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

KEYNOTE ADDRESS BY DEPUTY MINISTER OF COMMUNICATION AND DIGITAL TECHNOLOGIES, MR MONDLI GUNGUBELE (MP) AT THREAT 2025 CYBERSECURITY CONFERENCE, DURBAN. 04 NOVEMBER 2025

Programme Director,

Threat leadership

Government representatives here,

Industry partners and the academia,

Esteemed guests,

Ladies and gentlemen,

Good morning.

It is an honour to stand here today to official open Threat 2025 under the theme, **"Cybersecurity in the Global South, Language, Locality and Policy".**

It becomes increasingly clear that the future of cybersecurity in the Global South will be shaped not only by technology, but by language, locality, and policy.

The challenges we face are global in reach, yet profoundly local in impact, exploiting our linguistic diversity, our policy gaps, and our uneven access to digital infrastructure.

Threat 2025 reminds us that the challenges of the digital age are no longer distant possibilities, they are present realities demanding coordinated action and resilience.

South Africa is rapidly digitising.

From digital government services and e-health to online education, fintech, and digital agriculture, our society is becoming more connected, more data-driven, and more dynamic than ever before.

Digital transformation offers us a powerful pathway, a pathway to inclusion, to innovation, and to economic renewal.

It empowers our young people to build careers and opportunities that simply did not exist a decade ago.

The mandate of the Department of Communications and Digital Technologies is clear: to steer South Africa toward an inclusive, prosperous, and secured digital future, a future where every citizen can participate, contribute, and thrive in the digital economy.

Ladies and gentlemen,

As we embrace the Fourth Industrial Revolution, rolling out 5G networks, expanding fibre connectivity, and building our digital public infrastructure, we must recognize that the threats we face are becoming just as sophisticated as the technologies we deploy.

Cybersecurity, therefore, cannot be seen as a mere technical add-on.

It is the foundational layer of trust upon which our economic growth, our democracy, and our social progress must rest.

Here in South Africa, we are determined to strike the right balance between safeguarding our national security and advancing our digital connectivity goals.

We are committed to universal access, digital literacy, and the inclusive development of digital public infrastructure that leaves no one behind.

But we must also acknowledge the challenges faced by developing countries.

Many struggle to enforce effective legal responses to transnational cyber threats.

Our institutions are often under-resourced, our skills pipelines too narrow, and our legislative processes too slow to keep pace with rapid technological change.

We must remember that cybersecurity is not only about protection, it is also about principles.

We must continue to balance our security concerns with the respect for human rights and fundamental freedoms that underpin our democratic values.

Cybersecurity Across Cultures: The Power of Perspective

Esteemed guests,

The theme of this conference is both timely and profoundly important.

It reminds us of a crucial truth that the digital world is borderless.

Information flows freely across continents, in milliseconds.

And yet; our responses to cyber threats often remain limited by borders or by local laws, by language, by values, and by societal norms.

Programme director,

Cybersecurity threats do not ask for passports.

From sophisticated ransomware attacks to foreign-influenced disinformation campaigns, they cross national and cultural lines without hesitation.

But how we perceive those risks and how we act upon them, how we choose to report or respond to these are all shaped deeply by our cultural context.

In some societies, cybersecurity is seen primarily as a matter of national defence.

In others, it's about protecting privacy, trust, and digital well-being.

And in many places, there remains a gap between awareness and action and not because of apathy, but because of differences in understanding, priorities, and even language.

That's why this gathering is so important.

By embracing a *triple helix approach*, bringing together industry, policymakers, and academia, we create the conditions to bridge these divides.

We can share not only our technologies but our perspectives.

We can learn how trust is built differently across societies, and how ethics, governance, and innovation can complement and not compete across cultures.

As we move forward, we must go beyond simply translating technical solutions.

We must harmonize our security practices to make them inclusive, accessible, and rooted in the local realities of the people we serve.

Cybersecurity is not just a technical challenge. It's a human one that depends on empathy, collaboration, and cultural understanding.

So, as we begin this conference, let us remember diversity is not a barrier to security but rather it is one of our greatest strengths.

The Global Framework for a Global Threat: The UN Cybercrime Treaty

In our pursuit of harmonisation and shared understanding, we must look to the global frameworks that unite our efforts.

The recently adopted United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes that the UN Cybercrime Treaty is one such milestone.

Its adoption recognises a vital truth that national laws alone can no longer combat transnational cybercrime.

For South Africa, and for much of the Global South, this Treaty represents a historic and foundational step of a shared legal vocabulary for justice in cyberspace.

The Treaty strengthens our global response through three key pillars:
1. Standardised criminalisation, which ensures that our cybercrimes are recognised across borders.
2. Enhanced cooperation, which enables faster investigations and evidence sharing.
3. Capacity building, for supporting developing nations to implement its provisions.

Together, these principles form the basis of a global framework for a global threat and a more secure digital future for all.

Distinguished guests and academics,

Connecting the Treaty to Culture: More Than Just Law

The UN Cybercrime Treaty goes beyond law, it speaks to social and cultural realities.

Its Preamble calls for mainstreaming a gender perspective, recognising that cybercrime disproportionately affects women, girls, and minority communities.

Victim protection measures must be culturally sensitive, considering language, local resources, and societal stigma.

And capacity building acknowledges the digital divide: cybersecurity cannot be global if developing economies lack the skills and resources to cooperate across borders.

In summary, the Treaty fosters not just legal alignment, but a shared, inclusive global security culture.

The Human Layer of Defence: Digital Literacy and Cultural Awareness

The most sophisticated technology is only as secure as its most vulnerable user.

In South Africa, securing our digital future rests on two pillars: digital literacy and culturally informed awareness.

Digital literacy being the ability to use, evaluate, and create content with digital tools and it is no longer a luxury.

It is essential for modern citizenship and the foundation of cyber resilience.

After all, studies show that over 80% of data breaches are caused by human error.

A digitally literate citizen can recognize phishing, avoid malware, and respond appropriately to threats, effectively becoming the first line of defence.

Literacy also fosters digital ethics, helping individuals discern credible information from disinformation, a major societal and political threat.

But awareness alone is not enough.

In a diverse country like South Africa, a one-size-fits-all approach fails.

Cultural norms, demographics, and communication styles shape how people perceive risk and act on it.

Effective cybersecurity is therefore a cultural design challenge, one that requires deep understanding of local realities, languages, and social norms to drive real behavioural change.

Conclusion

The work we do here over the next two days in workshops, panels, and networking breaks is the engine that will drive our secure digital future.

Let us use this conference to build a security architecture that is not only technically robust, but also culturally aware and aligned with global standards.

Let us embrace the spirit of collaboration, ensuring that as South Africa and the continent leap into the digital age, we do so securely, inclusively, and together.

I wish you all a highly productive and successful THREAT 2025.

I thank you!

Ngiyabonga!

Enkosi!