M.A.), Research- and Event Cooperation, Leibniz Institute for Media Research | Hans-Bredow-Institut (HBI); also associated with the TUM Medical Education Center, Technical University of Munich in the area of Digital Education / eLearning; she gives workshops for volunteers and associations on Internet security topics (Deutschland sicher im Netz e.V. / Federal Ministry of the Interior, Germany); and is founding member of netzforma* e.V. – Verein für feministische Netzpolitik, where she deals with topics such as promoting equal access to the Internet, protection against violence online and the right to privacy.

Annette Mühlberg

Annette Mühlberg works as head of the project team “digitization” for the United Services Union (ver.di) in Berlin and is member of the Steering Committee of the German IGF and the Platform Cooperative Consortium. She was chair of the At-Large Advisory Committee of ICANN and member of the Enquête-Commission on “Internet and Digital Society“ of the German Bundestag.

Daniel Nanghaka

Daniel K. Nanghaka is the Executive Director of ILICIT Africa (Integrating Livelihoods thru Communication Information Technology for Africa), Lead of The-Internet.Africa a platform to promote adoption for Modern Internet Standards for Africa, former Chair of FOSSFA (Foundation of Open Source Software for Africa), and Chair of ICANN At-Large Outreach and Engagement Sub Committee, Member of the Third Accountability and Transparency Review Team at ICANN, Founder of Project Thread which is developing MESH Networks for disaster and emergency communications in Bududa. Daniel is passionate about the Internet Technology transformation in Africa and strongly advocates for promotion of local content, Mapping, FOSS, Building Community Networks and Software Development, particularly supporting youth development and social justice programs. He has been active in the field of ICT and Internet Governance where he has contributed to various fora both locally and internationally. He holds a Bachelor’s Degree in Information Technology, Certificate in Software Engineering, Certificate in Scalable Network Infrastructure (AfNOG), trained in Information for Collaborative Development at the United Nations Institute of Training and Research, Impact Business Modelling and Investment (Ghana).

Nnenna Nwakanma

Nnenna advocates for policy and systemic changes that are needed for meaningful internet access, open data, open government and the open web across Africa, bringing together local and international stakeholders to advance the digital agenda. She works to drive affordable internet access, data rights, digital freedom and digital responsibilities of stakeholders, sectors and actors.

Nnenna is a respected technology voice and leader in Africa. Her capacity to network and bridge the gap between the local and the global has made her a voice bearer for women, rural populations, the unconnected and the civil society across the world.

Nnenna is a Diplo alumnus, an ICT4D Strategist, an expert in eParticipation and Citizen Engagement, one of the early pioneers of the Africa Data Revolution, a respected voice in the UN's Internet Governance Forum, a pioneer and continued advisor on internet governance in Africa, and Faculty at the Schools of Internet Governance. She has over 15 years of experience working with the United Nations Systems in human rights, information society, gender, data digital equality and sustainable development.

Her career has allowed her to work closely with many civil society organisations, the African Development Bank, the Digital Solidarity Fund and has seen her involved in many phases of the UN's Africa Information Society Initiative. As well as leading a highly regarded consultancy platform, Nnenna has in recent years co-founded The Free Software and Open Source Foundation for Africa, and served as a board member of the Open Source Initiative. She has lived and worked in five African countries and is fluent in English, French and a number of African languages.

Christopher Painter

Chris Painter is a globally recognized leader and expert on cyber policy, Cyber Diplomacy and combating cybercrime. He has been on the vanguard of US and international cyber issues for over twenty-five years – first as a leading federal prosecutor of some of the most high-profile cybercrime cases in the country, then as a senior official at the Department of Justice, the FBI, the Senior Director for Cyber Policy at the White House National Security Council and finally as the world's first top cyber diplomat at the State Department. In his State Department role, Mr. Painter helped create a whole new area of foreign policy focus and there are now cyber diplomats in over thirty countries. Among other things, he currently serves as a Commissioner on the Global Commission for the Stability of Cyberspace, Chair of the Global Forum for Cyber Expertise Working Group on Strategy and Policy, a member of the Board of Directors for the Center for Internet Security and an Associate Fellow at Chatham House.

Latha Reddy

Ambassador Latha Reddy is currently the Co-Chair of the Global Commission on the Security of Cyberspace since 2017. She is also a Distinguished Fellow at think tanks in India and overseas, and serves on the boards of several companies and organizations. She served in the Indian Foreign Service from 1975-2011 and as India's Deputy National Security Adviser from 2011-2013. She has wide experience in multilateral and bilateral diplomacy, and in recent years, has focused on cyber policy issues, with emphasis on internet governance, norm-building and international cyber cooperation.

Uri Rosenthal

Present positions (A.O): Commissioner Global Commission on Stability of Cyberspace, Special Representative to Global Conference on Cyberspace ('London process'); Chairman Dutch Advisory Council for Science, Technology and Innovation Policy; Chairman Dutch Supervisory Council for Veterans Care; Adviser Crisis Research Center, Tsinghua University, Beijing, China; Adviser Crisis Management Center, Nanjing University, China

Previous positions: Politics: Minister of Foreign Affairs Kingdom of The Netherlands, 2010-2012; Chairman Parliamentary Group People's Party for Freedom and Democracy, Senate, 2005-2010; Member Parliamentary Group People's Party for Freedom and Democracy, Senate, 1999-2005

Corporate: President COT Institute for Safety, Security and Crisis Management (since 2008 an Aon Company). Focus on political leaders, high-level public officials and corporate leaders: instant advice in acute crises; post-crisis strategic and organizational development.

Academic: Professor of Political Science and Public Management, Erasmus University Rotterdam and Leiden University, 1980-2010. Dean Netherlands School of Government, 1989-1999: professional school for high-fliers Dutch civil service and public sector specialists in corporate sector. Vice-chairman Netherlands Science Foundation, 1999-2004

Michael Rotert

Through his work at various national and international bodies, Prof. Rotert is committed to providing intensive support for the success of the Internet. He has been Chairman of eco Association of the Internet Industry and has been President of EuroISPA (European Internet Services Providers Association), and industrial speaker of the German delegation of the G8 Cybercrime group. He also works as an expert for the EU, UN and the U.S. Department of Commerce. In 1991 he was one of the founding members of ISOC (Internet Society) in Copenhagen.

Richard Samans

Richard Samans is a Managing Director of the World Economic Forum, Chairman of the Climate Disclosure Standards Board and member of the ILO Global Commission on the Future of Work. He previously served as Director-General of the Global Green Growth Institute; Special Assistant to the President for International Economic Policy and Senior Director for International Economic Affairs of the US National Security Council during the Clinton Administration; and economic policy advisor to US Senate Democratic Leader Thomas A. Daschle.

Marietje Schaake

Marietje Schaake has been named Stanford University's Cyber Policy Center's international policy director, as well as international policy fellow at the University's Institute for Human-Centered Artificial Intelligence (starting November 1). Between 2009 and 2019 she served as a Member of European Parliament for the Dutch liberal democratic party where she focussed on trade, foreign affairs and technology policies. Marietje regularly speaks at conferences and in international media. She is a Member of the Global Commission on the Stability of Cyberspace and the Transatlantic Commission on Election Integrity, and affiliated with a number of non-profits including the European Council on Foreign Relations and the Observer Research Foundation in India. She writes a bi-weekly column for the Dutch NRC newspaper.

Thomas Schneider

Thomas Schneider is Ambassador and Director of International Affairs at the Swiss Federal Office of Communication (OFCOM). He has been representing Switzerland in various international fora since the 2003 WSIS Summit, responsible for the hosting of the IGF 2017 in Geneva and chaired committees like ICANN's GAC (2014-2017) or the Council of Europe's CDMSI (2018-2019). He has also been an initiator of EuroDIG and the Swiss IGF.

Jimmy Schulz

Jimmy Schulz is a German internet entrepreneur and politician of the Free Democratic Party (FDP). After finishing his secondary education at the Ottobrunner Gymnasium, he studied political science at the University of Texas at Austin and in Munich, Germany. His passion for IT started at school, during which he worked at various IT companies and later, in 1995, founded CyberSolutions GmbH, which entered the stock

market in 2000. He is currently CEO of CyberSolutions Ltd., which has its company seat in Riemerling/Hohenbrunn. Jimmy Schulz has been actively fighting for civil rights and internet freedom for more than 20 years. From 2009 to 2013, he was a member of the German Parliament. He was spokesperson for the FDP in the commission of enquiry: “Internet and digital society.” From 2014 to 2016, he was a member of the ICANN At-large Advisory Committee (ALAC) and Vice Chairman of the Internet Society ISOC Germany (2015-2017). Since 2018, he has been a member of the Presidium of ISOC Germany. In 2017, he was again elected as a member of the German Parliament and is now chairing the Committee on the Digital Agenda.

Jörg Schweiger

Dr. Jörg Schweiger is Member of the Executive Board and CEO of DENIC eG, the managing organisation of Germany’s ccTLD .de. He regularly represents DENIC at international organisations, associations and conferences such as NETmundial, IGF or EuroDIG, and has a 12-year track record engaging in the ICANN multistakeholder ecosystem (ccNSO, NomCom, Working Group chair/co-chair). He is also a member of the IGF-D Steering Committee and Chairman of the Board of Directors of the Council of European National Top-Level Domain Registries, CENTR.

Max Senges

Dr. Max Senges is a Visiting Scholar at Stanford‘s Center on Democracy, Development, and the Rule of Law (CDDRL) and, while he is also a Senior Policy Manager at Google Germany, the assessments and positions expressed in this paper are only his and not his employers’.

Brett Solomon

Brett is the Executive Director of Access Now, an organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, global advocacy, and direct technical support, Access Now fights for open and secure communications for all. Brett is also the founder of RightsCon, Access Now‘s Annual Summit on the internet and human rights. Before Access Now, Brett honed his skills at Avaaz, GetUp, Oxfam Australia, and Amnesty International Australia. Brett has a Bachelors in Arts and Law and a Masters in International Law, and is on the Board of AllOut.

Lynn St. Amour

Ms. Lynn St.Amour served as the Chair of the United Nations Internet Governance Forum Multistakeholder Advisory Group (IGF-MAG) for four years (2016 – 2019). She served from 2001 to 2014 as President and CEO of the Internet Society (ISOC), a global non-profit dedicated to the open development, evolution and use of the Internet. Currently, she is President and CEO of Internet-Matters, an Internet consulting Company. This contribution was made in a personal capacity.

Ilona Stadnik

Ms Ilona Stadnik is a PhD candidate at the School of International Relations, St Petersburg State University, and a former Fulbright Visiting Researcher at Georgia Tech, Internet Governance Project (2018/2019). Her research covers international cyber norm-making, Russian-US relations in cybersecurity, and global Internet governance.

Christoph Steck

Christoph Steck is Director Public Policy & Internet for Telefonica. In this role, he defines Telefonica´s positions on Digital Policies, Internet Governance and other issues related to the Digital Economy. He is a Member of the IGF MAG, Chairman of the Internet Governance workgroup of ETNO and Vice-chair of the Business at OECD (BIAC) Committee on Digital Economic Policy. He has overseen the publication of the influential Digital Manifesto of Telefonica and was selected to be a member of the ICANN High-level Panel on Global Internet Cooperation & Governance and to present the private sector at the High-level Committee of NETMundial. Christoph studied Law and Human Rights at the Universities of Cologne, Munich and London (UCL) and is a qualified German lawyer. He also holds a Master of Business Administration (MBA) from IE Business School and is Associate Professor at the School of Human Science and Technology of IE University in Madrid as well as Fellow of Aspen Institute Spain.

Leonid Todorov

Leonid Todorov is General Manager of the Asia Pacific Top Level Domain Association (APTLD). Leonid also is a co-founder of the Russian IGF, sits on the Multistakeholder Steering Group of the Asia Pacific Regional Internet Governance Forum (APrIGF). He also is a member of the CCNSO ICANN's Strategic and Operations Plan Standing Committee Council and observer at the CCNSO Council. He has authored and co-authored publications on ccTLDs' operation, Internet governance, new gTLDs, public policy and international cooperation in the ICT area, and cybersecurity, and presented at various national and international events.

Andrew Wyckoff

Andrew Wyckoff is OECD's Director for Science, Technology and Innovation. The views expressed here are his own and do not reflect the OECD or its Member Countries.

Peixi XU

Professor, Communication University of China (CUC), Beijing. He is also Director of Global Internet Governance Project of CUC. He is author of Global Governance from Traditional Media to the Internet (Tsinghua University Press) and The Shaping Cyber Norms (China Social Sciences Academic Press).

Michael Yakushev

Michael Yakushev is one of best-known Russian experts on cyberlaw, internet governance, and digital transformation. He represented Russian Civil Society sector at DOT-Force, formed by G8 in 2000. He was also a member of WGIG (Working Group on Internet Governance under U.N.Secretary General) in 2004-2005, being the Head of Legal Department of the Federal Ministry of Telecommunications. Michael chaired the Board of cctld.RU Coordination Center for many years, and he was Vice-President of ICANN for Eastern Europe and Cenral Asia in 2014-2017. Since 2017 he works as Vice-President, Government Relations, of Vympelcom – Russian mobile operator.

Houlin Zaho

Houlin Zhao was first elected 19th Secretary-General of the ITU at the Busan Plenipotentiary Conference in October 2014. He took up his post on 1 January, 2015. ITU Member States reelected Houlin Zhao as ITU Secretary-General on 1 November 2018. He began his second four-year-term on 1 January 2019. Prior to his election, he served two terms of office as ITU Deputy Secretary-General (2007-2014), as well as two terms as elected Director of ITU‘s Telecommunication Standardization Bureau (1999-2006). Houlin Zhao is committed to further streamlining ITU‘s efficiency, to strengthening its membership base through greater involvement of the academic community and of small- and medium-sized enterprises, and to broadening multi-stakeholder-participation in ITU‘s work.

Jonathan Zittrain

Jonathan Zittrain is the George Bemis Professor of International Law at Harvard Law School and the Harvard Kennedy School of Government, Professor of Computer Science at the Harvard School of Engineering and Applied Sciences, Director of the Harvard Law School Library, and Co-Founder of the Berkman Klein Center for Internet & Society. His research interests include battles for control of digital property and content, cryptography, electronic privacy, the roles of intermediaries within Internet architecture, human computing, and the useful and unobtrusive deployment of technology in education. He performed the first large-scale tests of Internet filtering in China and Saudi Arabia, and as part of the OpenNet Initiative co-edited a series of studies of Internet filtering by national governments: Access Denied: The Practice and Policy of Global Internet Filtering; Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace; and Access Contested: Security, Identity, and Resistance in Asian Cyberspace. He is a member of the Board of Directors of the Electronic Frontier Foundation and a former member of the Board of Advisors for Scientific American. He has served as a Trustee of the Internet Society, and as a Forum Fellow of the World Economic Forum, which named him a Young Global Leader, and as Distinguished Scholar-in-Residence at the Federal Communications Commission, where he previously chaired the Open Internet Advisory Committee.

IMPRINT

Editors

Wolfgang Kleinwächter, Matthias C. Kettemann and Max Senges
with Katharina Mosene

Design and Layout

Vagedes & Schmid GmbH

Printing

Druckerei Gläser · Blücherstraße 22 · 10961 Berlin

ISBN 978-3-87296-148-8 (print)

ISBN 978-3-87296-152-5 (Ebook)

Kleinwächter, Wolfgang; Kettemann, Matthias C.; Senges, Max (2019) (eds.): Towards a Global Framework for Cyber Peace and Digital Cooperation: An Agenda for the 2020s. Hamburg: Verlag Hans-Bredow-Institut

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

LEIBNIZ-INSTITUT FÜR MEDIENFORSCHUNG HANS-BREDOW-INSTITUT