MINISTRY
COMMUNICATIONS AND DIGITAL TECHNOLOGIES
REPUBLIC OF SOUTH AFRICA

Private Bag X860, PRETORIA, 0001 – iParioli Office Park, 1166 Park, Hatfield, PRETORIA

Tel: +27 12 427 8000 – Email: Media@DCDT.gov.za URL: www.dcdt.gov.za

SPEECH BY DEPUTY MINISTER OF COMMUNICATION AND DIGITAL TECHNOLOGIES, MR MONDLI GUNGUBELE (MP) AT THE OFFICIAL OPENING OF THE 2ND ANNUAL CYBERSECURITY INDABA, PRETORIA. 29 NOV 2025

Programme Director, Mr Fingerz

Captains of industry,

Partners from the private and public sectors,

Innovators and students,

Esteemed guests,

Ladies and gentlemen,

Good morning!!

It is an honour and privilege to join you today at the 2025 Cybersecurity Indaba, under the fitting theme “Next-Gen Cybersecurity: Innovation for Tomorrow’s Challenges.”

This gathering comes at a defining moment not just for cybersecurity professionals, but for South Africa’s digital destiny. We stand at the intersection of immense opportunity and growing risk, a place where the choices we make today will shape the digital landscape of our nation for generations to come.

Its these gatherings that reminds us that a secure digital Africa begins with each of us and every organization, every citizen, and every click contributing to a safer online community.

South Africa is rapidly digitising. From digital government services and e-health to online education, fintech, and digital agriculture, our society is becoming increasingly connected and data-driven. Digital transformation offers us a pathway to inclusion, to innovation, and to economic renewal. It enables small enterprises to reach global markets, farmers to access real-time weather intelligence, and young people to build careers that did not exist a decade ago.

But as we embrace these opportunities, we face an uncomfortable paradox: the more we digitise, the more we expose ourselves to cyber risk. Cybercrime in South Africa has escalated sharply, affecting our citizens, our financial institutions, and even critical national infrastructure. Reports show that South Africa ranks among the most targeted countries in Africa for ransomware, phishing, and business email compromise.

And beyond economic loss, the threat goes deeper. Cyber threats erode public trust, weaken national security, and can undermine the digital public infrastructure that underpins modern governance. This is the new reality of our digital age one that demands a new kind of vigilance, a new kind of innovation, and a new kind of leadership.

So, what does it mean to shape South Africa’s digital future?

It means ensuring that as our country digitises through initiatives like the National Digital and Future Skills Strategy, Broadband rollouts, and Digital Public Infrastructure cybersecurity is not an afterthought, but a foundation, security by design.

Ladies and gentlemen**,**

Our vision should be to build a cyber-resilient nation, one that is not only just connected, but also secure; not only innovative, but also trusted. To achieve this, we must weave

cybersecurity into every thread of our digital transformation from policy and infrastructure to education and innovation.

We must recognise that cybersecurity is not a cost, but an enabler of digital trust, and therefore an enabler of digital progress. Trust is the currency of the digital economy. Without it, citizens will hesitate to use digital ID systems, businesses will be reluctant to move online, and innovation will stall.

So, shaping South Africa's digital future is, at its core, about protecting trust the trust of our people, our businesses, and our partners. The cybersecurity landscape is evolving faster than ever before. We now live in a world of AI-powered attacks, deepfakes, and data manipulation threats that blur the line between truth and deception, security and vulnerability. Our students here are the primary victims.

Cybercriminals are exploiting machine learning to automate attacks, quantum computing threatens to disrupt encryption as we know it, and the Internet of Things introduces millions of new attack surfaces into our networks. This new threat environment demands more than reactive measures it demands next generation thinking. Traditional cybersecurity models firewalls, perimeter defences, and isolated incident response are no longer enough.

Fellow government leaders and industry partners,

We need proactive, adaptive, intelligence-driven security systems that can predict, prevent, and respond in real time. That means integrating artificial intelligence, cloud security, behavioural analytics, and zero-trust architectures into our core digital infrastructure.

But technology alone is not enough. We need a culture of cybersecurity, one that begins in our schools, continues in our workplaces, and is embedded in our public institutions. If we are to advance cybersecurity innovation for the next generation, we must harness South Africa's greatest resource, its people.

Across our universities, SMMEs, and research centres, there is extraordinary talent waiting to be unlocked.

The Department of Communications and Digital Technologies (DCDT) through Cybersecurity Hub in partnership with institutions such as the CSIR, is already laying the groundwork for this ecosystem. But to go further, we must strengthen four key innovation pillars:

Research and Development (R&D)

We must invest in local R&D to develop home-grown cybersecurity solutions tools that understand our local context, languages, and threat environments. This means supporting innovation hubs, university labs, and public-private partnerships that turn academic research into market-ready technologies.

Skills and Capacity Building

The future of cybersecurity lies in the skills of our young people. We must nurture the next generation of ethical hackers, analysts, digital forensics experts, and AI security researchers. Cybersecurity education must become mainstream, not confined to computer science departments, but part of our national digital literacy. We must make cybersecurity careers accessible, attractive, and aspirational.

Cybersecurity is a team sport (collaboration)

No single institution can secure the digital future alone. We must strengthen collaboration between the government, private sector, academia, civil society, and international partners. By sharing threat intelligence, best practices, and innovations, we can build a collective shield that protects our national interests.

Policy and Regulation

Innovation thrives in an environment of clarity and trust. Our regulatory frameworks, from data protection and privacy laws to cybersecurity legislation, must keep up with

technology. We must balance security with innovation, ensuring that regulation empowers rather than restricts progress.

To the partners from the private and public sectors**,**

Together, these four pillars R&D, skills, collaboration, and policy, will form the foundation of a resilient, innovative cybersecurity ecosystem for South Africa. To the young people in the audience, students, researchers, and digital innovators, this moment belongs to you. You are not just users of technology; you are architects of the future.

The cybersecurity challenges of tomorrow will not be solved by the tools of yesterday they will be solved by your creativity, your innovation, and your courage to question the status quo. You must see cybersecurity not as a barrier, but as a pathway to empowerment.

From developing AI-driven threat detection systems, to creating secure fintech platforms, to designing privacy-respecting data systems, the next generation must lead the charge toward a secure, inclusive digital society.

Our digital future does not exist in isolation.

South Africa's cybersecurity journey is part of a continental and global mission to ensure that Africa's digital rise is underpinned by security and trust. Through frameworks such as the African Union Convention on Cybersecurity and Data Protection (Malabo Convention) and initiatives under SADC, ITU and BRICS, we are helping to build a harmonised cybersecurity architecture for Africa.

This cooperation allows us to share expertise, strengthen resilience, and promote African-led cybersecurity innovation that reflects our values and priorities. We must continue to champion cyber sovereignty the principle that nations should have the capacity and autonomy to protect their own digital infrastructure, while upholding global norms of openness and cooperation.

Ladies and gentlemen, the future is being written right now in our policies. If we want a digital future that is inclusive, secure, and prosperous, we must act decisively today.

Let us:

• Invest in next-generation cybersecurity research and innovation.

• Empower youth and women in the digital security field.

• Strengthen public-private partnerships for digital resilience.

• Modernise our laws to address emerging technologies like AI and quantum computing.

• And most importantly, embed cybersecurity into every national digital transformation strategy from health and education to infrastructure and industry.

Because the question is not whether we will face new cyber threats, we will. The question is whether we will be ready. And readiness requires foresight, innovation, and unity. In closing, shaping South Africa's digital future is not just about technology; it is about people, trust, and purpose. It is about ensuring that the next generation inherits not a fragile, fragmented digital world, but one that is secure, trusted, and empowering.

Let us be the generation that built the foundations of a cyber-resilient South Africa where innovation thrives, where privacy is protected, and where every citizen can safely participate in the digital economy. The journey ahead will not be easy. But if we work together across sectors, across disciplines, and across generations, we can build a digital future worthy of our nation's promise.

As we embrace the theme of Next-Gen Cybersecurity: Innovation for Tomorrow's Challenge, let us remember: Innovation without security is unsustainable. But security without innovation is impossible.

Let us pursue both boldly, wisely, and together.

Thank you.