GLOBAL INFORMATION SOCIETY WATCH 2021-2022

Digital futures for a post-pandemic world

Association for Progressive Communications (APC)
and Swedish International Development Cooperation Agency (Sida)

Global Information Society Watch 2021-2022
Digital futures for a post-pandemic world

Operational team
Valeria Betancourt (APC)
Alan Finlay (APC)
Maja Romano (APC)

Project coordination team
Valeria Betancourt (APC)
Cathy Chen (APC)
Flavia Fascendini (APC)
Alan Finlay (APC)
Leila Nachawati (APC)
Lori Nordstrom (APC)
Maja Romano (APC)

Project coordinator
Maja Romano (APC)

Editor
Alan Finlay (APC)

Assistant editor and proofreading
Lori Nordstrom (APC)

Assistant proofreader
Drew McKevitt

Publication production support
Cathy Chen (APC)

Graphic design
Monocromo

Cover illustration
Matías Bervejillo

Sida

APC would like to thank the Swedish International Development Cooperation Agency (Sida) for their support for Global Information Society Watch 2021-2022.

Published by APC
2022

Global Information Society Watch 2021-2022 web and e-book
ISBN 978-92-95113-52-7
APC-202211-CIPP-R-EN-DIGITAL-342

Internet governance of the future

Anriette Esterhuysen[1] and Wim Degezelle[2]

The past

Twenty years ago, at the start of the preparatory process for the World Summit on the Information Society (WSIS), the internet – a "network of networks" – and internet governance were still abstract and largely unknown concepts to many delegates. In response, at the end of the first phase of the WSIS, the UN Secretary-General mandated a multistakeholder Working Group on Internet Governance (WGIG)[3] to investigate, define and make proposals on the governance of the internet to inform negotiations at the second and final phase of the WSIS in Tunis in 2005. The WGIG's working definition for internet governance was formally adopted in Tunis:

> 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.[4]

This definition, along with the affirmation in the Tunis Agenda (the final WSIS output document) that "the management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations,"[5] and the formation of the Internet Governance Forum (IGF),[6] promised a dynamic and inclusive future for internet governance.

David Souter recently described this period as a time when internet governance was "bright and shiny", when "new technologies and new ways of governing technologies suggested that there might be ways of changing how public policy gets made – not least by bringing more diversity into decision-making through multistakeholder participation."[7] It presented an opportunity for civil society actors to be part of evolving a new, fairer, global governance model at a time when there were wider calls in the UN for more inclusive and accountable global governance.[8] In its statement at the conclusion of the WSIS process, civil society expressed support for the idea of the IGF, committed to participate in it, but reiterated its view that "the forum should be more than a place for dialogue" and "should also provide expert analysis, trend monitoring, and capacity building, including in close collaboration with external partners in the research community."[9]

Civil society organisations have since participated actively in the IGF and in other post-WSIS global, regional and national policy processes.[10] They collaborated with institutions from other stakeholder groups to produce multiple internet governance frameworks, norms, principles and guidelines. Examples include the Brazilian Principles for the Governance and Use of the Internet,[11] the Necessary

1 Anriette Esterhuysen is an APC associate and a senior advisor on internet governance.

2 Wim Degezelle is an internet policy analyst and consultant.

3 Working Group on Internet Governance. (2005). *The Working Group on Internet Governance: Background Report.* https://www.itu.int/net/wsis/wgig/docs/wgig-background-report.pdf

4 Tunis Agenda, paragraph 34. https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

5 Ibid., paragraph 35.

6 The Tunis Agenda, in article 72, asked the UN Secretary General to convene a forum for multistakeholder dialogue, called the Internet Governance Forum. https://www.intgovforum.org

7 Souter, D. (2022, 21 June). Inside the Digital Society: Does internet governance require a reboot? *APC.* https://www.apc.org/en/blog/inside-digital-society-does-internet-governance-require-reboot

8 For example, at the UN World Summit on Sustainable Development (Johannesburg, August 2002), the failure of global financial, trade and environmental governance to effectively manage the uneven effects of globalisation featured prominently. The outcome document emphasised the need for all levels of policy formulation and decision making to be inclusive of developing country voices and also called for strengthened partnerships with civil society. Johannesburg Declaration on Sustainable Development, 2002, paragraph 26. https://www.un.org/esa/sustdev/documents/WSSD_POI_PD/English/POI_PD.htm

9 Various. (2005). *"Much more could have been achieved": Civil Society Statement on the World Summit on the Information Society.* https://waccglobal.org/wp-content/uploads/2020/07/Much-more-could-have-been-achieved.pdf

10 For example, the regional WSIS action plans in Africa and Latin America and the Caribbean.

11 Developed by the Brazilian Internet Steering Committee in 2009. https://www.cgi.br/principles

and Proportionate Principles on the Application of Human Rights to Communications Surveillance,[12] the Charter of Human Rights and Principles for the Internet,[13] the African Declaration on Internet Rights and Freedoms,[14] the Manila Principles on Intermediary Liability[15] and the Feminist Principles of the Internet.[16] The Code of Good Practice on Information, Participation and Transparency in Internet Governance[17] was developed by APC with the Council of Europe and the United Nations Economic Commission for Europe, and civil society contributed to the milestone Human Rights Council resolution of 2012 that affirmed that human rights that apply in the "offline world" also apply online.[18]

Civil society invested time and resources in the IGF's Multistakeholder Advisory Group (MAG), in IGF intersessional work (Dynamic Coalitions and Best Practice Forums) and, in 2011 at the Nairobi IGF, initiated the "day zero" tradition of having linked events on the day before the official IGF programme. Several of the national, regional and youth IGFs (NRIs) that emerged from 2008 onwards were initiated by civil society groups and contributed to them building closer relationships with national governments and regional intergovernmental institutions.

This WSIS- and IGF-inspired multistakeholder public policy engagement "bubble" reached a peak in 2014 with the NETmundial,[19] a response to the shock of the Snowden revelations and the controversy around the Internet Assigned Numbers Authority (IANA) transition. It was hosted and organised by the then left-leaning government of Brazil with the technical community, in close collaboration with civil society, governments and the academic and business sectors. The resulting NETmundial Multistakeholder Statement[20] was drafted collaboratively, with all interest groups having to compromise to some extent. Several civil society actors were not fully happy with the NETmundial process and outcome documents, which they felt favoured the "core interests of the most resourceful parties, which, at the global level, are often the US and big business."[21] However, the vast majority accepted the outcome and celebrated its strong commitment to the internet as a global public resource that should be managed accordingly, and to the emphasis given to openness, transparency, inclusion and human rights.

To date, NETmundial remains the largest and most inclusive multistakeholder process for distilling principles for internet governance. Its innovative process enabled collective and transparent drafting, with contributions from 1,480 stakeholders from 97 countries collected via an online platform, followed by face-to-face negotiation and consensus building.

Sadly, and despite receiving widespread endorsement, the NETmundial principles were never systematically promoted, "socialised" and legitimated by the stakeholders that negotiated them. Nor did they move from the multistakeholder into the multilateral space – in fact, some UN member states actively opposed formal recognition of the NETmundial principles in UN forums.[22] The work of consolidating principles for governing the internet – once a core theme at the IGF – came to a halt.

NETmundial did have impact. The IANA transition, one of the most controversial internet governance processes of the post-WSIS era, benefited from both the NETmundial process – which outlined a roadmap for the transition – and the IGF, as a platform for providing broader, and global South, engagement. NETmundial also proves that collective multistakeholder drafting of text is possible, even if not easy.

But would the NETmundial principles, if they had been globally socialised and adopted by both multilateral and multistakeholder decision-making forums, have enabled a more coherent public interest and human rights-centred approach to internet governance? Would this have helped harmonise the spate of national-level internet-related regulation that has emerged in the last few years, and as such, safeguarded the internet as a global public resource from fragmentation produced by the actions of internet companies and national governments? Would current efforts to regulate corporate behaviour on the internet have been more global and cooperative, as opposed to fragmented along geopolitical, regional or national lines? Perhaps or perhaps not;

12 Developed by the Electronic Frontier Foundation and a coalition of NGOs in 2013-2014. https://necessaryandproportionate.org/principles

13 Developed by the IGF Internet Rights and Principles Dynamic Coalition in 2011. https://internetrightsandprinciples.org/charter

14 Drafted in 2014 as a Pan-African initiative to promote human rights standards and principles of openness in internet policy formulation and implementation on the continent. https://africaninternetrights.org

15 Developed through an open, collaborative process conducted by a broad coalition of civil society groups and experts from around the world in 2015. https://manilaprinciples.org/index.html

16 Originally drafted in 2014 at the first Imagine a Feminist Internet in Malaysia, organised by APC. https://feministinternet.org

17 https://www.apc.org/en/projects/code-good-practice-information-participation-and-t

18 "The promotion, protection and enjoyment of human rights on the Internet", A/HRC/RES/20/8, resolution adopted by the UN Human Rights Council on 16 July 2012. https://digitallibrary.un.org/record/731540?ln=en

19 https://netmundial.br

20 https://netmundial.br/netmundial-multistakeholder-statement

21 Just Net Coalition. (2014, 5 May). The JNC Response to the NETmundial Outcome Document. *ALAI*. https://www.alai.info/85299-2

22 Evident in, for example, discussions at the UN Commission on Science and Technology for Development (CSTD) on WSIS follow-up and the resulting Economic and Social Council (ECOSOC) resolution in 2015.

but having some soft law instruments that expanded on the WSIS principles would definitely have provided – at least in the context of UN processes – a more focused and potentially influential global approach to discussing solutions to emerging internet-related policy and regulation challenges.

The present

Today, internet-related issues are priorities on many policy agendas. Having grown from 1.1 billion users in 2005 to more than four billion users today,[23] the internet is at the centre of a process of digitalisation that is transforming the workplace, social and political processes, business and trade, as well as people's personal lives, a transformation accelerated by COVID-19.

However, several of the challenges that were on the table during the WSIS remain unresolved. For example, access to the internet remains unequal, between and within countries and regions. The availability and affordability of infrastructure and devices, local content in local languages, and the human capacity needed to reap the benefits of using the internet are "old challenges". On the other end of the spectrum, many new challenges have emerged and are emerging from hyper connectivity and the resulting dependence on internet-based systems and services. With new opportunities come new threats and risks. Datafication, surveillance-based business models, artificial intelligence, machine learning and automated decision making, cybercrime, mis- and disinformation and harmful content create a whole new range of challenges and policy questions.

Internet governance is no longer a stand-alone discipline but has become part of broader "digital governance" and "digital transformation". The range of internet-related policy and regulation issues continues to expand, cross borders, and intersect with other spheres. Linked to this is a proliferation of venues. Some are new, such as the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes,[24] but many pre-date internet governance, for example, national legislatures, telecoms regulatory bodies, trade organisations, competition commissions and human rights institutions. What is new is that they have to give serious attention to internet-related aspects of their areas of work. This constitutes a challenge in its own right, particularly for civil society organisations who lack the human and financial resources required to follow all these processes effectively.

COVID-19

The early 2020s will always be associated with the COVID-19 pandemic, a global crisis which affected almost everyone everywhere, in developed and developing countries. The severity of the pandemic's impact depended on multiple factors, but four of these are worth noting, because they contain lessons learned that are also relevant to internet governance. They are equitable and sustainable development; publicness (as in resilient public infrastructure and services); coordinated collaboration; and trust and human rights.

First, **equitable and sustainable development**. As the World Health Organization (WHO) recently put it:

> The pandemic has laid bare the social fractures in our societies and it is no longer possible to ignore the fact that many people are struggling to live a decent and dignified life and are unable to meet essential needs for safe and secure shelter, food, fuel and income. The coexistence of material deprivation and discrimination by gender, race and religion have emerged in the risks of infection, excess loss of life, and growing poverty and poor health faced by ethnic minorities, women, informal workers, and the poor and vulnerable.[25]

Digital equity proved to be vital for accessing information, education and culture, for staying in touch with friends and family, and for people to be able to continue working to earn a living. Access to the internet and the ability to use it in a meaningful way[26] softened the social, psychological and economic impact of lockdowns and quarantine, and the impact of *not* having access became starkly visible, which highlighted the need for digital inclusion.

But achieving equitable and sustainable digital development is not easy. As the extent and sophistication of internet-based transactions and applications increase, those without the needed devices, bandwidth and skills tend to fall even further behind, and the digital inequality actually

23 According to data from the International Telecommunication Union (ITU), 50% of the world population (around four billion people) used the internet at the end of 2019. Other sources, such as Internet World Stats, put the mid-2021 figure at well over 4.5 billion. ITU. (2020). *Measuring digital development: Facts and figures 2020*. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf

24 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

25 WHO. (2022, 7 July). WHO encourages stakeholders to embed health equity in COVID-19 recovery plans. https://www.who.int/europe/news/item/07-07-2022-who-encourages-stakeholders-to-embed-health-equity-in-covid-19-recovery-plans

26 Which in turn relates to issues such as skills, affordability, quality of broadband internet connectivity, etc.

increases. In addition, increased digitalisation, once seen as a more sustainable alternative to industrialisation, has become a contributor to climate change, pollution and habitat destruction through massive energy use, electronic waste and its dependency on rare minerals, the mining of which has fuelled conflict and damage to sensitive ecosystems (e.g. the sea bed). Internet and digital governance, policy and regulation need to consider the impact of innovation and growth on people, communities, biodiversity and the natural environment.

Second, and linked to equitable and sustainable development, is **"publicness"** and resilient public services and infrastructure. Under-investment in resilient public health systems[27] left national and global health authorities struggling to respond effectively to the crisis. Once vaccines became available, the ability of health services to manage the vaccination supply chain, from procuring vaccines, to communicating with the public, to storing, delivering and administering vaccinations, impacted on economic recovery and a return to normal life. Dependency on the internet during the pandemic revealed under-investment in internet infrastructure and services. Many people did not have reliable broadband access, particularly in rural areas. Despite being a priority since the WSIS, enabling policy and regulation to expedite universal access are still not in place in many parts of the world. While some countries approach access to the internet as essential, and even as a right, others have introduced new barriers, for example, through taxation of social media and voice over IP (VoIP) service or through internet shutdowns.

Much internet infrastructure is built and maintained by the private sector and the technical community, which is a characteristic of internet infrastructure, and a primary reason for its governance being multistakeholder. However, this does not, and should not, negate the need for such infrastructure to be incentivised and regulated in the public interest and for the internet to be understood and protected as a commons or public good.

Third, **coordinated collaboration**. Around the world, the effort to address the pandemic and prevent it from getting worse was marred by insufficient international and multistakeholder coordination and collaboration. The already insufficient resources (and capability) of the WHO were exacerbated by the United States' withdrawal of support (since reversed by President Biden) and former President Trump's consistent public attacks on the institution and its leadership.[28] Even the expansive regulatory machinery of the European Union could not produce clear and coordinated responses on vaccine approvals, lockdowns or travel restrictions.[29] With respect to vaccine development, the complexity resulting from so much COVID-19-related research and development being led by the private sector had not been anticipated. When it was most needed, there was simply not enough active coordination or collaboration between public and private health and pharmaceutical authorities and regulators. Neither government nor business seemed to engage the media and civil society sufficiently, and they rarely presented common positions. This created a climate of uncertainty, prone to mis- and disinformation and an overall trust deficit, which made responding to the pandemic more difficult.

Effective internet governance also relies on cross-border multistakeholder and multilateral collaboration. This too lacks a clear and coordinated commitment by both public and private sector actors to protecting and governing the internet as a global commons or public good. Increasingly, people's use of the internet – and access to news and information – takes place through privately owned, commercial platforms. As pandemic-related panic set in, mis- and disinformation were spread on social media.[30] The response from platforms was delayed at best, and often inadequate. From states it was often rushed and overly aggressive. Several used the pandemic to justify legislation that criminalised COVID mis- and disinformation online, using vague definitions that endangered freedom of expression, particularly people's freedom to challenge state responses to the crisis.[31]

27 In general, but with multiple issues that relate to internet governance challenges, such as connectivity to exchange data and information between public health institutions, collect data, adequately inform and sensitise the general public, manage vaccination campaigns, etc.

28 KFF. (2022, 19 May). The U.S. Government and the World Health Organization. https://www.kff.org/coronavirus-covid-19/fact-sheet/the-u-s-government-and-the-world-health-organization

29 Springall, J. (2022, 5 March). How will we ever overcome the confusion and complexity of COVID-19 travel? *Euronews*. https://www.euronews.com/travel/2022/03/05/how-will-we-ever-overcome-the-confusion-and-complexity-of-covid-19-travel

30 https://www.poynter.org/ifcn-covid-19-misinformation

31 Fish Hodgson, T., Farise, K., & Mavedzenge, J. (2020, 5 April). Southern Africa has cracked down on fake news, but may have gone too far. *Mail & Guardian*. https://mg.co.za/analysis/2020-04-05-southern-africa-has-cracked-down-on-fake-news-but-may-have-gone-too-far; Dushyant, & Manzar, O. (Eds.) (2020). *The New Normal: How to Survive a New World Order*. Digital Empowerment Foundation. https://www.defindia.org/wp-content/uploads/2021/02/The-New-Normal-Full-Book-by-DEF.pdf

This brings us to the fourth factor, **trust and human rights**. Many governments underestimated the importance of building trust through strengthening their own public information and communication systems. Trust was further undermined by rushed COVID contact-tracing solutions, which in some cases were introduced without data protection frameworks being in place and were rolled out in a manner that could be described as "surveillance by stealth". What data was collected, where and how long it was stored, and how it was processed and used were often unclear, including who had access to the data or with whom data and results were shared.[32]

The trust deficit during the pandemic existed at multiple levels, between countries, between citizens and states, between private and public health care entities, and between consumers and corporations. Trust is intrinsically linked to human rights. One of the most profound characteristics of the human rights framework that has evolved over the last 75 years is that it puts individuals at its centre, not citizens. As duty bearers for upholding and promoting human rights, all states have the responsibility to do so for all of humanity, not just for their citizens. One can argue that one of the weaknesses in the global response to COVID-19 was that it followed national, citizen-oriented lines, rather than being rooted in international collaboration aimed at protecting and supporting humanity at large. Internet governance too needs to be grounded in international human rights laws and standards as a means of avoiding harms, exclusion and fragmentation.

Internet governance of the future

The future of internet governance is often presented in binary terms,[33] a trend reinforced by the conflict in Ukraine, and described recently by Alex Klimburg and others as two alternate futures:

> In the best case, the world can hope for a bright, stable digital future, with different parts of cyberspace working in tandem and available globally, and where international cooperation makes it increasingly safe and secure. The alternate vision is bleaker: a "splinternet" of competing internets and walled gardens, where cybercrime is rife, and the calamitous threat of civilization-crashing cyberwar is ever-present.[34]

The problem with binary views of the future of the internet is two-fold. First, they overlook the diverse reality that characterises how people today (can) use and experience the internet. The idealised "free and open internet" has never existed for people who have no access or intermittent, poor quality access, for people who have to spend more than 20% of their monthly household income for broadband, or who live in countries where the government shuts down the internet unilaterally. Second, binary rhetoric to describe the future of the internet, particularly when repeatedly expressed by government representatives in international forums, could become self-fulfilling prophecies contributing to and accelerating the very polarisation they predict. Jason Pielemeier and Chris Riley point this out in their critique of a recent report by the US Council on Foreign Relations[35] that declared the era of the global internet as being over:

> The internet is a network of networks, and despite the advanced information controls imposed in some jurisdictions, its technical design – including the critical Internet Protocol and Border Gateway Protocol – [is] designed to maintain interconnection above all else. Separating countries into friends and enemies also, ironically, buttresses the long-standing goals of China, Russia, Iran, and other authoritarian regimes to center internet governance in "cyber sovereignty" rather than internationally protected human rights.[36]

32 The WHO published an excellent set of guidelines on contact tracing in February 2021. These guidelines emphasise the human component of contact tracing, warn of risks to individual privacy and security, and state very clearly that it is not necessarily the most appropriate response: "Contact tracing efforts need to be balanced against other resource requirements, and the impact of contact tracing should be assessed relative to other health interventions. Planning for contact tracing includes ensuring that the costs of setting up and maintaining an effective system are secured and that the social and economic consequences of quarantine are addressed for affected individuals." WHO. (2021, 1 February). Contact tracing in the context of COVID-19: Interim guidance. https://apps.who.int/iris/bitstream/handle/10665/339128/WHO-2019-nCoV-Contact_Tracing-2021.1-eng.pdf

33 At the 2018 IGF held in Paris, at UNESCO, President Macron posited the idea of the "internet of California", self-regulated by companies against the "internet of China", controlled by government. He proposed a middle way where governments work with other stakeholders to regulate the internet "properly". See: https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron

34 Klimburg, A., Perucica, N., & Dobrygowski, D. (2022, 24 May). How to safeguard the internet after the war in Ukraine. *World Economic Forum*. https://www.weforum.org/agenda/2022/05/safeguarding-the-internet-post-ukraine

35 Segal, A., Goldstein, G. M., & Schmemann, A. (2022). *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*. Council on Foreign Relations. https://www.cfr.org/report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf

36 Pielemeier, J., & Riley, C. (2022, 1 September). In Defense of the Global, Open Internet. *Lawfare*. https://www.lawfareblog.com/defense-global-open-internet-0

They continue:

> In a moment of historic expansion of internet connectivity, most governments around the world still haven't firmly established their position on the spectrum between an authoritarian and freedom-centric approach to internet governance. If the United States, in particular, portrays the future of the internet as inevitably isolationist, it is as likely to push governments *toward* authoritarian models as it is to incentivize governments away from them.[37]

Is there a way forward for internet governance that avoids binary thinking and reaffirms the internet as an interconnected, interoperable network and, ultimately, a global public resource? Is there a role for the IGF, which will be convening for the 17th time this year?

The IGF is being questioned for not effectively producing outcomes that feed into policy processes. This critique, while not entirely without merit, has unfortunately resulted in undervaluing the IGF's long-term impact as a platform for networking, learning, and open dialogue and debate. The reality is that in a world where many governments have never given full support to the idea of multistakeholder global governance, and many more have inconsistent human rights records, the IGF succeeded as an inclusive and open forum covering all aspects of internet governance, including human rights and the multistakeholder approach.

Critiques of the IGF, particularly by states, can also be seen as a reflection of a nascent shift away from mainstreamed and substantive commitments to establishing global, cooperative, inclusive, multistakeholder internet governance. Governments that were foremost among those that championed inclusive, multistakeholder, human rights-oriented internet governance now seem to advance an "us against them" approach in relation to "non-like-minded" states, rather than systematically joining forces with civil society and other non-state actors to seek common ground and strive for cooperation.

Conclusions and call to action

There are no shortcuts to achieving the inclusive, people-centred, human rights-oriented information society that civil society organisations have envisaged since the WSIS. Realising this vision requires a holistic approach that considers the factors discussed above: equitable and sustainable development, the publicness of the internet, coordinated collaboration, and trust and human rights. To do so, civil society should take stock, analyse and prioritise, and do so collaboratively – within civil society, but also with other sectors/stakeholder groups.

Take stock and prioritise. Assessing progress, success and setbacks of the last 20 years is a good basis for civil society from the global South and North to collaborate and plan future action. The Global Digital Compact, the Summit of the Future, cybersecurity processes and WSIS+20 are opportunities. The diversity within civil society might not allow achieving complete consensus about everything, but that should not matter. Gathering together to assess the past, share perspectives and look at the main developments in different policy spaces that affect internet governance will provide building blocks for this holistic view and approach. There are bound to be areas of commonality that can underpin some form of collective input into formal policy processes.

Invest in, and demand, inclusive multilateral and multistakeholder governance processes. In 2003 civil society proposed that "[p]rocedurally, decision-making processes must be based on such values as inclusive participation, transparency, and democratic accountability."[38] These words are still relevant today across the board of multilateral, multistakeholder, and national or industry-level internet-related policy and regulatory processes. Division within civil society on whether it should support the multistakeholder approach or not has been unproductive. What matters is how transparent, inclusive, participative and accountable any policy process is. Lack of transparency and accountability can hide and enable capture by vested corporate or national interests. The multistakeholder approach is not a substitute for effective multilateral governance. We need both multistakeholder and multilateral processes, and both need to be more effective and inclusive. Sadly, the recently published draft modalities for the upcoming Summit of the Future,[39] a multilateral process that claims it will facilitate multistakeholder input, suggests that opportunity for non-state actor engagement will be limited and constrained. Civil society's only way of working around that is to work collaboratively, particularly during the preparation for the Summit.

37 Ibid.

38 WSIS Civil Society Plenary. (2003). *"Shaping Information Societies for Human Needs": Civil Society Declaration to the World Summit on the Information Society*. https://www.itu.int/net/wsis/docs/geneva/civil-society-declaration.pdf

39 United Nations General Assembly. (2022, 7 September). Draft resolution submitted by the President of the General Assembly: Modalities for the Summit of the Future. A/76/L.87. https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/76/L.87&Lang=E 2022. https://daccess-ods.un.org/tmp/2137181.31184578.html

Challenge fragmentation of the internet *and* of internet governance. Internet-related regulation is here to stay, whether it is intended to reduce online harm, regulate corporate behaviour, hold platforms accountable for disseminating false information, or combat cybercrime. Walled gardens, national firewalls, censorship, surveillance, shutdowns and the exploitation of personal data are all part of today's internet and go against the ideal of one unfragmented internet. At the same time, faith in the value of open and inclusive dialogue, and in the IGF as a platform to facilitate such a dialogue, seems to be in decline, fuelled by "new cold war" discourse. But this does not need to be the case. The open internet's core protocols continue to enable interoperability and interconnection to all those who have access to it. Civil society can counter fragmentation of the internet and of internet governance by advocating for and participating in collaborative coordination, and policy and regulation that harmonise across borders, building on common existing international norms and principles (spanning the fields of human rights, social justice, peace and sustainable development) as a foundation.

Reuse, mix and remix. When it comes to formulating positions, principles and norms, there is a vast body of work already done by civil society itself, as well as by other stakeholder groups, such as the UN First Committee's Group of Governmental Experts' norms on responsible state behaviour in cyberspace. Adapting to context changes and being agile is crucial in the digital space, but it is not necessary to go back to the drawing board empty handed. The statements and principles cited above, along with tools such as UNESCO's Internet Universality Indicators,[40] are all valuable. So are ones not yet mentioned such as the Just Net Coalition's Delhi Declaration,[41] or the Communication Rights in the Information Society (CRIS) Campaign's handbook on assessing communication rights,[42] more recent norms and guidelines focused on platform governance or human-centric cybersecurity, or the human rights-based approach (HRBA). The HRBA is not just about human rights and building trust. It is an approach that builds on the norms and principles outlined in the Universal Declaration of Human Rights, and the subsequent legally binding UN treaties, but it also challenges unequal power relations and social exclusion. Many governments are familiar with this approach through the EU Consensus on Development agreement[43] and the UN Common Understanding of the HRBA.[44] This means that civil society has a common language to draw on when using the HRBA in internet policy processes. Its core elements are captured by the acronym PLANET: participation; links to human rights obligations; accountability; non-discrimination; empowerment and capacity development; and transparency. Sida recently published two helpful guides to using this approach in digitalisation and internet policy and development.[45]

Find and mind the gap. Assessing past work is also a way of identifying gaps. For example, early civil society documents, and the NETmundial statement, refer to the internet as a public resource, or a public good. The Global Commission on the Stability of Cyberspace proposed the norm to protect the public core of the internet.[46] The UN Secretary-General highlights the need for digital public goods in his *Our Common Agenda* report.[47] But no one has explored systematically what the normative implications of approaching the internet itself as a commons would be for policy and regulation. Civil society should consider whether there are pivotal shifts needed to redirect the trajectory of internet governance away from becoming contested terrain between states and corporations, and help it move towards protecting the internet as a global public good or commons, to be governed in the public interest based on international human rights norms. In this context, civil society could consider and propose possible instruments, for example a UN-based framework agreement that captures the WSIS principles in a way that can be used to hold states accountable for upholding them. Gaps can also be more specific, and addressed as such – for example, norms for online advertising and content moderation during elections to enhance trust and prevent manipulation and that can be used to hold companies and political parties accountable.

40 https://www.unesco.org/en/communication-information/internet-governance/internet-universality-indicators

41 https://justnetcoalition.org/delhi-declaration

42 CRIS Campaign. (2005). *Assessing Communication Rights: A Handbook*. https://archive.ccrvoices.org/cdn.agilitycms.com/centre-for-communication-rights/Images/Articles/pdf/cris-manual-en.pdf

43 https://international-partnerships.ec.europa.eu/policies/european-development-policy/european-consensus-development_en

44 UN Sustainable Development Group. (2003). *The Human Rights Based Approach to Development Cooperation: Towards a Common Understanding Among UN Agencies*. https://unsdg.un.org/resources/human-rights-based-approach-development-coordination

45 Sida. (2022). *Human Rights Based Approach and Digitalisation*. https://cdn.sida.se/app/uploads/2022/05/03092839/10205933_Sida_TN_HRBA_Digitalisation_webb.pdf; Sida. (2022). *HRBA and a Free, Open and Secure Internet*. https://cdn.sida.se/app/uploads/2022/05/03093124/10205933_Sida_TN_HRBA_Secure_Internet_webb.pdf

46 https://hcss.nl/gcsc-norms

47 https://www.un.org/en/common-agenda

Context matters. For civil society, an equitable, inclusive public and human rights-oriented internet is not an isolated goal. As civil society engages in internet governance of the future, it must stay aware and engaged with working for social and economic justice, gender equality, peace and environmental sustainability – locally and globally. David Souter recently pointed out:

> Technology's development's not independent of what's happening in the wider world around it. External circumstances – individual events, changes in the way we live, trends in geopolitics – affect digital development just as much as digital development affects the wider world.[48]

Staying connected to the "wider" world means, for example, being connected to local issues and contexts, networking with communities and community-based organisations, and interacting with national, regional and local government. It means working collaboratively but also being constructively critical, by asking questions rather than making assumptions; by listening to people who are affected directly by issues discussed in policy spaces; by building alternative solutions and working in partnership; by caring for our planet and all lives; and by carefully evaluating – and acting on – the impact of digitalisation on the environment as well as how digitalisation can help to mitigate climate change and manage its effects.

48 Souter, D. (2022, 20 July). Inside the Digital Society: What impact has COVID had in practice? *APC*. https://www.apc.org/en/blog/inside-digital-society-what-impact-has-covid-had-practice

GLOBAL INFORMATION SOCIETY WATCH 2021-2022

DIGITAL FUTURES FOR A POST-PANDEMIC WORLD

Through the lens of the COVID-19 pandemic, this edition of Global Information Society Watch (GISWatch) highlights the different and complex ways in which democracy and human rights are at risk across the globe, and illustrates how fundamental meaningful internet access is to sustainable development.

It includes a series of thematic reports, dealing with, among others, emerging issues in advocacy for access, platformisation, tech colonisation and the dominance of the private sector, internet regulation and governance, privacy and data, new trends in funding internet advocacy, and building a post-pandemic feminist agenda. Alongside these, 36 country and regional reports, the majority from the global South, all offer some indication of how we can begin mapping a shifted terrain.

GLOBAL INFORMATION SOCIETY WATCH
2021-2022 Report
www.GISWatch.org

APC

Sida