



“ACCESS, ACCESSIBILITY, AND DIGITAL INCLUSION”

Part B of the Sixth Annual Meeting
11 November 2021 to 12 November 2021

Meeting Report



South African
Internet Governance Forum
ZAIGF

ACCESS, ACCESSIBILITY, AND DIGITAL INCLUSION

Meeting Report

Settings	
Document Title	2021b Internet Governance Forum Engagement Report
Project Title	ZAIGF (South African Internet Governance Forum)
Medium of Engagement	Hybrid
Document Authors	Tsholofelo Mokone
Doc. Version	
Sensitivity	Medium
Date	



DOCUMENT HISTORY

Changes to this document are summarised in the following table in reverse chronological order (latest version first).

Revision	Date	Created by	Brief description of
V1.00	22/01/2022	Internet Governance Coordinator	1. None. The document is in its original format

LIST OF TABLES	P04
LIST OF FIGURES	P04
FOREWARD	P05
BACKGROUND OF SOUTH AFRICAN INTERNET GOVERNANCE FORUM (ZAIGF)	P06
WELCOME REMARKS	P07

Session Features

SESSION 1	P08
Theme: THE RIGHTS OF PERSONS WITH DISABILITIES IN INTERNET GOVERNANCE	
Scope: The session presents a discussion forum on people with disabilities' rights. The discussion identifies barriers to Internet infrastructure access for individuals with impairments while offering a platform for the community with disabilities to express their concerns on Internet governance and the ICT sector participation	
SESSION 2	P09
Theme: ARTIFICIAL INTELLIGENCE (AI) TECHNOLOGIES EMPLOYED IN SOUTH AFRICA	
Scope: This session encourages a conversation on the state of AI technology in South Africa and how it is employed to meet social concerns. The session addresses the influence of AI technology on the continent's widespread digital divide.	
SESSION 3	P10
Theme: CYBERSECURITY, CYBERCRIME AND CYBERSECURITY AWARENESS STRATEGY	
Scope: The session debates the economic effect of cybercrime and the critical significance of digital literacy for South Africa's youth as a post-COVID-19 approach for cybersecurity awareness	
SESSION 4	P11
Theme: THE INTERNET AND ME: YOUR DATA, MY DATA, AND OUR DATA	
Scope: This session includes ordinary persons in public policy by fostering an interactive discussion about the future of the Internet and its governance, citizen involvement, and its future	

SESSION 5 P15

Theme: INTERNET FOR AND WITH THE CITIZENS

Scope: The session continues the previous session. It aims to foster conversation about how to engage regular citizens in Internet policy debates

SESSION 6 P16

Theme: MIS- AND DISINFORMATION, AND COVID-19 VACCINE INFODEMIC MANAGEMENT

Scope: The session discusses the critical nature of regulating the flood of information on the COVID-19 vaccination to avoid misinformation and deception

SESSION 7 P17

Theme: COMMUNITY NETWORKS IN PREVIOUSLY DISADVANTAGED COMMUNITIES

Scope: The session facilitates a debate on the critical nature of a people and environment-centred approach to connectivity

**GOVERNING THE PROCESS
(STEERING AND ORGANISING COMMITTEE ENGAGEMENTS)**

Participant feedback P18

Recommendations P18

LIST OF TABLES

Table 1: Document history P02

Table 2: Themes P08

Table 3: Participant feedback P18

LIST OF FIGURES

Figure 1: South Africans' use of the Internet P14

FORWARD

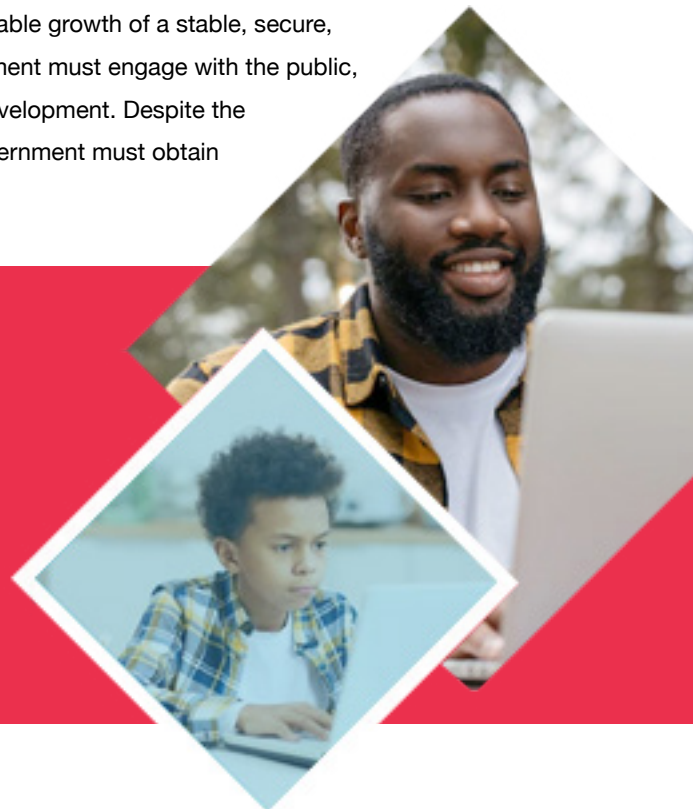
The ZAIGF Committee, in collaboration with the ZA Domain Name Authority (ZADNA) and the Department of Communication and Digital Technologies (DCDT), convened Part B of the sixth annual meeting of the South African Internet Governance Forum (ZAIGF). The annual meeting was convened in hybrid format under the overarching theme, ACCESS, ACCESSIBILITY, AND DIGITAL INCLUSION. It provided a sustained and relevant forum for open, responsible, professional, and egalitarian debate on South Africa's Internet governance.

The digital divide is defined as the difference between people with access to information and communication technologies (ICTs) and those lacking access. To close the divergence between the “haves” and the “have-nots”, it is widely recognised that expanding access to digital technology will eliminate these disparities; however, access does not always imply accessibility. Simply providing the means to participate in a democratic society does not ensure participation or eradicating the digital divide. Reducing technology and access concerns—or even “haves” and “have-nots” might be problematic since it ignores the social processes that must be addressed for effective technology. This simplicity creates the illusion that progress is being conducted in nations and their “connected” individuals.

This report reflects the presentations and discussions during the ZAIGF, collating government, civil society, and private sector stakeholder observations. Here, digital divergence is not merely a lack of technology—it is a layered form of exclusion dependent on and inextricably linked to other pernicious infrastructural, security, social, and economic challenges.

This report also reflects participating stakeholders' and audience's recommendations. A consistent theme emanating from the recommendation by the panellist members and audience participating in the forum is that government needs to increase its collaboration efforts with stakeholders to ensure the sustainable growth of a stable, secure, and robust Internet ecosystem. To deliver the aforementioned, the government must engage with the public, civil, and technical sectors in dialogues and fora on continuous Internet development. Despite the global pandemic grounding the world, the participants agreed that the government must obtain creativity to engage with the stakeholder groups and communities.

The ZAIGF Multi-Stakeholder Committee Secretariat extends its heartfelt gratitude to all the 2021 Part B ZAIGF participants, with a special thanks to the ZAIGF Multi-Stakeholder Committee for convening the ZAIGF, the Acting Director-General of DCDT, Nonkubela Jordan-Dyani, and the ZADNA Board Chairperson, Palesa Legoze.



The South African Internet Governance Forum (ZAIGF) is a multi-stakeholder forum of actors from the ICT sector. ZAIGF was established in September 2011 to develop a coordinated and coherent approach in dealing with Internet governance concerns in South Africa. As indicated in the Tunisia Agenda for the Information Society, Internet management should be “multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society, and international organisations”.

The forum is a multi-stakeholder platform for discussing Internet public policy issues pertinent to South Africa. It facilitates and strengthens open and transparent dialogues on Internet governance, defining the future of the Internet ecosystem in South Africa.

Some of the forum’s other objectives include:

- Creating a South African multi-stakeholder platform for an inclusive dialogue on Internet-related matters and policies
- Creating an inclusive information society
- Collaborating: Government, civil society, business, and academia to bridge the divergences to bring all South Africans into the Internet space knowledge society
- Strengthening the multi-stakeholder dialogue model for continental Internet governance engagements at regional and global fora.

Molehe Wesi, CEO of ZADNA, officially opened the 2021b South African Internet Governance Forum (ZAIGF). Molehe Wesi appreciated the participation of Nonkqubela Jordan-Dyani, acting Deputy Director-General of the Department of Communications and Digital Technologies, in his opening remarks. He also thanked the ZADNA Board Chairperson, Palesa Legoze, for her attendance and the Chairperson and members of the ZAIGF Multi-Stakeholder Committee. He acknowledged and valued the participation of members from the private sector, civil society, and academia in the ZAIGF.

Mr Wesi acknowledged the significance of the ZAIGF and its proceedings. He recognised that the restricted access and accessibility of online and Internet-related materials resulted in a knowledge vacuum on critical Internet and domain name system (DNS) infrastructures. He expressed optimism in the discussions, remarking they would attempt to generate solutions supporting the South African Government's goal of addressing access, accessibility, and the digital divide concerns.

The 2021B ZAIGF was also privileged to receive a keynote address from Nonkqubela Jordan-Dyani, the acting Deputy Director-General of the Department of Communications and Digital Technologies. In her keynote address—on behalf of the Minister and Deputy Minister of Communications and Digital Technologies—Nonkqubela Jordan-Dyani recognised the members of the ZAIGF Multi-Stakeholder Committee, the ZADNA Board Chairperson, and CEOs of participating entities. She also acknowledged ZAIGF and the South Africa School on Internet Governance (ZASIG) attendees before the meeting. She applauded and emphasised the importance of increasing youth participation in Internet policy dialogue, accentuating that the success of the policymaking in South Africa relies on including all stakeholders, embracing the youth.

Acknowledging the role of the Internet Governance Forum (IGF), Ms Jordan-Dyani noted that at a United Nations (UN) level, the IGF—an outcome of the World Summit on Information Society (WSIS), is recognised and applauded by the global community for its role in facilitating unique global policy dialogue. Ms Jordan-Dyani applauded the part of the ZAIGF in facilitating multi-stakeholder dialogue on evolution and Internet deployment concerns, in keeping with the 2005 Tunis Agenda, to which South Africa reaffirmed its commitment in 2016.

Ms Jordan-Dyani noted South Africa remains confronted with various socioeconomic difficulties relating to ICT though much was achieved over the years in complying with the Tunis Agenda. The country continues to struggle with access and accessibility concerns. The digital divide is South Africa's other plague. It exaggerates the divide between the rich and the poor by separating those with access to technology from those lacking access, including those with disability and gender concerns.

South Africa committed at WSIS to a people-centred, inclusive, and development-oriented information society. According to this commitment, the mission of connecting the disconnected remains vital. This extends beyond the ICT and Internet infrastructure deployment in communities. This undertaking entails developing web-based programs and solutions accommodating the impaired Internet user demands. It also entails empowering communities to capitalise on the Internet's potential for socioeconomic growth and development.

The DCDT developed the Digital Economy Masterplan to lay the foundation and ensure all people have access to the digital economy and its potential. The South African Government also embraced the 4th Industrial revolution (4IR) prospects to advance the country's economy. Other government initiatives emphasised by Ms Jordan-Dyani in her address included the broadband rollout, the topical high demand spectrum licensing, and the analogue switch-off (ASO) process, critical for terminating the digital divide, geographically ensuring connectivity for everyone in South Africa.

According to Ms Jordan-Dyani, The DCDT anticipates the minister officially proclaiming that the entire nation is linked with access to the Internet. Until then, everyone must contribute to preserving essential information and Internet infrastructure. Ms Jordan-Dyani acknowledged the cybersecurity framework as a crucial resource for ensuring the safety of critical information, primarily because of South Africa's escalating cyber threats. The framework promotes increased use of digital platforms by assuring a safe environment. Other initiatives emphasised by Ms Jordan-Dyani include the Digital Skills and Future of Work Programme and the Data and Cloud Programme to ensure safer data management. Ms Jordan-Dyani emphasised that it is the government's priority to protect Internet users; however, everyone has equal responsibility towards this goal.

Ms Jordan-Dyani, acting Deputy Director-General of the Department of Communications and Digital Technologies, applauded ZADNA and the ZAIGF Multi-Stakeholder Committee for convening the sixth annual ZAIGF. She also complimented the ZAIGF Multi-Stakeholder Committee on their nomination and participation in the sixth global annual IGF in Katowice, Poland. She outlined essential subjects she believed needed to be discussed during the annual global IGF, including the following:

- Approach to address data security breaches
- Content management: storage of content and accountability of unlawful content
- DNS abuse and IP Infringement
- Expropriation of IP addresses

Ms Jordan-Dyani emphasised the importance of global IGF strengthening – a democratic decision-making process to allow governments of smaller developing countries – the custodians of policy in their respective countries, a contribution in global policy decisions consistent with the principles guiding multinational and multilateral policy formulation processes. All stakeholders can influence global policy decisions.

SESSION FEATURES

The meeting featured interactive and robust dialogue, directing a broad range of themes and concerns under the overarching theme “ACCESS, ACCESSIBILITY, AND DIGITAL INCLUSION” with the sub-themes indicated in Table 2.

Session	Topic
Session 1	The rights of persons with disabilities in Internet governance
Session 2	Artificial Intelligence (AI) Technologies used in South Africa
Session 3	Cybersecurity, cybercrime, and cybersecurity awareness strategy
Session 4	The Internet and me: your data, my data, and our data
Session 5	Internet for and with the citizens
Session 6	Mis-and disinformation and COVID-19 vaccine infodemic management
Session 7	Community networks in previously disadvantaged communities

The ZAIGF 2021 (b) presenters, panellists, and participants discussed diverse topics that cannot be summarised verbatim; however, below is a summarised version of concerns discussed in the respective session(s):



THEME: THE RIGHTS OF PERSONS WITH DISABILITIES IN INTERNET GOVERNANCE

Sub-theme: The session presents a discussion forum on people with disabilities' rights. The discussion identifies barriers to Internet infrastructure access for individuals with impairments while offering a platform for the community with disabilities to express their concerns on Internet governance and the ICT sector participation.



Stakeholders from the Centre of Human Rights and Blind South Africa (BSA) presented Session 1 of the ZAIGF. The session focused on accessibility for the physically impaired. Both panellists affirmed that people with disabilities encounter discrimination with online resources and technology. Legislative regulations are non-compulsory, although legislative regulations address the accessibility problem.

The Blind SA representative asserted that since online devices are complex, they propagate discrimination against the physically challenged. Both the panellists acknowledged that even if online resources are accessible, they are unusable. This, they believe, is because several individuals without physical limitations like theirs decide on their behalf without their involvement.

The Centre for Human Rights' representative elaborated on "limited participation by the physically impaired in IG discussions". She asserted that persons with disabilities are often neglected, appealing to the audience to observe and count the physically disabled members present at the forum.

She claimed that until recently, there had been little effort to engage the physically impaired in such dialogues. She remarked organisations made only sporadic efforts to educate the physically impaired on constantly changing Internet technology. The physically disabled must, therefore, depend on outdated devices to stay updated with technological advancements.

The Blind SA panellist added that the cost of assistive technologies to help them access the Internet in information is high. The cost of a brail for the blind, for instance, can reach R100 000. Most physically impaired South Africans cannot afford this, further indicating over 65% of the physically impaired population cannot be active in the continuous enhanced global cyberworld.

The panellists concluded the session, pronouncing that the government should enact regulations to guarantee domains make information and Internet resources more accessible to the physically disabled. They must develop measures to ensure affordable assistive technologies while upskilling individuals physically impaired, enabling engagement in governance structures through technology.

ARTIFICIAL INTELLIGENCE (AI) TECHNOLOGIES EMPLOYED IN SOUTH AFRICA

Sub-theme: This session encourages a conversation on the state of AI technology in South Africa and how it is employed to meet social concerns. The session addresses the influence of AI technology on the continent's widespread digital divide.



A ZADNA stakeholder, the State Information Technology Agency (SITA), and a stakeholder from Phukubje Pierce Masithela (PPM) Attorneys presented the ZAIGF Session 2. The session focused on South Africa's readiness to leverage AI technologies to address societal challenges.

A consensus was reached among the panellists that the South African Government may not be fully prepared to integrate AI technologies into socioeconomic development programmes. The SITA representative maintained that the government is still researching AI technologies and their potential benefits to communities. The government also assesses the country's preparedness to use AI for development. The PPM representative also confirmed the narrative that South Africa is not fully prepared to integrate AI technologies into development programmes, contending that the country lacks laws governing using AI technologies; however, published papers and presidential reports advocate for AI technologies in the 4th industrial revolution (4IR) and data cloud policies.

The ZADNA representative cautioned against "lip-frogging" into AI technologies, despite their growing use through smartphones, social media, and banking applications. He contends that lip-frogging in AI technologies can prolong the inequality and unemployment crisis in South Africa.

The SITA representative defined AI as a "combination of diverse types of technologies that learn and act like humans". The ZADNA representative contended that increased advocacy and AI technologies can constrain the labour market's capacity to absorb the 700,000 youths who remain jobless. He contends it can divert the state's attention from concerns of inequality, the digital divergence, and developing an inclusive society—particularly provided improper digital skills.

The PPM Attorney representative expressed another risk associated with hastily employing AI technologies in South Africa's service delivery and development programmes. He contends people develop AI technologies to further their own interests. They are, therefore, predisposed to discriminate along with racial or gender stances, as observed in real-life case studies of AI bias in the USA and the Netherlands. The panellist agreed that the South African Government should develop legislation that protects against AI biases. The only legislation protecting against AI biases is the protection of the Personal Information Act (POPIA). The PPM Attorney representative explains Section 57 (1) of POPIA requires that a responsible party needs to obtain authorisation from the regulator before processing personal information, including unique identifiers. It also offers people the right to question the outcome of automated responses.

The panel and audience concluded the session by agreeing that for South Africa to participate in the global digital economy and benefit from AI technologies, it would need to develop its own AI technologies. These technologies should be connected to its social challenges, rather than adopting western AI technologies unsuited to address South Africa's socioeconomic challenges; however, in the absence of technological development capacity to develop South African AI technologies, the PPM Attorney representative affirmed that before adopting and implementing Western-developed AI technologies, it would be in the best interests of citizens to conduct human rights due diligence on the technologies adopted. This would assure avoiding inherently biased AI technologies adoption and use.

CYBERSECURITY, CYBERCRIME AND CYBERSECURITY AWARENESS STRATEGY

Sub-theme: The session debates the economic effect of cybercrime and the critical significance of digital literacy for South Africa's youth as a post-COVID-19 approach for cybersecurity awareness



A Snail Attorneys at Law stakeholder, Cybersec Clinique, and a cybersecurity specialist presented Session 3 of the ZAIGF. The session focused on distinguishing cybersecurity from cybercrime and understanding the cybercrime network, including the offender, the cybercrime victims, and market sustaining cybercrime activities in South Africa.

The session began with an analysis of the distinctions between the two concepts. The panellists agreed that cybercrime is the malicious violation of a third party's online confidentiality and vulnerability. The representative from the Cybersecurity Clinic noted that cybercrime occurs when there is an offender, a victim, and a market; it is often necessary to understand cybercriminals' modus operandi.

Cybersecurity refers to the practice of defending against cybercrime. It comprises laws, actions, best practices, and frameworks with instructions for individuals on how to be safeguarded against illegal online activities. According to the cybersecurity specialist, policies alone do not provide adequate protection against cybercriminals. To achieve adequate security against breaches, businesses and governments must employ individuals with the requisite knowledge and devices for identifying and mitigating technological breaches. This remains the 'missing leg' of cybersecurity.

According to the specialist, most organisations and government departments have comprehensive policies and documents concerning cybersecurity; however, they lack the human capacity to ensure protection from online criminal activities. The representative corroborated the above discussion, reasoning that most organisations and government departments lack a response framework. This led to numerous violations and offences over the past few years, with no response plan to redress the violations that enable continuity of operations in an organisation.

The specialist explained individuals are hacked but are unaware of how to defend themselves. They are unaware, for example, connecting to any online portal indicates exposure to the risk of the Internet source's owner evaluating the websites visited while linked to their Internet source. They are also unaware that purchasing Internet-enabled devices and embedded software exposes them to cybersecurity vulnerabilities. This is worsened by the absence of specialised personnel to monitor the devices purchased for critical government institutions.

The representative from Snail Attorneys at Law emphasised cybersecurity is about being responsible for using and processing data. This means that individuals need to safeguard personal information. Some best practices for doing this include not disclosing passwords to strangers, updating them often, and not leaving sensitive information or electronic files accessible. It is important to know that governments lack the resources, or the promptness required to react to cybercrime. Individuals, customers, and companies should take responsibility for their own Internet safety.

According to the Cybersecurity Clinic's representative, social media is the greatest danger of cybersecurity. Individuals put identifying information on social networking platforms, making it simple to become cybercrime victims. A growing need exists for government to increase digital literacy and online behaviour training initiatives, educating individuals on how to protect themselves online.

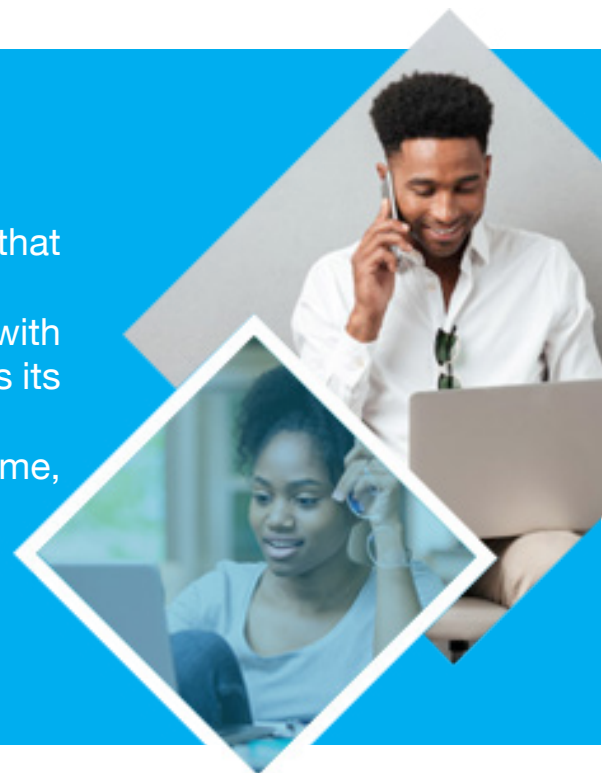
Snail Attorneys' representative emphasised that cybersecurity begins with you! He emphasised the importance of downloading programs for no reason, stating that web applications can hack persons. The Cybersecurity Clinic's representative reiterated her colleague's observations, asserting that previously a face app that photo edited images using AI to apply filters and resurrect the idea as an older adult. The face app was top-rated, but what most people were unaware of was that it collected user identifying information. Nobody knows what face app creators are doing with all that data. She reiterated the need for government to advance awareness campaigns, teaching people how to protect themselves from cyber-crime by not giving away personally identifiable information.

The specialist commented that several South African regulations are uncooperative to detect and punish cybercrime. For example, several rules or laws of evidence restrict how cybersecurity specialists acquire and use cyber-evidence, often causing several unsolved cybercrime cases. Online privacy is likewise non-existent. The specialist reports that governments globally spy on their citizens. Technologies are available to assist civilians in protecting themselves from government probing, but no one is discussing them owing to the concept of transparency and openness.

Other cybercrimes cited by the panellists include domain hacking or domain theft—the act of changing the registration of a domain name without the original registrant's consent or by abusing privileges on domain hosting and registrar software systems.

Additional cybercrime indicates sim card identity theft. This occurs when an individual loses their sim card and personal cell phone number, which may have been used to register personal information on numerous sites. Regrettably, according to a representative of the Cybersecurity Clinic, this offence is committed under the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA). The Act allows others to acquire cell phone numbers, enabling cybercriminals to hack and access victims' personal information registered under that number.

The panellists concluded the session by agreeing that South Africa is a long way from becoming a cyber-secure nation; however, if government collaborates with cyber experts to reconsider legislation and advances its efforts to raise awareness on how individuals and businesses can protect themselves from cybercrime, they will have won half the combat.



THE INTERNET AND ME: YOUR DATA, MY DATA, AND OUR DATA

Sub-theme: This session includes ordinary persons in public policy by fostering an interactive discussion about the future of the Internet and its governance, citizen involvement, and its future.



The ZAIGF Multi-Stakeholder Committee's Deputy Chairperson and Founder and CEO of Girl Code, Baratang Miya presented Session 4 of the ZAIGF. The session commenced with a discussion among the participants on the advantages of Internet access and the frustrations associated with lacking Internet access. The audience agreed that Internet access is a fundamental human right—restricting access violates that right. Consensus existed among the audience that Internet connectivity translates into access to information, cost-effective mass communication, and global and local networking prospects.

Building on the discussion, the presenter emphasised that the Internet is an enormous network linking computers globally—the infrastructure connects everything. It was also critical for the presenter to clarify between the Internet and the World Wide Web (WWW) since observing certain government officials demonstrates that the distinction between the two ideas is muddled. The WWW is simply an application running on the Internet. This primary device is used to access information. It is defined as the information system on the Internet, allowing documents to be connected by hypertext links, enabling the user to search for information by moving among documents.

The Internet is growing at a rapid pace. Using the Internet is growing at an even faster rate—communication is unprecedented. More platforms than ever exist; they all are more active than ever before. The presenter disclosed numbers of what occurs every 60 seconds online to gain perspective:

- Every 60 seconds – 500 hours of content are uploaded to YouTube
- Every 60 seconds – 21.1 million texts are sent
- Every 60 seconds – 197.6 emails are sent
- Every 60 seconds – 200,000 people tweets
- Every 60 seconds – 695,000 Instagram stories are shared
- Every 60 seconds – 69 million messages are sent
- Every 60 seconds – 5,000 TikTok downloads
- Every 60 seconds – 2 million views on Twitch
- Every 60 seconds – 3.4 million snaps are created
- Every 60 seconds – 1.4 million people scroll Facebook
- Every 60 seconds – 28,000 subscribers watch Netflix
- Every 60 seconds – 414,714 apps are downloaded from the Apple Store
- Every 60 seconds – \$1.6 million is spent online

An audience member raised a vital observation and suggestion in response to the stats provided about the growing use of the Internet and growing content. She observed less capacity in ISP to monitor the content uploaded onto the Internet as the number of Internet users increases. She validated the statement by contending this is most evident in the rise in the number of prejudicial, biased, and hateful content uploaded daily. She further recommended that the government investigate endorsing the establishment of more institutions that will monitor the content uploaded on the Internet without infringing on the rights of people online.

The presenter used the diagram below (Figure 1) to statistically illustrate that about 50% of South Africans use the Internet

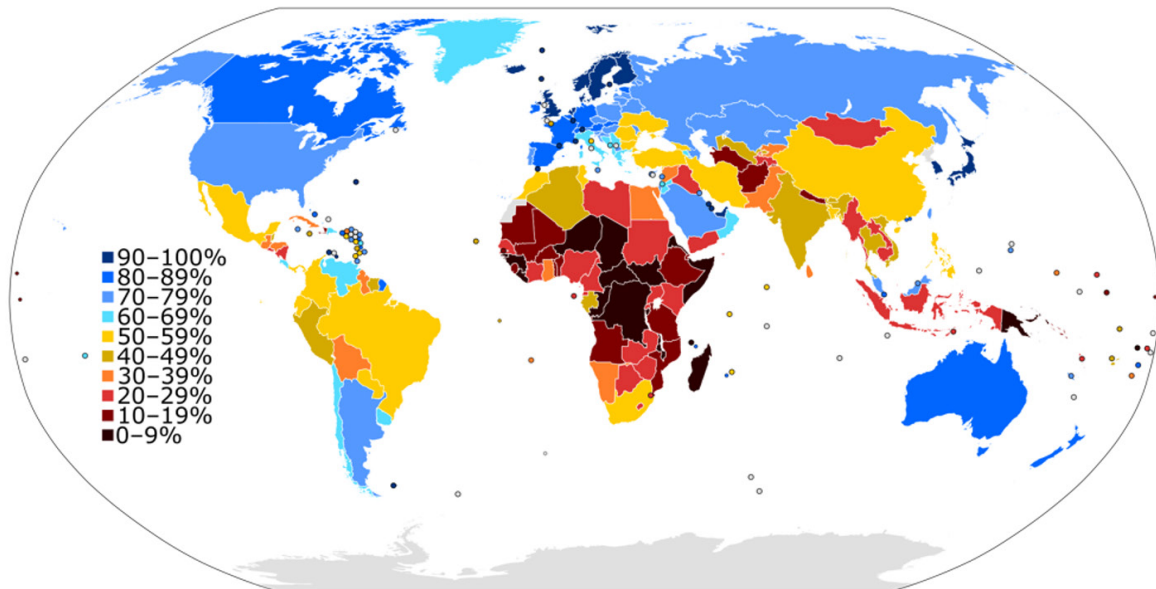


Figure 1: South Africans' use of the Internet

Though the statistics provided are slightly outdated, the presenter used them to deduce that South Africans have not exhausted the opportunities and benefits provided by the Internet. They are ineffectively exploiting digital marketing opportunities to enrich themselves. Most South Africans use the Internet at an Internet café to create a resume. Social media is another reason South Africans use the Internet. It is eminent that South Africans are not fully embracing the opportunities on the Internet. She concluded that South Africans do not fully understand that “citizens make the Internet work”.

The discussion progressed to include an exercise that tells a story about individuals' Internet behaviour. The presenter classified the information shared by participants on their social media pages into these categories: time zone, shopping patterns, device location, SMS, phone call history, and typing speed. She illustrated the AI analyses of the same data shared could have determined an individual's diet, real estate, intelligence quotient (IQ), income level, employment status, and political affiliations. The presenter explained data shared are precious resources that can be sold, owned, and bought by a company when departing a device.

After establishing the data report about individuals' Internet behaviour, the presenter did a practical exercise about digital identity and governance. She recommended that the youth in the audience, without an online persona, create one. Internet persona is a social identity that an Internet user establishes in online communities and websites. It may also be actively constructed by having someone tweet, post, or record a person's activities. People can have one or more Internet persona: educational, social, finance, and health. The advantages of an Internet persona are that it reciprocates to the data producer. It realises aggregation to determine the value of the data.

The session concluded with the realisation that the youth is increasingly exposed to risk, be it targeted harassment and ‘doxxing’ or radicalisation and conspiracy theories on the Internet. They emphasised that it is critical to increasing awareness of these harms, but more important to help them build a more inclusive and well-informed Internet community. The audience also suggested that decisions about policies on data use, storage and management should not be left to external entities because they have a more extensive data set or complicated terminology. The decisions should not be conducted in isolation, excluding citizens or Internet users, especially citizens with physical disabilities.

INTERNET FOR AND WITH THE CITIZENS

Sub-theme: The session continues the previous session. It aims to foster conversation about how to engage regular citizens in Internet policy debates



Session 5 of the ZAIGF was a continuation of Session 4. The ZAIGF Multi-Stakeholder Committee's Deputy Chairperson and Founder and CEO of Girl Code, Baratang Miya, presented the session. The session focused on how the participants observe digital space appearance.

The session started with the presenter distinguishing between a public sphere and a digital public sphere. She remarked that a public sphere is not necessarily – or even usually – a physical location for face-to-face meetings; it is a platform primarily constituted and maintained by communication. It is a podium where opinions and information are disseminated.

According to the presenter, a digital public sphere has radically revolutionised, transforming the communication and the dissemination of opinions in South Africa. It leads to an increase in the volume or intensity of communication rather than a qualitative shift.

The session concluded with an interactive dialogue among the audience, identifying the following as vital elements in a democratically healthy digital public sphere:

- Citizens can inform themselves based on facts and are exposed to trustworthy and independent analysis and a plurality of views
- All opinions are expressed and heard safely and freely, independent of race, gender, or sexual orientation, and without fear of abuse, violence, or hate speech
- Adequate checks and balances, accountability, and transparency apply, upholding democratic principles, fundamental rights, and protecting citizens

MIS- AND DISINFORMATION, AND COVID-19 VACCINE INFODEMIC MANAGEMENT

Sub-theme: The session discusses the critical nature of regulating the flood of information on the COVID-19 vaccination to avoid misinformation and deception



The Media Monitoring Africa (MMA) presented Session 6 of the ZAIGF, moderated by a member of the ZAIGF Multi-Stakeholder Committee. The session focused on the pandemic of misinformation, disinformation, and infodemic and its consequences.

While the COVID-19 is a health crisis, it is critical to recognise an information crisis. Both misinformation and disinformation include disseminating erroneous information for various purposes and objectives. The MMA representative illustrated how COVID-19 epidemic disinformation is observed, mentioning the former United States President Donald Trump; he was the primary source of COVID-19 misinformation during the outbreak's first months. The presenter contended that former President Trump's influence on disinformation is displayed in the volume and content of erroneous material discussed, even if he was not the direct source.

According to an MMA representative, mis- and disinformation subtly advances a specific narrative. This is exceedingly dangerous because it jeopardises the credibility of news reports regarding the COVID-19 pandemic. In South African politics, it threatens the integrity of democracy. The MMA representative contends that disinformation casts doubt on the legitimacy of institutions and procedures to citizens. It is used in the COVID-19 pandemic to advance an anti-covid and anti-vaccination agenda to systematically advance a particular economic, political, and ideological goal.

Following a dialogue about the role of evidence in mis- and disinformation, the presenter demonstrated how its effectiveness depends on their capacity to control the receiver's emotions. He closed the session by contending that misinformation is about power and the desire to undermine democracy by employing all means possible.

COMMUNITY NETWORKS IN PREVIOUSLY DISADVANTAGED COMMUNITIES

Sub-theme: The session facilitates a debate on the critical nature of a people- and environment-centred approach to connectivity



Stakeholders from the Pan African Information Technology Association (PICTA) and from the Internet presented Session 7 of the ZAIGF.

The PICTA representative displayed access and accessibility challenges encountered by rural and peri-rural communities. He contends that rural and peri-rural communities were overlooked in the Internet dialogue. This is most apparent in the connectivity of rural and peri-rural communities. Accessibility “is about one’s ability to access the Internet”. The PICTA representative questioned how accessibility could be achieved if rural and peri-rural communities were not connected. He contended that rural and peri-rural community members could not connect because of inadequate Internet infrastructure. There is no bandwidth!

These communities cannot afford connectivity because of poverty and unemployment challenges. The other frustration expressed by the PICTA representative is that whenever stakeholders or government engage rural and peri-rural community members on the Internet, it is usually conducted without enquiring about community members’ Internet needs; they are being informed what their Internet need might be. He expressed the Internet is not a luxury but is essential, like water, electricity, and sanitation.

Representatives from the Internet and Njinjicom concluded this session, echoing the sentiments shared by the PICTA representative. The panellist emphasised the importance of increasing female participation in rural and peri-rural communities on the Internet and its governance. A need was identified to improve education and skills development initiatives and entrepreneurial opportunities in the Internet ecosystem. A lack of knowledge exists on the Internet ecosystem in rural and peri-rural communities; several companies want to partner with the government to expand training initiatives to rural and peri-rural communities.

GOVERNING THE PROCESS (STEERING AND ORGANISING COMMITTEE ENGAGEMENTS)

The ZAIGF Committee, with ZADNA (The secretariat of Internet governance in South Africa), facilitated the preparatory process for the ZAIGF 2021. The committee held weekly meetings to discuss the Internet governance focus, suggesting topics for the ZAIGF and speakers to be invited to form panels. The committee, with the secretariat, secured the speakers and shared the invitation for the public and ZADNA members. The ZAIGF was held in a hybrid format over two days.

Participant feedback

• Sessions were highly informative, with increased female participation
• Some participants expressed interest in participating as a panellist in the ZAIGF and ZASIG in 2022
• The panellist expressed concern about receiving the invitations late, with limited time for publicising the event on social media platforms and the Internet
• The panellist expressed concerns about not extending the invitation to ZADNA members

Recommendations

- Norms and regulations imply a lengthy process and consultations while technology develops rapidly. It is, therefore, necessary to collaborate concerning the multi-stakeholder model. All actors need to cooperate to create a safer and more trustworthy online environment.
- Barriers to Internet governance should be managed to reflect the value of the Internet by modernising rules, legislation, and policies.
- For the future of this country, the focus should be on developing Internet access and inclusion to evolve globally.
- Internet governance should continue to be provided high priority, as decisions in this domain directly affect the life of all South Africans and the future of societies, including the stability of their human rights, regarding access and inclusion.





South African
Internet Governance Forum
ZAIGF