



"DIGITAL INTERDEPENDENCE"

Sixth Annual Meeting
24-25 March 2021

Meeting Report



South African
Internet Governance Forum
ZAIGF

"DIGITAL INTERDEPENDENCE"

Meeting Report

Settings	
Document Title:	2021 Internet Governance Forum Engagement Report
Project Title:	ZAIGF
Medium of Engagement	Online
Document Authors:	Tsholofelo Mokone
Doc. Version:	V1:00
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	Short Description of Changes
V1.00	22/04/2021	Internet Governance Coordinator	1. None. The document is in its original format

TABLE OF CONTENTS

EXECUTIVE SUMMARY	5
BACKGROUND OF ZAIGF	6
OBJECTIVES OF THE ZAIGF	6
WELCOMING REMARKS	7
HIGHLIGHTS OF SESSIONS	8
SESSION 1	9
Theme: Education and access to the Internet	
Sub-theme: Internet access as an enabler for skills, knowledge and information acquisition for rural and marginalised communities during the COVID-19 pandemic.	
SESSION 2	11
Theme: Universal access and connecting the unconnected	
Sub-theme: Community Networks continue to connect the unconnected and marginalised in the most affordable ways, but they still face challenges	
SESSION 3	13
Theme: Enhancing a multi-stakeholder approach	
Sub-theme: Multi-stakeholder approach in infrastructure and cyber security	
SESSION 4	15
Theme: Digital economy and opportunities	
Sub-theme: Integration of the real economy with the digital economy and effects of AI and 5G	
SESSION 5	17
Theme: Unlocking the digital potential – skills development in the digital age	
Sub-theme: Digital literacy programme design to empower young people and educate them on how to use the Internet responsibly.	
SESSION 6A	19
Theme: Disinformation in the lead up to the 2021 local government elections	
Sub-theme: Lessons learned during the COVID-19 pandemic, platform responsibilities, and the impact on media.	

SESSION 6B	21
Theme: Promoting cyber security during the COVID-19 Pandemic	
Sub-theme: The nature of a cyber incident that took place in South Africa, and the type of capacity-building initiatives that have been undertaken to combat data protection and cybercrime.	
SESSION 7	22
Theme: Privacy and protection of personal information	
Sub-theme: The data cyber security and protection legislation which is in place in South Africa, how it's regulated, and the challenges, failures and successes.	
The panel was represented by Advocate Zanyiwe Asare from Digitally Legal, Professor Sizwe Snail ka Mtuze from the Information Regulator, and Ms Abongile Mashele from the Film and Publications Board (FPB). The different perspectives on cyber security and data protection legislation in place in South Africa, as well as the challenges, failures and successes.	
SESSION 8	23
Theme: Critical Internet Resources – Domain abuse, WHOIS access model and law enforcement	
Sub-theme: What are the current domain-name abuse incidents in South Africa, and how they have been resolved.	
Governance of the Process (Steering and Organising Committee engagements)	
Feedback from participants and Speakers	
Comments on the preparatory process	
Recommendations	
ZAIGF 2021 AGENDA	26
WELCOMING NEW COMMITTEE MEMBER AND THANKING OF OUTGOING COMMITTEE MEMBERS	30

EXECUTIVE SUMMARY

The sixth annual meeting of the South African Internet Governance Forum (ZAIGF) was hosted online by the ZAIGF Committee, in conjunction with the ZA Domain Name Authority (ZADNA) and Department of Communication and Digital Technologies (DCDT), under the overarching theme:

Digital Interdependence. It served as a sustainable and relevant platform for transparent, accountable, professional, and egalitarian discussion on Internet Governance in South Africa.

The theme “Digital Interdependence” paints a picture of the interconnected character that South Africa has taken on, during the 2019/2020 time period of the COVID-19 Pandemic. There has been an increase in human interaction in the ever-expanding digital web. However, to enjoy the evolution and use of these technologies, it is important to consciously and deliberately go about it with the involvement of civil society, the private sector, and the government. This helps to recognise their interdependence and helps them work together to address the profound risks arising from the dramatic increase in interconnectivity and reinforcing the underlying interdependence.

This report reflects the presentations and discussions that took place during the ZAIGF forum. It collates the views of stakeholders from government, civil society, and the private sector, in the way digital technologies are offering new opportunities and presenting new challenges in harnessing a safe and inclusive digital economy.



BACKGROUND OF ZAIGF

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

The forum facilitates and strengthens open and transparent dialogues on Internet governance, which shapes the future of the Internet ecosystem in South Africa.

OBJECTIVES OF THE ZAIGF

ZAIGF is a multistakeholder platform for discussing Internet public policy issues that are pertinent to South Africa. Its objectives are to:

- Create a South Africa multi-stakeholder platform for an inclusive dialogue on Internet-related matters and policies;
- Create an inclusive information society;
- Work together: Government, civil society, business, and academia to bridge the gaps that exist to bring all South Africans into the Internet space knowledge society;
- To strengthen the multi-stakeholder dialogue model for continental Internet Governance engagements at regional and international forums.

The forum facilitates and strengthens
**OPEN AND TRANSPARENT
DIALOGUES ON INTERNET
GOVERNANCE,**
which shapes the future of the
Internet ecosystem in South Africa.



WELCOMING REMARKS

The 2021 ZAIGF was officially opened by the ZADNA CEO, Mr Molehe Wesi. In his opening address, Mr Wesi acknowledged the attendance of the Deputy Minister of the Department of Communications and Digital Technologies, Hon. Pinky Kekana. He also acknowledged the attendance of the members of the ZA Multi-Stakeholder Committee on Internet Governance in South Africa, the board members, and executive managers of participating entities, and the ZADNA board, partners, and staff.

Mr Wesi recognised the importance of the South African Internet Governance Forum (IGF) and the deliberations thereof. He expressed his confidence in the discussions that would take place, pointing out that they sought to produce solutions that would support the government's objective in the provision of a safe, secure, and inclusive Internet space.

The 2021 ZAIGF was also privileged to receive a keynote address from Deputy Minister Hon. Kekana, who reminded the ZAIGF participants that the IGF is a global multi-stakeholder forum that facilitates and strengthens dialogue on Internet policy. It is a United Nations (UN) process that provides inclusive dialogue on public policy issues, inherent through the development and use of the Internet. According to Hon. Kekana, such dialogues serve to bring together stakeholders from government, the ICT community, research, civil society, academic business, and previously disadvantaged areas, to facilitate a common understanding of how to maximise Internet opportunities and address the risks and challenges that arise thereof.

Hon. Kekana highlighted that the 2021 national IGF event, under the theme "Digital Interdependence", is aimed at providing a refreshing perspective on new ways in work and life in the new normal, which has been brought about by the increase in the use of technology, ahead of the 2021 Global IGF, which will be hosted from the 6th to the 10th of December 2021, in Poland, Katowice. She emphasised the importance of inclusion in this new way of working and living.

She further added the 2021 national IGF serves as a platform to solicit views on public Internet policy issues. The ZAIGF multi-stakeholder committee, the research, and the ICT community, etc. have been consulted on the convening and execution of this event. The stakeholders, including the global IGF, were requested to provide topics that they regarded as a priority for the 2021 IGF. From the ten themes identified, an overwhelming number of responses identified the "inclusion of vulnerable groups, security and trust" as the most important sub-themes to be prioritised for the forum. The technical challenges of infrastructure development, digital divide, data privacy and AI development and adoption were recognised as critical topics for discussion and resolution. According to Hon. Kekana this dynamic coalition of the IGF is a testament to the successful and continuous multi-stakeholder discussion on Internet and Internet Governance issues, from which, the ZAIGF has been benefitting.

Hon. Kekana concluded her welcoming address by thanking the attendees for their participation in the Internet Governance Forum. She extended her well-wishes for a successful and impactful 6th ZAIGF. She also extended her well-wishes for the newly ushered ZAIGF committee members.

HIGHLIGHTS OF SESSIONS

The meeting featured interactive and robust dialogue, addressing a broad range of themes and issues under the overarching theme “Digital Interdependence”, with the following sub-themes.

Settings	Topic
Session 1	Education and access to the Internet
Session 2	Universal access and connecting the unconnected
Session 3	Enhancing a multi-stakeholder approach in South Africa
Session 4	Digital economy and opportunities
Session 5	Unlocking the digital potential – skills development in the digital age
Session 6a	Disinformation in the lead up to the 2021 local government elections
Session 6b	Promoting cyber security during the COVID-19 Pandemic
Session 7	Privacy and protection of personal information
Session 8	Critical Internet resources – Domain abuse, WHOIS access model and law

THEMATIC SESSIONS

The ZAIGF 2021 presenters, panellists and participants discussed a diverse array of topics that cannot be summarised *verbatim*. However, below is a summarised version of pertinent issues that were discussed in the respective session(s):



THEME: EDUCATION AND ACCESS TO THE INTERNET

Sub-theme: Internet access as an enabler for skills, knowledge, and information acquisition for rural and marginalised communities during the COVID-19 pandemic.



Session one was represented by stakeholders from Broadband Infraco (BBI), a licensed State-owned company in the telecommunications sector and a Level 1 BEE ICT Company called KONECTA. The session focused on the Internet as an enabler of skills, knowledge, and information acquisition for rural and marginalised communities during the pandemic. This pays particular attention to the measures taken to “improve quality access and online education”, as well as the “successes, failures and recommendations to move to a better future”.

In opening the session, it was pointed out that education is a basic human right. It is recognised globally as the basis for social and economic development. Ambitions for education are captured in Sustainable Development Goal 4 (SDG 4) of the 2030 Agenda, which aims to “ensure inclusive and equitable quality education and promote lifelong learning opportunities for all by 2030”.

The Internet was dubbed a cross-cutting enabler for education. It provides unparalleled access to information and facilitates connections to educational resources, virtual labs, ideas, and people. In fact, during the COVID-19 pandemics’ hard lockdown, the South African government promoted online learning as the only alternative. Unfortunately, this mode of education exposed the stark reality of inequality that exists in South Africa, excluding many rural learners from teaching and learning, due to a lack of resources to connect to the Internet.

One of the panel members pointed out that, KONECTA has concerted its effort to help government narrow down this digital divide by providing a “free hotspot”. This is part of the organisations Social Responsibility obligations. However, for the organisation to extend its reach, it relied on partnerships with various stakeholders. Its most recent partnership was with the DCDT. The partnership enabled the organisation to deploy more than R5 million worth of free Wi-Fi in Alexandra taxi hubs. Consequently, this enabled access to education for those students and learners who use the Internet as they commute to school or institutions of learning.

The organisation also provides Internet education. This initiative seeks to educate people on how to connect to the Internet, and what they can do with the Internet once they have connected, besides using the Internet for social media. She stressed the importance of developing peoples' understanding of what the Internet is, and its value and benefit. Arguing that, "if people knew how to use the Internet and the power of the Internet, they stood a better chance of benefitting from the opportunities provided for by the Internet.

The panellists recognised the challenge of digital infrastructure and agreed that the challenge was not just a government problem. They suggested that the role of government should be the creation of an enabling environment for smooth integration between stakeholders from the SMMEs, corporates, civil society, etc.

Another panel member made several recommendations to address the infrastructural challenges. He recommended lowering the cost of data to ensure Internet access for children in rural and marginalised areas. The panel member also recommended teacher training and community education. He argued that teachers need to understand how the systems that will be rolled out work. The recommendation was supported by panel members arguing that "educating Internet users on how to use technological devices before they are rolled out was also stressed as a critical component of online education". They went on to argue that education can best be facilitated through a multi-stakeholder approach, suggesting the provision of more zero-rated educational websites, to fast track the rolling of programmes aimed at upskilling teachers, technical trainers, and future users of the Internet.

Communities need to be educated on the importance and necessity of digital infrastructure. The panel members agreed that this will play a role in addressing the trend of infrastructure vandalism in communities. According to the panellist, there is increasing education that needs to be done, and it is the responsibility of all stakeholders to educate the public. This will not only address issues of vandalism and theft but to also facilitate connectivity in rural and marginalised areas, further enabling equal participation in the digital economy.



THEME: UNIVERSAL ACCESS AND CONNECTING THE UNCONNECTED

Sub-theme: Community Networks continue to connect the unconnected and marginalised in the most affordable ways, but they still face challenges



The 2020 lockdown in South Africa has highlighted the stark reality that some employees can work remotely and may continue to do so after the lockdown ends. Others have immense difficulties finding reliable connectivity. The same can be said for school learners, with the privileged using fibre networks to access online schooling, while the poor risk being left behind. This has compelled the South African government to take a closer look at its connectivity solutions.

This session focused on how universal access and Internet connectivity can be maximised through community networks. It paid particular attention to what has been done to support community networks in South Africa and identifying the successes and failures in institutionalising these community networks.

Community networks are a computer-based system that seeks to help support communities by supporting, augmenting, and extending already existing social networks. They put technology in the hands of local citizens, providing solutions of access and affordable connections in underserved communities. South Africa has several community networks, however, there has been growing recognition of the challenges experienced by community networks. This was identified as largely being a result of limited institutional support.

The session was represented by stakeholders from the Independent Communication Authority of South Africa (ICASA), the Department of Communication and Digital Technologies (DCDT) and Management Automation (Pty) Ltd, a local wireless Internet Service Provider (WISP). It started with an account of ICASA's progress towards implementing the Digital Economy Masterplan, which was initiated at the start of Covid-19 to inform the impact of Covid-19 on the digital economy.

This was then followed by a discussion on the government's SA Connect Program, which is aimed at delivering broadband access to 90% of the country's population by 2020, and universal access by 2030. It was acknowledged that the National State of Disaster under the COVID-19 lockdown has affected the implementation of the program. The discussions on the SA Connect Program sought to provide a directive on when the second phase would be implemented, also to determine whether the second phase would focus on underserved communities and the departments' capacity to offer subsidies to low-income users.

Panel members provided an update on the department's progress in implementing the SA Connect Program. Due to the magnitude of the SA Connect program, government decided that it should be implemented in phase one and phase two. Phase one of the project sought to connect all schools, health facilities, government offices, Thusong Centres, and post offices in eight rural district municipalities to broadband services. Phase one of the project was completed in January 2021, despite the delays encountered. Phase two of the program has not yet been carried out. It is expected to commence once the inquest from the feasibility study commissioned by Development Bank of Southern Africa (DBSA) and DCDT has been finalised.

The feasibility study seeks to assist government with the best way to implement the next phase of the broadband project, by addressing technology options that can be considered by the country, governance requirements, funding, and implementation models. Furthermore, the study questions whether State-Owned Entities (SoEs) are capable of being implementation agencies.

The challenges encountered by community networks were also discussed in this session. Panel members acknowledged that limited access to technical skills and awareness of challenges experienced by community networks volunteers are some of the challenges that are limiting community networks' ability to connect the unconnected. These challenges are prominent in rural communities, more than it is in urban communities. One of the panel members acknowledged that, even though expert support is provided to the technical development of community networks, experts often lack pre-existing knowledge of the challenges experienced by these communities. This makes skills training difficult to achieve. It was, therefore, recommended that experts should be introduced to a community where they are deployed to assist. This would assist them to be sensitive to the real issues of the community and, it will enable to facilitate better training for community networks volunteers.

The cost of the spectrum was also acknowledged as a challenge for community networks. While there is no earmarked framework on the high-demand frequency spectrum for community networks, it has emerged that there are initiatives that have been put in place by authorities to ensure the provision of affordable Internet connectivity in rural communities. These initiatives include the TV whitespace wideband networks in South Africa (TVWS), which are unused channels in the broadcast TV spectrum. A panel member acknowledged that, TVWS enables the provision of affordable Internet access to rural community networks without subjecting them to spectrum fees. This initiative can also be exploited by SMMEs for commercial use.

Through the panel discussion, it also emerged that provinces have the authority to roll out their own broadband infrastructure. This would be supported by coordination forums that ensure that there are no duplications, to ensure that the roll-out is aligned with the national broadband policy. Currently, government is planning to establish a centralised Project Management Office, that will ensure the implementation of broadband is done in a coordinated manner. He also highlighted the importance of working together in this regard, to ensure that community networks connect the unconnected.

SESSION 3

THEME: ENHANCING A MULTI-STAKEHOLDER APPROACH

Sub-theme: Multi-stakeholder approach in infrastructure and cyber security



A multi-stakeholder approach is an organisational approach to governance or policymaking, which brings together stakeholders such as businesses, civil society, governments, research institutions and non-government organisations. They will participate in the dialogue, decision-making and implementation of solutions to common problems and goals. It is not a new approach to policymaking. The approach has been tested and applied to a range of policy spaces, and it has been deemed suitable to address challenging policy issues and produce credible and workable solutions.

The South African government, through DCDT has embraced a multi-stakeholder approach to Internet governance. These strides are significant in the government's objective to ensuring inclusivity and greater public participation in shaping domestic Internet policy.

This session was focused on identifying gaps and making a recommendation to South Africa's multi-stakeholder approach to infrastructure development and cyber security. It was represented by stakeholders from UjuDigital, and the DCDT.

To start the discussion, panel members applauded the government's efforts to create a truly multi-stakeholder Internet Governance community. The panel member pointed out that, government is willingness to consider the inputs of stakeholders in proposed bills and policies, fosters an inclusive policy-making process. However, this process is limited by a short-handed consultation process, as seen in the E-toll debacle. Poor consultation limits government's ability to ensure an effective multi-stakeholder approach to policymaking.

The panel member acknowledged that poor coordination is at the centre of this challenge. If the government had a centralised coordination structure, then it will be able to leverage consultation and ensure the successful implementation of programmes.

The other noteworthy challenge identified, is funding when it comes to infrastructure roll-out. Commercialising infrastructure development has hobbled the country's prospect of narrowing down the digital divide. One of the panel members acknowledged that, infrastructure funding has been left in the hands of the private sector for a long time. Improved multi-stakeholder coordination could improve government's ability to address the challenges of infrastructure roll-out and the effective execution of programmes. It is, therefore, important to ensure that the stakeholder approach to Internet Governance is enhanced.

With discussion, it emerged that progress has been made on the National ICT White paper. The Minister has issued a policy directive on High-Demand Spectrum, as well as the Wireless Open Access Network. From a multi-stakeholder perspective, the principal objective for the departments on these issues is to transform the industry and the sector, ensuring wider participation by SMMEs, women, youth, and persons with disabilities. Through the policy directives given, the department is advocating for universal service and access, and the affordability of cost of communication. Ensuring that the rural and underserved communities can afford to receive services.

It also emerged that the government has agreed to establish a State digital infrastructure company, aggregating all the ICT infrastructure. This seeks to ensure that the digital divide is closed. Stakeholders from the private sector and civil society will be required to form part of the digital infrastructure roll-out. ISPs and SMMEs must share and play a role in this regard.

SMMEs can partner with the government, as set aside for them in the ICT SMME strategy. There is also deliberate intent by government to procure from local ICT SMMEs. There are a number of SMME training programmes across the country. Government, through NEMISA, is working with the likes of Google and IBM to provide soft digital skills. Government has invited SMMEs to get in touch with ICT Chamber and participate in the offering provided by government.

Despite existing gaps in South Africa's multi-stakeholder approach, the panel members agreed that South Africa is on an effective path towards a multi-stakeholder approach in infrastructure.



THEME: DIGITAL ECONOMY AND OPPORTUNITIES

Sub-theme: Integration of the real economy with the digital economy and effects of AI and 5G



The session, which was represented by stakeholders from Brand SA, IfoundIT, Ecommerce, PAICTA and CHEKALEFA, focused on the effectiveness of the digital economy and its opportunities. It sought to identify some of the challenges that exist in the digitalising processes of the economy, as well as the measures needed to address those challenges.

There was a consensus among the panellists on the kind of challenges faced by South Africa and the African continent in digital infrastructure. The panellists seemed to agree that South Africa and Africa at large do not have the most recent and relevant infrastructure to drive the digital economy. However, the continent has the potential to develop the digital infrastructure, or the digital solutions to cater to the infrastructure that Africa already has.

Panellists agreed that there is a major digital divide within the continent. This is a result of the lower ends of the market or rural communities not having access to digital solutions such as smart phones or integrated points of sales systems, which are regarded as necessary components for growing the digital economy. This divide is slowing down the continent's prospects of achieving a fully integrated digital economy that we are working towards, and it is also slowing down South Africa's prospects of fully benefitting from the digital economy.

One of the panel members highlighted that there was an urgent need for digital transformation in our thinking and approach to basic service delivery for South Africa to fully benefit from the digital economy. In agreement, another panel member indicated that there needed to be an improvement from the traditional approach to processing data with artificial intelligence (AI) and algorithms that provide decision factors.

The panel members agreed that the continent doesn't have a shortage of digitally skilled individuals to facilitate transition into a permanent state of the digital economy. In fact, they argued that there is a lot of effort by tech-hubs and institutions of higher learning that revamp their curriculums to ensure that they have courses that are aligned to the digital economy. Africans are on the right track in skilling themselves for the digital economy. What these skilled individuals need is the necessary digital infrastructure.

In addressing the threats that are posed by the digital transformation on labour and the traditional economy, the panellist argued that it is important for regulators to understand the country's social environment in shaping its digital economy, and to not be completely engulfed by the technology waves. In closing, the panellist stressed the importance of ensuring that key skills are continuously empowered into the workforce to ensure that people always remain relevant. A Member of the ZAIGF steering committee, acknowledged that a lot of work is done by stakeholders from the government, civil society, the private sector, and educational stakeholders in advancing courses offered on the Internet. However, more work still needs to be done to ensure that access to the Internet is equitable and that the rights of users are protected for the society at large.

The continent

DOESN'T HAVE A SHORTAGE OF DIGITALLY SKILLED INDIVIDUALS

to facilitate transition into a permanent
state of the digital economy



THEME: UNLOCKING THE DIGITAL POTENTIAL – SKILLS DEVELOPMENT IN THE DIGITAL AGE

Sub-theme: Digital literacy programme design to empower young people and educate them on how to use the Internet responsibly.



The session discussed existing digital literacy programmes that empower and educate young people on how to use the Internet responsibly. It was represented by an all-female panel, from Girl Code, Girl Hype, Media Monitoring Africa (MMA) and BITF who, in addition to speaking about “unlocking the digital potential of young people,” raise awareness about the existing gender gap in digital literacy.

There was a general consensus among the panellist members that the voice and influence of young women on the Internet is important. There is a gender disparity in technology. One of the panel members argued that the disparity is historically attributed to subscribed gender roles, which saw many men equipping themselves with the skills and knowledge necessary, to amplify their voice in the Internet space. In agreement, another panel member pointed out that research proves that a large number of executive positions in the tech industry are held by men, most of which being white men. Therefore, there is a growing and urgent need to unlock the digital potential for young black girls.

There are several programmes that are initiated to correct and close the gender gap. These programmes seek to create a network of women who will become active participants in the digital technology space. The programmes also educate and empower young girls on how to become active and responsible digital citizens.

The panel members agreed that, if we want to effectively unlock the digital potential of young people as a collective, digital and media literacy skills need to be embedded in South Africa's school curriculum. They identified the lack of basic digital and computer skills as an existing challenge that limits young people's potential and ability to meaningfully engage in the digital world.

They argued that the above-mentioned challenges are accompanied by a lack of access to basic digital infrastructure, digital devices, and access to data, especially in the rural parts of South Africa. The panel members alluded to an urgent need to enable young women in cybersecurity skills to close the limits and also bridge unemployment through active involvement in that segment of the digital space.

They highlighted that as part of empowering young girls to become responsible digital citizens and get jobs, leaving a digital footprint is important, especially on social media. Panel members stressed the importance of educating young people on using the Internet responsibly and creating an identity on the Internet that markets young people better.

The panel members encouraged young learners to be active and responsible participants in the digital space.

There is a growing
**AND URGENT NEED TO
UNLOCK THE DIGITAL
POTENTIAL FOR YOUNG
BLACK GIRLS**



THEME: DISINFORMATION IN THE LEAD UP TO THE 2021 LOCAL GOVERNMENT ELECTIONS.

Sub-theme: Lessons learned during the COVID-19, platform responsibilities. Impact on the media.



This session was focused on disinformation and the measures needed to combat disinformation in South Africa, in the wake of the 2021 local elections. It was represented by a panel consisting of representatives from (MMA) and Google South Africa.

Disinformation, which is defined as information that has been falsified with the deliberate intention to deceive and/or harm a person, social group, or a country¹, threatens and disrupts our process of freedom of expression and democracy.

One of the panel members pointed out that 41% of the 900 complaints received by MMA, is disinformation. The panel member adds that these numbers were expected to increase during the 2021 South African local elections. However, the panel member acknowledged government effort to addressing that disinformation was a challenge. They argued that it was encouraging to see that government authorities were taking the issue of disinformation seriously and imposing regulations that sought to penalise people who spread disinformation.

Another panel member noted that the kind of disinformation trend that they noticed during the 2019 national elections, largely has to do with election logistics. For instance, people openly shared incorrect addresses of election stations. The panel members agreed that the problem with this kind of disinformation is that it isn't serious, until it's disrupting an individual's ability to participate in the elections. Artificial Intelligence has also been playing a key role in disinformation through the manipulation of videography. As such, it is important for the IEC and political parties to receive digital literacy and be equipped with tools that will allow them to participate meaningfully on social media. The panel member pointed out that there was a need for shared responsibilities in ensuring that Internet users get accurate information on critical topics. She urged political parties to maximise their participation on social media. This will act as a means of countering election-related disinformation, and that political party websites and social media platforms can be a source for accurate information.

¹https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf

The panellists both presented the different measures that are employable to counter, combat and redress disinformation. One of the panel members spoke of the MMA's 411 initiative aimed at empowering citizens to be able to identify and deal with disinformation. The 411 relies on public participation, with citizens identifying and reporting disinformation through the complaints process. Another measure identified, was the Google SA Project Shield, which seeks to protect high-profile websites.

They agreed that education on disinformation is important to combat it and that training citizens the importance of fact-checking information to combat disinformation. They stressed that the media and media personalities also have a responsibility to fact-check information and ensuring that they provide accurate information. There are sufficient tools to help them combat disinformation and means to empower them to share credible information.

Disinformation, which is defined as information that has been falsified

**WITH THE DELIBERATE
INTENTION TO DECEIVE AND/OR
HARM A PERSON, SOCIAL GROUP
OR A COUNTRY,**

threatens and disrupts our process of freedom of expression and democracy.



THEME: PROMOTING CYBER SECURITY DURING THE COVID-19 PANDEMIC.

Sub-theme: The nature of the cyber incident that took place in South Africa, and the type of capacity building initiatives that have been undertaken to combat data protection and cybercrime.



This session was centred on discussing the types of cyber incidents, how it changed since the start of the COVID-19 pandemic, and the capacity-building initiatives undertaken in data protection to combat cybercrimes. It was represented by a panel consisting of representatives from Packet Clearing House (PCH), WolfPack Information Risks and the Moses Kotane Local Municipality.

The panel members began the session with a description of the types of cybersecurity attacks that have been experienced by organisations and individuals. Ransomware attacks were identified as the most common type of cyberattacks. A ransomware attack is a type of malware that encrypts a victim's files, and the attacker demands a ransom from the victim to restore access to the data upon payment. Fortunately, in the context of the two ransomware attacks reported, organisations have robust recovery systems in place to recover the stolen information without paying the demanded ransom.

Other attacks included hacking, in which an attacker hacks a company system or school's email addresses and creates keywords for notification of payments and invoices to alert them when payment activity is taking place. Government departments, organisations and schools are prone to such cyber security attacks.

The panel members agreed that individuals were prone to online abuse, which includes a diversity of malicious behaviours ranging from sharing embarrassing or cruel content about a person, to impersonation, doxing, stalking and electronic surveillance to the non-consensual use of photography and violent threats. In fact, it was noted that online abuse is mostly targeted at women, which is sometimes called Cyber-sexism or cyber-misogyny. Cyber-attacks differ with every incidence, but most cyber-attacks experienced in South Africa were mainly aimed at extorting money and/or in some instances, malevolent engagements.

They stressed the importance of creating awareness programmes aimed at educating the public of their security and privacy rights. There was a general consensus among the panel members that people, especially end-users, do not know their rights. Unless they are likely to be affected by cyber security on a personal level, they are often not interested in cyber security workshops. Therefore, it was recommended that awareness and education campaigns need to address how individuals can protect themselves from cyber-crimes.

THEME: PRIVACY AND PROTECTION OF PERSONAL INFORMATION.

Sub-theme: The data cyber security and protection legislation is in place in South Africa, how it is regulated, the challenges, failures, and successes.



THE SESSION FOCUSED ON CYBER SECURITY AND DATA PROTECTION LEGISLATION IN SOUTH AFRICA.

The Protection of Personal Information Act, also known as POPIA, is South Africa's data protection law. It seeks to safeguard personal information that is both off and, on the Internet, to protect people from harm.

The panel, which was represented by Digitally Legal, the Information Regulator, and Film and Publications Board (FPB), who brought different perspectives on cyber security and data protection legislation in place in South Africa, as well as the challenges, failures, and successes.

The session began by acknowledging that South Africa is not a cyber-secure country. It is the 31st worst country in the world when it comes to cyber security. It has poor data protection and practicing processes, therefore, highlighting the importance of POPIA in setting standards that ensure the protection of personal information. They expressed their confidence in the Information Regulator's capacity to enforce compliance of POPIA.

There was a general consensus among the panellist that more needs to be done to address the literacy of South African citizens on their right to privacy, as well as reporting mechanisms in place, which illiteracy could have arisen because of socio-economic dynamics.

They stressed the importance of a partnership between citizens, regulators, and industry players, to ensure that government is supported to effectively regulate the industry.

It was stressed that the 1st of July 2021, was the sunset day where private and public bodies needed to be POPIA compliant.

THEME: CRITICAL INTERNET RESOURCES – DOMAIN ABUSE, WHOIS ACCESS MODEL AND LAW ENFORCEMENT

Sub-theme: What are the current domain name abuse incidents in South Africa, and how have they been resolved?



THIS SESSION SOUGHT TO ENGAGE PANELLISTS ON CRITICAL INTERNET INFORMATION. IDENTIFYING WHAT THE CURRENT DOMAIN NAME ABUSE INCIDENTS IN SOUTH AFRICA WERE AND HOW THEY HAVE BEEN RESOLVED.

As with the session above, the panel, which was represented by stakeholders from ZA Central Registry (ZACR), Domain Name Services (DNS) and Department of Communications and Digital Technologies (DCDT), shared consensus that everything begins with domain names. This is important as the country moves forward with 4IR and the Internet of Things. Domain names provide digital identity and online presence.

In this regard, South African registries are responsible for preventing data breaches, and ensuring that domain-name abuse does not take place in South Africa. In the past year, registries noticed the spoofing of Covid-19-related domain names. This was obviously due to the COVID-19 pandemic. However, the abuse of domain names seen by registries, includes scamming, phishing, and IP infringements, which are all dealt with differently.

The biggest challenge that registries experience from domain abuse is that of privacy concerns. Therefore, registrants do not provide accurate information. This consequently deteriorates the value of registry data, and law enforcement cannot act against domain abuse. Another challenge that they spoke about was the lack of synergy between registries and law-enforcement agencies. One of the panel members acknowledged that, there is no end-to-end flow of information between registries and law enforcement agencies. He added that this has made it difficult for registries to come up with mitigation strategies against domain abuse. As it currently stands, registries are reactive and not proactive to domain abuse. Dispute resolution is a reactive strategy. This is simply because of the lack of synergies in the flow of information on complaints lodged with law enforcement.

The Panel members stressed the importance of working together with law enforcement in addressing infringements and domain abuse.

An important, statistical observation in the complaints of domain-name abuse is that there is a general decline in complaints. The panel member acknowledged that, before 2018, there were 59 cases lodged for abuse. These complaints were from 55 different domain names. In 2020, there was an increase in the number of domain-name registrations. There are 1.3 million domain-name registrations, but only 25 abuse cases were lodged that year. These cases were from 37 different domain names. Another panel member argued that the decrease in the number of domain-name abuse cases are due to the measures, rules and regulations that are in place. They ensure that domain-name abuse is taken seriously and that offenders will not get away with such abuse.

GOVERNANCE OF THE PROCESS (STEERING AND ORGANISING COMMITTEE ENGAGEMENTS)

The preparatory process for the ZAIGF 2021, was facilitated by the ZAIGF committee, together with ZADNA (The secretariat of Internet Governance in South Africa). The committee held weekly meetings to discuss the Internet Governance focus, and to suggest topics for the ZAIGF and speakers to be invited to form panels to speak to the topics agreed upon. The committee, together with the secretariat, secured the speakers and shared the invitation for the general public and ZADNA members.

The committee decided to hold the entire engagement online over the Zoom platform, with an extension to YouTube and Twitter. It took place over two full days and ended with the voting and appointment of new committee members who would replace the existing committee members

FEEDBACK FROM PARTICIPANTS AND SPEAKERS

Comments on the preparatory process

- Sessions were very informative with increased participation of women.
- Some participants raised non-exclusion of other relevant stakeholders such as USAASA as panellists.
- it was highlighted that the invitations went out rather late, with limited time for publicising the event on social media platforms and the Internet.

RECOMMENDATIONS

- Norms and regulations imply a long process and consultations, while technology is developing fast. This is one of the reasons why it is necessary to act jointly concerning the multi-stakeholder model, in the sense that all relevant actors need to work together to create a safer and trustworthy online environment.
- Barriers to Internet Governance should be dealt with to reflect the value of the Internet, by modernising rules, legislation, and policies.
- As the future of this country, we need to focus on growing our Internet access and inclusion so that we can evolve along with the rest of the world.
- Internet Governance should continue to be given high priority, as decisions in this domain have a direct impact on the life of all South Africans and the future of our societies, including the stability of their human rights with respect to access and inclusion.

AN IMPORTANT,
STATISTICAL OBSERVATION
IN THE COMPLAINTS OF
DOMAIN-NAME ABUSE IS
THAT THERE IS A GENERAL
DECLINE IN COMPLAINTS





South African
Internet Governance Forum
ZAIGF



communications
& digital technologies
Department:
Communications & Digital Technologies
REPUBLIC OF SOUTH AFRICA

DAY 1: 24 MARCH 2021

OPENING CEREMONY: 09:00-10:00

- >Opening and welcome: ZADNA CEO Mr. Molehe Wesi
- >Overview of the 2021 ZAIGF: Mr. Thato Mfikwe
- >Presentation by Honourable Pinky Kekana: Challenges within the Internet governance space.

SESSION 1: EDUCATION AND ACCESS TO THE INTERNET: 10:00-11:00

Moderator: Ms. Kelebogile Molopyane

Discussion: Internet access as an enabler for the acquisition of skills, knowledge and information for marginalised communities and rural areas, especially during the pandemic: What has been done to improve quality access and online education. What are the successes, failures, and recommendations to move forward towards a better future.

Panel: BBI, USAASA, KONECTA, NEMISA



TEA BREAK 11:00 – 11:30

SESSION 2: UNIVERSAL ACCESS AND CONNECTING THE UNCONNECTED: 11:30-12:30

Moderator: Ms. Dudu Mkhwanazi

Discussion: Community Networks (CN) continue to connect the unconnected and marginalised in the most affordable way, but they still face challenges. How is USSASA supporting the work of CNs with its successes and challenges? What regulatory challenges are faced, and what are the new policy developments to curb this?

Panel: DAGELF(WISP), ICASA, DCDT, SAWICT

2021 ZAIGF AGENDA

DAY 1: 24 MARCH 2021

SESSION 3: ENHANCING A MULTI-STAKEHOLDER APPROACH IN SA: 12:30-13:30

Moderator: Mr. Muzi Makhaye

Discussion: Multi-stakeholder approach in infrastructure development and cyber security

Panel: Civil Society, DCDT, DIAMATRIX, UJUDIGITAL



LUNCH 13:30 – 14:30

SESSION 4: DIGITAL ECONOMY AND OPPORTUNITIES: 14:30–15:30

Moderator: Dr. Vukosi Marivate

Discussion: Integration of the real economy with the digital economy and effects of AI and 5G

Panel: Ecommerce, IfoundIT, Proudly SA, Brand SA, PAICTA, CHEKALEFA



Wrap up and Close of the 1st Day: 15:30 – 16:30

Speaker: ZA Committee Member

2021 ZAIGF AGENDA

THEME
'DIGITAL
INTER(DEPENDENCE)'

DAY 2: 25 MARCH 2021

OPENING AND WELCOME: 09:00 - 09:30

Speaker: Ntsako Manganyi

RECAP OF DAY ONE AND DAY 2 OVERVIEW: 09:30 - 10:00

Speaker: Andile Skosana

SESSION 5: UNLOCKING THE DIGITAL POTENTIAL WITH SKILLS DEVELOPMENT IN THE DIGITAL AGE (216 IG LIST): 10:00 - 11:00

Moderator: Ms. Nomshado Lubisi

Discussion: Digital literacy programme designed to empower young people and educate them on how to use the Internet responsibly

Panel: Girl Code, Girl Hype, MMA, BITF



TEA BREAK 11:00 – 11:30

SESSION 6a: DISINFORMATION IN THE LEAD UP TO 2021 LOCAL GOVERNMENT ELECTIONS: 11:30 - 12:15

Moderator: Ms. Nomshado Lubisi

Discussion: Lessons learned during Covid-19, and platform responsibilities. Impact on the media, and discussions with stakeholders.

Panel: Google SA, MMA

2021 ZAIGF AGENDA

DAY 2: 25 MARCH 2021

SESSION 6b: PROMOTING CYBER SECURITY DURING THE COVID-19 PANDEMIC (211 IG LIST): 12:15 – 13:00

Moderator: Dr Kiru Pillay

Discussion: What kind of cyber incidents took place in SA, and how it has changed since the start of the pandemic. What capacity building initiatives have been undertaken in data protection and combating cyber-crime.

Proposed panel: Inx-Za, DCDT, Wolfpack, Moses Kotane Local Municipality

SESSION 7: PRIVACY AND PROTECTION OF PERSONAL INFORMATION: 13:45 – 14:30

Moderator: Mr. Lucien Pierce

Discussion: What is the cyber security and data protection legislation in place in South Africa, how is it regulated, and the failures, challenges and successes.

Proposed panel: FPB, Information Regulator, Adv Zanyiwe Asare



LUNCH 14:30 – 15:15

SESSION 8: CRITICAL INTERNET RESOURCES - DOMAIN ABUSE, WHOIS ACCESS MODEL AND LAW ENFORCEMENT: 15:15 – 16:00

Moderator: Mr Peter Madavhu

Discussion: What are the current domain abuse incidents in SA. How have they been resolved, and what has been the successes and failures?

Proposed panel: ZACR, DNS, DIAMATRIX

ZA MULTISTAKEHOLDER COMMITTEE ON INTERNET GOVERNANCE ELECTIONS: 16:00 – 17:00

Moderator: Mr Peter Madavhu

WRAP UP AND CLOSURE OF THE ZAIGF: 17:00 – 17:30

Speaker: Molehe Wesi

ZAIGF is governed by a committee elected by its members. We are pleased to share that several individuals will be joining as ZAIGF committee members. Their addition to the forum will help to continue to position ZAIGF as a critical multi-stakeholder platform, which facilitates dialogue on public policy issues, inherent to Internet Governance in an open and transparent manner.

THE OUTGOING ZAIGF COMMITTEE MEMBERS ARE:

- Mr Peter Madavhu, outgoing ZAIGF Chairperson from .ZA Domain Name Authority (ZADNA).
- Mr Moses Hoboyi, Committee Member from the Department of Communications and Digital Technologies (DCDT).
- Ms Komeshni Patrick, Committee Member from ThinkCode.
- Mr Ntsako Manganyi, Committee Member from Media Monitoring Africa (MMA).
- Mr Andile Sefiri Skosana, Committee Member from Masitech.
- Mr Thato Mfikwe, Committee Member from ISOC Gauteng Chapter.

THE INCOMING ZAIGF COMMITTEE MEMBERS ARE:

- Ms Kelebogile Molopyane, CEO of Africa Beyond the Fourth Industrial Revolution (AB4IR), and one of the founding directors of the Drone Council South Africa.
- Ms Baratang Miya, the founder and CEO of Girlhype.
- Mr Thato Mfikwe, the CEO of the Soweto Wireless User Group and the president of the Internet Society South Africa, Gauteng Chapter.
- Ms Nomshado Lubisi, communications manager at Media Monitoring Africa.
- Adv Lerato Seema, the Policy, Licensing and Regulations Manager at .ZA Domain Name Authority (ZADNA).
- Dr Kiru Pillay, the Chief Director of Cybersecurity Operations, at the Department of Communications and Digital Technologies.
- Ms Tinyiko Simbine, the Co-founder and CFO of GirlCode.
- Adv Zanyiwe Asare, the Director of Digitally Legal.

The new committee members will serve a three-year term, providing both diversity of perspective and depth of expertise.

WE WELCOME
the new committee members, and extend a
HEARTFELT THANK YOU
to the outgoing committee members for their
contributions and dedication to ZAIGF's mission.

