MINISTRY
COMMUNICATIONS AND DIGITAL TECHNOLOGIES
REPUBLIC OF SOUTH AFRICA

KEYNOTE ADDRESS BY THE DEPUTY MINISTER OF COMMUNICATIONS AND DIGITAL TECHNOLOGIES, HON PHILLY MAPULANE AT THE SOUTH AFRICAN INTERNET GOVERNANCE FORUM (ZAIGF2024), UNIVERSITY OF JOHANNESBURG 29 FEBRUARY 2024

Programme Director

ZADNA Board Chairperson, Ms. Palesa Legoze ZAGNA
Deputy Chair Ms Veronica Motloutsi CEO of FPB Dr Mashilo
Boloka

Director of School of Consumer Intelligence and information Systems Dr

Stella Bvuma

Chairperson of ZAIGF, Ms Latty Thlake and your committee members Senior officials from the Department

Distinguished guests, Ladies &
Gentlemen

Good morning!!

Let me take this opportunity and thank the South African Domain Name Authority (ZADNA), in collaboration with the South African

Internet Governance Forum (ZAIGF), for the invitation to come here and address you at this important gathering. Convened under the theme, "**Empowering South Africa's Internet Growth through Multi-Stakeholder Collaboration, Safety, and Resilience**." The South African Internet Governance Forum provides a crucial platforms for stakeholders to engage on what progress we have made in our commitment to fostering an inclusive, secure and innovative digital future for South Africa and to protect its sovereignty.

This Forum serves as a crucial platform for us to engage in constructive discourse and foster collaboration and cooperation on various elements of Internet Governance. This forum, the 2024 ZAIGF, is following on the successes of the previous forums, were robust discussions on critical Internet governance pillars such as infrastructure, cybersecurity, human rights, legal and regulatory frameworks, economic development, and socio-cultural aspects took place.

Madam Chairperson,

The South African Internet Governance Forum (ZAIGF) is pivotal in South Africa's digital landscape. The significance arises from the growing importance of the Internet in driving the nation's advancement across various sectors, including commerce, education, healthcare, governance, and entertainment. Since 2012, internet access has been acknowledged as a fundamental human right, aligning with the United Nations Human Rights Council's affirmation of individuals' freedom of expression and opinion.

Ensuring sustainable access and fostering the robust growth of a secure and reliable internet infrastructure necessitates concerted efforts from diverse stakeholders. These collaborative efforts involve active participation from governmental bodies, private enterprises, civil society organizations, technical experts, and academic institutions in shaping policies and strategies for managing South Africa's internet ecosystem.

Given the inherently global nature of the Internet and the diverse interests of stakeholders invested in its evolution, the multi-stakeholder approach emerges as a fitting model for its governance. This approach facilitates ongoing internet development and holds broader applicability in digital governance realms.

However, adopting a multi-stakeholder approach presents its own set of challenges. These processes can be intricate and time- consuming, potentially susceptible to influence from vested interests. Moreover, existing multi-stakeholder mechanisms often address only a fraction of the multifaceted challenges arising from the widespread adoption of the Internet, leading to fragmented solutions lacking input from all relevant stakeholders.

Despite these challenges, the Department of Communications and Digital Technologies remains committed to fostering multi-stakeholder dialogues on Internet governance. This commitment stems from recognizing an open, secure, and nationally interoperable Internet in driving social and economic progress. As internet usage continues to surge, the ZAIGF retains its strategic and economic significance, serving as a forum to address critical issues such as privacy, data governance, combatting illicit content, tackling misinformation, and navigating the implications of emerging technologies like blockchain and artificial intelligence.

Approaching the 20-year review of the World Summit on the Information Society (WSIS+20), the ZAIGF provides a platform for reflection on leveraging multi-stakeholder, people-centered, inclusive, development- oriented, and non-discriminatory models to tackle internet governance challenges.

CURRENT STATE OF INTERNET PENETRATION IN SOUTH AFRICA

In 2022, Statistics South Africa conducted a country-wide Census which was the **first digital** Census conducted in the country, thus confirming that we are living the digital era. The results of the Census, which were released last year in October 2023. The results of this census indicated that there has been an upward trend in access to the internet services over the period 2011 -2022. According to the report, households with no access to internet decreased threefold (from 64,8% in 2011 to 21,1% in 2022). This represents an internet penetration of 78,9% in 2022. This is a commendable advance in attaining the technology goals of the National Development Plan of creating an inclusive information society and position the government to play an enabling role in the provision of broadband to underserved areas by ensuring that 80% of South Africans have access to the internet by 2030. The latest figures places us at the beach head not only of attaining the NDP goals but we have a possibility of surpassing them and connecting 100% of South Africans by 20230.

This penetration rate places South Africa at the of the rankings of internet penetration and freedom in the continent. This gives us the edge towards bridging the digital gap and help in global efforts to connect the 2.7 billion people across the world who remain unconnected.

ENHANCING ONLINE SAFETY AND CYBERSECURITY

However the advances we've made in internet penetration and use, which introduced greater variety and convenience into our lives, also opens more and more avenues for people to be targeted by cyber criminals and exposes us to many internet ills.

International and domestic cyber criminals increasingly view businesses and private individuals as attractive targets for a range of cybercrime.

This 'digital paradox' means that while governments and organisations can offer more services, more quickly, than ever before, yet at the same time cybercrime has become a powerful countervailing force that's limiting that potential.

The Cybersecurity threat landscape is exponentially growing in complexity aided by the increasing sophistication of threat actors, with threats characterised by speed and scale of propagation.

Critical infrastructure and critical information infrastructures, which is owned and operated by both government and the private sector, has become a strategic imperative especially in the light of recent attacks and so building cyber resilience throughout the national infrastructure is an imperative.

The borderless and seemingly indiscriminate nature of cyber-attacks mean it is of vital importance that organisations fund and implement measures that protect themselves and clients from financial losses, and the organisation from reputational damage and emerging regulatory imperatives.

Cybersecurity is of high priority in South Africa. We have experienced cyber-attacks especially data breaches, but we are learning from them.

As a country we have emerging legislative framework which include Cyber- crimes Act, Privacy Act and we are looking into a more enabling legislative.

It is against this backdrop that the Department established a Cybersecurity Hub in October 2015, which is one of the national Computer Security Incident Response Teams (CSIRTs) and which is aimed coordinating the cybersecurity domain in the private sector and civil society.

ROLE OF DIGITAL LITERACY IN EMPOWERING USERS TO NAVIGATE THE ONLINE WORLD SAFELY

Digital literacy has a role in empowering users to navigate the online world safely. Digital literacy is not just the ability to use digital devices, but the capacity to understand, critically evaluate, and use digital content in an effective and ethical manner.

In our increasingly digital world, digital literacy is as fundamental as reading and writing, serving as a key enabler for participating in the digital economy, accessing information, and engaging with society.

Digital literacy empowers users by providing them with the skills to distinguish between credible and unreliable information online, reducing the risk of misinformation and disinformation.

A digitally literate population is better equipped to recognize and avoid cyber threats such as phishing scams, malware, and other forms of cyberattacks, thereby enhancing individual and collective cybersecurity.

Educational institutions should integrate digital literacy into their curricula, ensure that students from all backgrounds have the opportunity to develop these essential skills.

ROLE OF ARTIFICIAL INTELLIGENCE

The United Nations estimates that over a billion new users have been added to the internet globally over the last five years. Yet one third of the world's population, approximately 2.6 billion people, are not connected to the internet.

South Africa, like many other countries especially the developing countries, is contending with this reality of bridging the digital divide, with vast disparities in access to education, healthcare, and economic opportunities. The rapid evolution of artificial intelligence (AI) presents both opportunities and challenges in addressing these gaps. However, in a society marked by significant resource inequalities, the utilization of AI technologies could either alleviate or exacerbate existing disparities, particularly in terms of employment and essential service accessibility.

ARTIFICIAL INTELLIGENCE INSTITUTE OF SOUTH AFRICA (AI HUBS)

AI's increasing presence in the workplace and its potential impact on job opportunities across various sectors - AI-powered tools, like ChatGPT, are increasingly proficient in tasks traditionally performed by humans, such as coding, software vulnerability identification, and content creation. As AI progresses, concerns arise regarding potential job displacement among knowledge workers, such as programmers, lawyers, and therapists.

As such, the Presidential Commision of the 4^{th} Industrial Revolution recommended that as a country we need to position ourselves and get the benefits from artificial intelligence and emerging technologies. Institutions of higher learning as centres of knowledge and development play a very critical role in ensuring that the future we envision as a country and the continent at large is realised, hence the Department is in collaboration with the University of Johannesburg and the Tshwane University of Technology and now going to the Central University of Technology to establish the hubs of the Artificial Institute of South Africa.

AI's capacity to automate routine tasks, thus shifting the focus of human workers towards more complex, creative, and decision-making roles must be harnessed. Educational and training initiatives are essential to prepare individuals for an AI-centric workforce and facilitate their transition into new roles as AI evolves.

Furthermore, it has the potential to generate new job opportunities through innovation and economic growth, particularly in AI research, development, and maintenance. This requires ensuring South Africa's workforce readiness for these emerging opportunities and promoting equitable access to education and training.

The collaboration among government, industry, academia, and civil society is essential for developing policies and strategies addressing AI challenges and harnessing its benefits for the workforce.

Programme Director,

However, ethical considerations, including transparency, accountability and privacy protection are central to the conversations on AI. It is crucial to safeguard user rights and freedoms while addressing potential biases in AI algorithms. Interdisciplinary collaboration is vital for developing a robust ethical framework guiding AI's responsible use, promoting human rights, social justice, and inclusivity in society.

MEASURES TO IMPROVE INTERNET RESILIENCE

It is critical to build resilient internet infrastructure capable of withstanding various challenges such as natural disasters, cyberattacks, and surges in demand, by among others

- Investmenting in redundant network architectures, data centers, and cloud services as part of the strategy to enhance resilience.
- Investing in innovation and emerging technologies in ensuring the reliability and sustainability of internet services.

CONCLUSION

As the 6th administration, we are committed to South Africa's internet growth through multi-stakeholder collaboration, safety, and resilience.

We are committed to continued cooperation and innovation among all stakeholders to achieve a digitally inclusive society.

Through our flagship programme, SA Connect we shall continue to strive to bridge the digital divide in our society by connecting the unconnected.

I wish you fruitful engagements at this 8th instalment of this forum and a successful conference.