GISWatch
SPECIAL EDITION

GLOBAL INFORMATION SOCIETY WATCH 2024
SPECIAL EDITION

WSIS+20: Reimagining horizons of dignity, equity and justice for our digital future

Association for Progressive Communications (APC),
IT for Change, WACC Global
and Swedish International Development Cooperation Agency (Sida)

Global Information Society Watch 2024 SPECIAL EDITION
WSIS+20: Reimagining horizons of dignity, equity and justice for our digital future

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)

Publication production support
Cathy Chen (APC)

Graphic design
Monocromo

Cover illustration
Matías Bervejillo

We would like to extend a special note of thanks to authors who have made ad honorem contributions to this edition of GISWatch.
We gratefully acknowledge the following: Ana Neves (Fundação para a Ciência e Tecnologia – Unidade FCCN)
APC would like to thank the Swedish International Development Cooperation Agency (Sida), IT for Change and WACC Global for their support for this Global Information Society Watch 2024 special edition.

Published by APC
2024

Global Information Society Watch 2024 Special Edition web and e-book
ISBN: 978-92-95113-67-1
APC-202404-APC-R-EN-DIGITAL-357

Disclaimer: The views expressed herein do not necessarily represent those of Sida, IT for Change, WACC Global, APC or its members.

The role of governments in policy and regulation in the digital sphere: An academic perspective

Wolfgang Kleinwächter
European Summer School on Internet Governance
https://eurossig.eu/eurossig/

Although the history of the internet goes back to the 1960s, governments did not see the internet as a political issue for many years. This has changed dramatically. In the 2020s, everything is now "cyber" or "digital": from the global economy to the wars in Gaza and Ukraine, from sustainable development to the protection of human rights. The internet is on the agenda of the United Nations (UN). It is discussed by the leaders of the G20, G7 and BRICS. There are endless diplomatic negotiations on related issues. And there are hundreds of cyber and digital conferences, including the Internet Governance Forum (IGF), where stakeholders from around the world are trying to identify issues, to develop policies and to solve problems. In the "2024 Security Index" of the Munich Security Conference (MSC), the perceived threat of instability in cyberspace ranks second behind climate change.[1]

The mothers and fathers of the internet, who are now grandmothers and grandfathers, were interested primarily in developing a technical environment to enable people to communicate freely. Security was not a number one issue. But their inventions did have political, economic, cultural, social and legal implications. And their grandchildren are now struggling with a commercialised and politicised internet, which is today's nerve centre of a globalised, but more and more fragmented and also polarised world.

In 2019, the UN High Level Panel on Digital Cooperation (HLP) labelled our time as the "age of digital interdependence".[2] In this age, the challenge is to both protect free communication and promote a secure cyberspace. If more than five billion people are now driving on the global "Information Superhighway", it needs "rules of the road" to avoid anarchy and a digital jungle.

Law making is primarily a responsibility of governments. However, in the information age, where everything and everybody is interconnected, law making is very complex. It needs more than governmental executive power and parliamentarian majorities. It needs the involvement of all stakeholders from business, civil society, academia and the technical community to build sustainable regulatory frameworks.

The "information revolution" has created a new global complexity with new contradictions. Manuel Castells told us already in 1998 that in a "Network Society" there is a conflict between "borderless spaces" and "bordered places".[3] And indeed, the borders of time and space have disappeared, but the borders among nations and in our minds continue to exist. To deal with this contradiction, we need a "double strategy" which recognises both the global nature of digital interdependence and respects the sovereignty of nation states as well as differences in political cultures.

Contradictions can be barriers for innovation, but also drivers for development. To find sustainable solutions for the new issues of the digital age – cybersecurity, artificial intelligence (AI), quantum computing, etc. – there is no alternative to a holistic approach and the involvement of all stakeholders. Looking for special solutions in separated silos will have unintended side effects. Excluding affected and concerned stakeholders will backfire. In other words, regulation in cyberspace is no longer a question of "yes" or "no"; it is a question of "how" and "who".

[1] Bunde, T., et al. (2024). *Munich Security Index 2024*. MSC. https://securityconference.org/en/munich-security-report-2024/munich-security-index-2024

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

[3] Castells, M., & Cardoso, G. (Eds.). (2005). *The Network Society: From Knowledge to Policy*. Johns Hopkins Center for Transatlantic Relations. https://www.dhi.ac.uk/san/waysofbeing/data/communication-zangana-castells-2006.pdf

From the myth of the early days to the new internet governance complexity

The myth of the early days of the internet, that the "network of networks" is a "virtual space" which is separated from "real places", fed an illusion that there is no need for regulation and it is enough to respect "netiquette". Futuristic visions, developed by William Gibson, John Perry Barlow and others, like the "Declaration of the Independence of Cyberspace"[4] or the "Cluetrain Manifesto",[5] helped to open our eyes to the "silent internet revolution" in the 1990s. But they also promoted misunderstandings and confusion about freedom and responsibilities, rights and duties, legitimacy and accountability in cyberspace.

The internet broadened individual freedom, created new economic opportunities and challenged existing regulatory frameworks. But what happened online was still subject to existing national and international legislation. The internet removed the barriers of time and space, it allowed innovation without permission, it enabled individual users to become global players; but this new freedom never included the freedom to steal money or to harm other people. What was illegal offline became illegal online.

In the 1980s and 1990s, the internet became more prominent in policy discussions in the United States, which were dominated by concepts of "deregulation" (under the Reagan administration, 1980-1988) and "private sector leadership" (under the Clinton administration, 1992-2000). The idea was to reduce the role of governments to that of "moderators" or "facilitators" and leave internet policy development and decision making in the hands of affected and concerned stakeholders, such as those from the technical community and innovative business players who developed the so-called "new economy".

This approach, which triggered the "dot-com boom" of the 1990s, enabled the fast development of the internet as a global infrastructure. Neither national parliaments nor international diplomatic codification conferences were involved in the making of TCP/IP[6] or the Domain Name System (DNS). When Jon Postel delegated the management of country code top-level domains (ccTLDs) to more than 100 countries, no government was involved. It was done by Postel himself via a handshake with a trusted manager. Internet governance mechanisms evolved in the shadow of governmental regulation.

But the regulatory mechanisms for the internet developed by the technical community are rather different from traditional public law making. Internet standards and codes, described in Requests for Comments (RFCs) documents produced by the Internet Engineering Task Force (IETF), are not the result of top-down decisions or majority voting of elected parliamentarian representatives. They are drafted "bottom-up" by respected and competent key players of the global internet community and adopted through "rough consensus". It is "humming",[7] not "voting". The number of RFCs has grown since 1969 to more than 10,000. This is the "Internet Lawbook".[8]

This coexistence of the "two worlds" worked quite well. The internet community was small and did not touch political controversies. This changed with the digitalisation of nearly all areas of daily life.

WSIS: A new approach to global problems

The first global policy response to the emerging internet challenges started in 2001 with the UN World Summit on the Information Society (WSIS). In his opening speech to the WSIS Geneva Summit in 2003, UN Secretary-General Kofi Annan pointed out:

> This Summit is unique. Where most global conferences focus on global threats, this one will consider how best to use a new global asset. We are going through a historic transformation in the way we live, learn, work, communicate and do business. We must do so not passively, but as makers of our own destiny.

And he added:

> Yet even as we talk about the power of technology, let us remember who is in charge. While technology shapes the future, it is people who shape technology, and decide what it can and should be used for.[9]

What in 2003 was "the future" is now the reality. But while times have changed, the problems are more or less the same. It therefore makes sense to look back and remember the lessons learned.

[4] Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace*. https://www.eff.org/de/cyberspace-independence

[5] https://www.cluetrain.com

[6] Communication protocols used to interconnect network devices.

[7] Resnick, P. (2014). *On Consensus and Humming in the IETF*. Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc7282

[8] https://www.ietf.org/standards/rfcs

[9] United Nations. (2003, 11 December). WSIS opening meeting discusses how digital divide is preventing equal sharing of opportunities concerning ICTs. https://press.un.org/en/2003/pi1541.doc.htm

WSIS became the first clash of cultures in the information age. For the first time in UN history, business, civil society, academia and the technical community were officially invited as participants to a UN summit. However, it was unclear how governments and non-governmental stakeholders could work hand-in-hand by developing policies for the digital age.

It was a complicated process. Governments realised that the internet was much more complex than previous communication technologies like telecommunications or broadcasting, which were regulated by national laws. Cross-border issues such as frequency coordination were negotiated among governments in conventions and led to the establishment of intergovernmental organisations like the ITU, WIPO or UNESCO.

The borderless, decentralised and open network architecture of the internet is very different from the hierarchical structures of broadcasting and telecommunication. With the internet, everybody is both sender and receiver (the end-to-end principle). There is no "central authority". Various groups of mainly private developers, providers and users of internet services manage parts of the whole infrastructure and communicate, coordinate and collaborate both informally and formally by sharing rights, duties and responsibilities voluntarily. Nobody controls everything. IETF does protocols, ICANN the DNS, regional internet registries (RIRs) and IP addresses, and the Internet Society (ISOC) discusses concepts.

The reality is that it is difficult to separate "real places" and "virtual spaces". Every virtual communication among netizens starts and ends with a real citizen. The challenge is to bring these two worlds together. It sounds simple, but the best way forward is to enhance cooperation between law makers and code makers. This is easier said than done.

WSIS produced a broad range of different ideas. Extreme positions on both sides of the spectrum contributed to a growing internet governance controversy. Concepts of private sector-led self-regulation conflicted with the call for strong governmental regulation, with a broad variety of mixed, multidimensional policy concepts and co-regulatory ideas in between.

What WSIS finally produced in its Tunis Agenda for the Information Society (2005) was a remarkable "grand compromise", based on a concept of "grand collaboration". The Tunis Agenda recognised that "policy authority for Internet-related public policy issues is the sovereign right of States." And it also recognised:

> [T]he 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.[10]

The Tunis Agenda made clear that governance in the information society needs the involvement of all stakeholders "in their respective roles". This formula, with its diplomatic ambiguity, allowed a differentiated approach. Each stakeholder has a special role, but no stakeholder can act alone or substitute another stakeholder. The conflict between "governmental leadership" and "private sector leadership" was solved by recognising that the information society doesn't need "leadership", but the collaboration of all stakeholders.

The agreement on the multistakeholder approach, which was one of the main WSIS outcomes, recognised that governments, business, civil society and the technical community have different but complementary roles, interests and capacities. Rule making by governments will fail if they don't engage and ignore the wisdom of affected and concerned non-state actors, including civil society. Leadership by the private sector alone will fail without rules, which guarantee stability, fair competition and respect of human rights.

However, there is no single multistakeholder model. The Tunis Agenda calls for "shared principles, norms, rules, decision-making procedures, and programmes". But it did not agree on a procedure, nor how stakeholders should interact. How deeply different stakeholders should be involved in policy development and decision making remains unclear and depends to a high degree on the specific subject. There is no "one-size-fits-all".

It is very natural that governments play a strong role in international cybersecurity. And it is also understandable that the technical community plays a leading role in internet standards. But it would be unwise if governments in cybersecurity negotiations ignore advice from non-state actors. And it would also be bad if governments do not raise their voices in discussions held by technical bodies, as they do via the Governmental Advisory Committee (GAC) within ICANN. Governmental ignorance is as bad as technical arrogance.

[10] https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

Governance *of* the internet and governance *on* the internet

The Tunis Agenda also differentiated between the "evolution" and the "use of the Internet".[11] This differentiation allowed another flexible approach to manage the interrelationship between internet-related technical and public policy issues. The UN Working Group on Internet Governance (WGIG), which was tasked by the WSIS Geneva Summit to produce a definition of internet governance, rejected the idea of a "narrow definition", which would have included only technical aspects, and proposed a "broad definition". The Tunis Agenda two years later recognised this broad definition, stating:

> 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.[12]

This is very relevant for today's discussion around new emerging issues such as the internet of things (IoT), cybersecurity, AI or social networks. There are calls now for data governance, AI governance, ICT governance, IoT governance, digital governance, cyber governance, platform governance, etc. But all these involve "using" the internet. Insofar as the essence of the broad WGIG definition – governance in the digital space needs the involvement of all stakeholders, and related processes have to be open, inclusive, transparent, bottom-up and human-centric – is also relevant for all the new digital issues, there is no need to reinvent the wheel.

Policies and regulation for AI, cybersecurity or social networks will fail if they are done behind closed doors, and are exclusive and top-down. And it will be impossible for governments to find sustainable solutions without non-governmental stakeholders. Certainly, there are specifics and it needs fine-tuning. But at the end of the day, it is the governance of the whole digital sphere that has to be multistakeholder, open, transparent, inclusive, bottom-up and human-centric.

Nevertheless, the internet is a layered system. Roughly said, it can be divided into the technical and political layers, and the transport and application layers. The "One World – One Internet" philosophy is rooted in the design of the universal internet identifiers and the common use of the same technical protocols (TCP/IP, DNS, BGP,[13] HTTP, IPv4 and IPv6, etc.) based on a unified but decentralised root and name server system. This differs from the application layer, where internet-related public policy issues are discussed.

The distinction between "evolution" and "use" of the internet allows us to differentiate between the governance *of* the internet and governance *on* the internet. It allows us to keep the internet unfragmented on the transport layer, but enables different approaches on the application layer. How governance works on these different layers is therefore necessarily different: on the transport layer, the technical community needs to lead and convene the discussions, with input from governments and civil society. Policy discussions for the application layer, though implemented by governments, can in theory be convened by any stakeholder. Therefore, what we call "internet governance" is not necessarily the same in all circumstances.

Nevertheless, internet governance, whatever the practicalities involved, needs to conform with the WSIS principles, as embedded in the general WSIS commitment, that an information society should be human-centric and development-oriented and has to be based on the respect of international law and human rights, as enshrined in the Charter of the United Nations (1945) and the Universal Declaration of Human Rights (1948).[14]

The message from WSIS was that governance in the information age needs co-regulatory models which take into consideration both the sovereignty of the nation state and the universality of global networks. Decisions have no formal legal status, but they are the substance of a policy, which, besides being human-centric and development-oriented, has to be adequate, efficient, accountable, predictable, fair, balanced, inclusive, safe and workable. And it must avoid the emergence of "responsibility holes" (cybersecurity weaknesses that no party has direct responsibility for) and "safe havens" for cybercriminals.

What is needed is a constructive co-existence among the different stakeholders, the development of innovative models of "co-governance". Such a multilayered, multiplayer mechanism of communication, coordination and collaboration is the best way to promote both stability and flexibility in the global internet governance ecosystem. The weakness of one partner in one area can be

[11] Ibid.

[12] Ibid.

[13] Border Gateway Protocol.

[14] https://www.itu.int/net/wsis/docs/geneva/official/dop.html

compensated by the strength of the other and vice versa. Policy and regulation become more and more issue-oriented, which means that for each topic a special governance model has to be designed.

Governments have to learn to share power with non-governmental actors, while non-state actors have to accept that they operate in a political environment of sovereign nation states. Governments have to understand that the legitimacy they get from national democratic elections today includes a greater international responsibility towards a global community. And stakeholders have to demonstrate that they understand that the rights and freedoms they are calling for are linked to duties and responsibilities.

From WSIS to the Global Digital Compact and WSIS+20

The world has changed in the last three decades. In the 1990s, the internet was primarily a technical issue with some political implications. In the 2020s, digital issues are big political problems with a technical component. Today our world is a digital world. Security means "cybersecurity", economy means "digital economy" and the UN Human Rights Council has stated that human rights have to be recognised both offline and online.

In just 30 years, the number of internet users grew from less than one million to more than five billion. The new emerging global internet infrastructure created a new environment for many public policy issues. Technology, economy and policy became more and more interwoven.

In the 1990s there were no smartphones, no social networks, no ChatGPT. Bridging the digital divide, managing domain names and access to the internet were top on the agenda. On today's political agenda are AI, IoT, platform regulation, digital oligopolies, sustainable development, cybercrime, cyberwar, digital trade and the protection of human rights like freedom of expression or privacy, among others.

The "old issues" are still on the table, but what we have seen is a fundamental shift from technical-dominated to political and economic-dominated discussions. When the Tunis Agenda was adopted in 2005, only a small number of intergovernmental organisations had "digital" or "cyber" in their workplans. In 2024, internet-related issues are a first priority within nearly every international organisation.

Conference halls around the globe are filled with diplomats who negotiate intergovernmental arrangements on digital issues: cybersecurity is discussed by the UN's Open-Ended Working Group, cybercrime by its Ad Hoc Committee, internet-based lethal autonomous weapon systems by the Group of Government Experts on Lethal Autonomous Weapons Systems (CGE LAWS), digital trade at the WTO, platform regulation in UNESCO, infrastructure development at the ITU. AI is negotiated at the UN, UNESCO, the OECD, the G20 and other organisations. The WSIS+20 review is being prepared by the UN's Commission on Science and Technology for Development (UNCSTD). More than 30 UN organisations are coordinating their digital activities in the UN Group on the Information Society (UNGIS). Additionally, the G20, G7, BRICS, the Shanghai Cooperation Organisation and numerous regional bodies such as the OECD, ASEAN, OSCE, OAS, etc. are working on intergovernmental arrangements. And from what we see in the wars in Ukraine and Gaza, the arms race in cyberspace is exploding.

In other words, the role of governments in the digital age is rather different from what it was 30 years ago. Governments no longer stand on the sidelines. They are back as a key player. At the same time, today's intergovernmental negotiations are different from what they were in the last century. They are embedded in a multistakeholder environment. Governments have to take note of what non-state actors have to say. There is a new culture of transparency, inclusivity and openness. Deals behind closed doors or exclusion of meaningful participation of non-state actors will lead to failure.

In this context, it is worth remembering the words of UN Secretary-General Kofi Annan when he addressed the opening session of the Global Forum on Internet Governance, organised by the UN ICT Task Force in New York in March 2004. He said:

> [W]e need to develop inclusive and participatory models of governance. The medium must be made accessible and responsive to the needs of all the world's people.

And he added:

> 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.[15]

[15] United Nations. (2004, 25 March). Secretary-General's remarks at the opening session of the Global Forum on Internet Governance. https://www.un.org/sg/en/content/sg/statement/2004-03-25/secretary-generals-remarks-the-opening-session-of-the-global-forum-internet-governance

His call for "policy innovation" triggered the WSIS concept of the multistakeholder approach, helped to establish the IGF, and launched a process of enhanced cooperation. But a lot of detailed questions remained unanswered. What is the legal basis for the multistakeholder approach? What are the procedures for interaction among state and non-state actors? How can the IGF produce more tangible output? And a lot of practical issues are still unsolved. More than two billion people are still offline. The digital divide is now a knowledge divide. The global South is lagging behind when it comes to AI or quantum computing. In other words, the Tunis Agenda was just the start of a beginning. More has to be done.

A big step forward was the 2014 NETmundial conference in Sao Paulo and its Multistakeholder Statement. NETmundial defined universal principles for multistakeholder cooperation.[16] This was very helpful. The principles offer very good guidelines for dealing with all the new issues, such as AI or IoT.

But what is still missing is how such collaboration should be implemented in policy development and decision making. The good news is that a majority of governments support the concept in principle. But preaching multistakeholderism is one thing; practising it is another. Many governments pay only lip service to the concept, but continue with their classical top-down policy making, which is often neither open and transparent nor inclusive.

It is certainly a step in the right direction if more and more governments organise consultations with business, civil society and the technical community before making decisions. But it remains unclear how the "input" of non-state actors leads to an "impact". The Tunis Agenda speaks about "sharing of decision making". "Consulting" is not "sharing". There is still a long way to go. Talking the talk is not enough; walking the walk is the issue.

A good case is the IGF. The IGF has its strengths and weaknesses. And there was a good reason why the IGF was designed for "discussion only". The fear in Tunis was that an IGF with a decision-making capacity would turn the new discussion platform into an intergovernmental battlefield. The hope was that a discussion-only platform would open minds, mouths and ears to allow all voices and arguments to be expressed and heard, to stimulate free and frank dialogue among all stakeholders on an equal footing. The expectation was that knowledge and wisdom produced in the IGF discussions would enable decision makers to find innovative solutions. Those decisions should not be made inside but outside the IGF, by mandated policy organisations, businesses and civil society ventures. But the weak point so far is that there is a missing link between the "discussion layer" in the IGF and the "decision-making layer" in intergovernmental organisations.

In 2021, UN Secretary-General António Guterres was wise to recommend in his Roadmap for Digital Cooperation to keep the strengths of the IGF, but to overcome its weaknesses.[17] He accepted the HLP recommendation to transform the IGF into an IGF+. The appointment of the UN Tech Envoy, the nomination of the IGF Leadership Panel, the introduction of the IGF Parliamentarian Track and other concrete steps have given more steam to the IGF.

The Global Digital Compact (GDC) is a unique opportunity to continue the walk, to inspire political innovations and to enhance the conceptual understanding of the multistakeholder approach.[18] There is no need to reinvent the wheel or to start new processes.

The GDC will not be the end of the story. It will be just the next step on the long road into our digital future. The next milestones are WSIS+20 in 2025 and the review of the Sustainable Development Goals (SDGs) in 2030. It would be wise if the GDC picks the IGF as its natural landing place. The IGF is the best multistakeholder platform we have. The GDC could invite the IGF, together with UNCSTD, to prepare an annual report on "The State of Digital Cooperation". Such a report could document progress, identify weaknesses, and recommend concrete steps on how to move forward. And it would be wise if governments could agree in 2030 to bring the SDGs and the WSIS objectives under one umbrella of "Comprehensive Development Goals" (CDGs). The world beyond 2030 will be a digital world. And the governance of the digital world has to be based on the multistakeholder approach.

Action steps

Based on the discussion above, the following are key advocacy priorities for civil society in the context of WSIS+20:

[16] https://netmundial.br/2014/netmundial-multistakeholder-statement

[17] https://www.un.org/en/content/digital-cooperation-roadmap

[18] https://www.un.org/techenvoy/global-digital-compact

- There is a need for civil society to raise its voice in digital intergovernmental negotiations and call for the inclusion of basic values such as human rights, sustainable development, as well as peace and mutual understanding. These are core values for all civil society organisations.
- Civil society organisations have to enhance communication and collaboration with other stakeholders, including businesses, the technical community, parliamentarians and governmental representatives. If the argument is right that governments alone will be unable to solve the problems of the digital age, one has to recognise that civil society organisations alone will also be unable to solve the problems. Civil society organisations have to be prepared to work with other players who have different core values and prefer different approaches. They have to be prepared to negotiate, to search for consensus and to make compromises.
- Civil society organisations active in the digital sphere have to put their own house in order. They have to enhance cooperation among themselves. If the dozens of civil society groups speak with one voice in intergovernmental negotiations, their impact will be much greater than if every organisation makes its individual contribution. United, civil society is strong. This is also a lesson from the WSIS process 20 years ago. It was the unity among civil society organisations, and their coordinated statements in plenary and working sessions, which finally organised the pressure needed for governments to accept the multistakeholder approach as the key principle for the governance of the digital sphere. The making of the WSIS Civil Society Declaration[19] in 2003 is a good source of inspiration for developing an enhanced civil society strategy to meet the coming challenges of the digital age.

[19] 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

GLOBAL INFORMATION SOCIETY WATCH 2024 SPECIAL EDITION

WSIS+20: REIMAGINING HORIZONS OF DIGNITY, EQUITY AND JUSTICE FOR OUR DIGITAL FUTURE

Twenty years ago, stakeholders gathered in Geneva at the first World Summit on the Information Society (WSIS) and affirmed a "common desire and commitment to build a people-centred, inclusive and development-oriented Information Society."

This special edition of Global Information Society Watch (GISWatch) considers the importance of WSIS as an inclusive policy and governance mechanism, and what, from a civil society perspective, needs to change for it to meet the challenges of today and to meaningfully shape our digital future.

Expert reports consider issues such as the importance of the historical legacy of WSIS, the failing multistakeholder system and how it can be revived, financing mechanisms for local access, the digital inequality paradox, why a digital justice framing matters in the context of mass digitalisation, and feminist priorities in internet governance. While this edition of GISWatch asks: "How can civil society – as well as governments – best respond to the changed context in order to crystallise the WSIS vision?" it carries lessons for other digital governance processes such as the Global Digital Compact and NETmundial+10.

GLOBAL INFORMATION SOCIETY WATCH
2024 Report
www.GISWatch.org

IT for Change

WACC
communication for all

APC

Sida