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

ADDRESS BY THE DEPUTY MINISTER OF COMMUNICATIONS AND DIGITAL TECHNOLOGIES, HON PHILLY MAPULANE (MP) AT THE THREAT CYBERSECURITY CONFERENCE HELD AT PROTEA HOTEL TECHNO PARK, STELLENBOSCH ON MONDAY, 20 NOVEMBER 2023

Prof Manoj Maharaj, Conference Chair Esteemed guests

Ladies and Gentlemen, Colleagues,

Good Morning

Thank you for the invitation to address you at this auspicious gathering of Cybersecurity enthusiasts. It is a privilege to stand before you today in the beautiful city of Stellenbosch, a place where innovation and tradition converge, much like the topics we are here to discuss at this distinguished cybersecurity conference.

We are in the town of Stellenbosch, the town that gave us two of the three Boer Generals during the Anglo-Boer war, Jan Smuts and Barry Hertzog who went on to become Prime Ministers after the war.

This is the town that produced the first apartheid Prime Minister, DF Malan.

We are at the home of Stellenbosch University, a university which owes its existence to the generosity of Jan Henoch Marais, the founder of the De Burger newspaper, who when he died in 1915, bequeathed 100 000 pounds sterling (equivalent to more than R100 million today) from his estate to the university through a trust that still carries his name. This endowment enabled the Stellenbosch University management to resist efforts to incorporate it into the new University of Cape Town. Marais's statue still stands in the university campus. His trust, Het Jan Marais Nationale Fonds, is also still in existence. Its mission, as laid down by Marais in his last

will and testament, is to "*advance the national interest on any terrain of the Afrikaans-speaking part of the population of South Africa anywhere in the country, but with preference to the town and the district of Stellenbosch*". In 2016 the fund's capital stood at a hefty R1.29 billion.

This is the University that produced Hendrick Verwoerd, the architect of apartheid, who was a professor of Philosophy here ate the age of 31.

Stellenbosch has always been at the centre of Afrikaners' political and cultural life; it was the incubator for apartheid as an ideology and the embodiment of Afrikaners' desire for Afrikaans mother-tongue education.

But is has now transformed itself into a financial capital of South Africa.

Stellenbosch is home to the head office of the country's leading companies like Mediclinic, Shoprite, Naspers (with market capitalisation in excess of R1.5 trillion), Rupert's Richemont and others, whose size and reach in the South African economy is enormous, with direct stakes of no fewer than 16 of the JSE top 100 companies. Other companies like FirstRand, Capitec, Rand Merchant Bank, Remgro, PSG group etc are either owned or associated with individuals from Stellenbosch.

Ladies and gentlemen welcome to Stellenbosch. This is its history, culture and heritage.

As we gather here today, we are reminded of the rapid pace at which our world is evolving. The digital landscape is no longer a separate entity but an integral part of our daily lives. This integration brings immense opportunities but also significant challenges, particularly in the realms of cybersecurity and digital governance.

Our discussions over the next few days will not only shape the future of cybersecurity but also the future of our societies. We are here to address critical themes that will determine how we navigate this new era of technological advancement.

Cyber threats and cyber crimes

The ubiquitous nature of Cyberspace and the Internet offer numerous advantages for society, especially for developing countries.

However, Cyberspace is also systemically vulnerable to new and serious threats and is attractive to geopolitical competitors and criminals alike.

The introduction of ICTs into many aspects of everyday life has led to the development of the modern concepts of the information society and the digital economy.

Essential services such as water and electricity supply now rely on ICTs, as do most businesses and organisations, as well as citizens.

The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries.

ICT applications such as e-government, e-commerce, e-education, e-health and e-environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services.

ICT applications can facilitate the achievement of the Sustainable Development Goals, reducing poverty and improving health and environmental conditions in developing countries, and in South Africa they help to respond to historical development challenges.

However, the growth of the information society is accompanied by new and serious threats.

While technological transformation introduces greater variety and convenience into our lives, it also opens more and more avenues for people to be targeted by cyber criminals.

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.

Because we spend an inordinate amount of time on the internet, the risks of cyber crimes are higher. In the latest Global Digital Report, drawing data from several sources and research groups, it was established that South Africa has the highest screentime worldwide, averaging 10 hours a day. In other words, South Africans are regarded as the biggest internet addicts in the world, spending an average of 9 hours and 38 minutes daily connected on any device. This is far higher than the global average of 6 hours and over 2 hours more than the USA.

Cyber-attacks

Cybersecurity has never been a higher priority, with recent attacks targeting organisations globally in a series of increasingly sophisticated attacks.

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.

In the recent past, there has been a number of documented attacks. An attack on the United States' Colonial Pipeline caused it to shut down for several days. President Joe Biden called a state of emergency.

In the United Kingdom, a technology supplier to the country's National Health Service fell victim to a ransomware attack in 2022, disrupting important functions.

In mid-2022, Estonia was the victim of its most intense cyber-attack since 2007.

In May last year, a ransomware gang infiltrated Costa Rican government system.

Increased internet penetration across our country can give rise to sophisticated attacks on our ICT infrastructure.

Here at the home front, Transnet was a victim of cyber attack, from which it suffered millions of rands.

Some few weeks ago, the South African National Defence Force also experienced cyber attacks, a development that has embarrassed them so much so that up to today it is still being talked about in hushed tones.

Recent malware attacks in the region have put organisations on high alert and, as a result, the network security market is poised for strong growth rates.

Emerging African Cybersecurity Legislation

In Africa, we are at a pivotal moment in shaping the future of our digital landscape. The recent initiatives in cybersecurity legislation across the continent reflect our commitment to creating a secure, resilient, and equitable digital environment.

The issue of cybersecurity is high on the agenda of many African governments, with many on the continent increasingly mindful of the shared public private responsibility for cybersecurity, and of

the need to mobilise both public and private organisations within a multi-stakeholder model.

A growing number of African countries have established - or are in the process of establishing - an enabling policy and legislative environment for cybersecurity.

Countries like Nigeria, Kenya, and South Africa are at the forefront, implementing comprehensive cybersecurity laws and policies. These legislative frameworks are not just about safeguarding against threats but also about fostering an environment where digital innovation can thrive. They are about ensuring that as our digital footprint grows, so does our ability to protect it.

Quantum Leap: Securing the Quantum Computing Era

As we embrace the quantum computing era, we are not just stepping into a new phase of technological advancement, but we are also venturing into uncharted territories of cybersecurity.

Quantum computing, with its unparalleled processing power, can solve complex problems in seconds, problems that traditional computers would take millennia to solve.

This leap forward offers extraordinary benefits in fields like medicine, logistics, and AI. However, it also brings significant risks, particularly the ability to break conventional encryption methods, exposing our most sensitive data.

Our task is to develop quantum-resistant cryptography and to re-envision our cybersecurity infrastructure, making it robust enough to withstand the quantum threat. We must be proactive, not reactive, in securing our digital future.

AI Frontiers: Harnessing Artificial Intelligence for Cyber Defence

In the domain of artificial intelligence, we stand at a inflection point where

AI's capabilities are expanding rapidly.

AI can significantly enhance our cybersecurity defenses, offering automated threat detection, rapid response to incidents, and predictive analytics to preempt attacks.

But it also raises concerns about AI being used for malicious purposes, like developing sophisticated malware or automating cyber attacks.

The challenge lies in staying ahead of the curve – utilizing AI to fortify our defenses while also ensuring ethical and responsible use.

We must also address the potential biases in AI systems and ensure that our AI-driven security measures are transparent and accountable.

Cybersecurity for a Sustainable Future: Strengthening Resilience in Developing Countries

In addressing cybersecurity for a sustainable future, our focus should be on global inclusivity and resilience. Developing countries often lack the resources and infrastructure to combat sophisticated cyber threats, making them vulnerable targets. Building cybersecurity resilience in these countries is not just an act of solidarity but a strategic necessity for global cybersecurity. We must foster international collaboration, share resources, and provide technical support to build robust cyber defenses globally. Initiatives should include training and capacity building, developing local expertise, and ensuring access to the latest technologies. By strengthening cybersecurity in developing nations, we are building a more secure and resilient global network.

The Bio-Cyber Nexus: Securing the Intersection of Biology and Cybersecurity

The intersection of biology and cybersecurity represents a thrilling yet daunting frontier.

The integration of biotechnology into our digital infrastructure – from health records to DNA sequencing – offers immense benefits in healthcare and research. However, it also opens up new vulnerabilities.

Bio-data breaches can have profound implications, far beyond traditional data leaks.

Protecting this sensitive information requires a unique approach, blending cybersecurity with ethical considerations.

We must develop specialized security protocols and ensure strict compliance and governance in handling bio-digital data. This convergence also highlights the need for cross-disciplinary expertise, where cybersecurity professionals and biotechnologists collaborate to safeguard our bio-digital future.

Securing the Metaverse: Protecting Virtual and Outer Worlds

The concept of the Metaverse, a collective virtual shared space, is rapidly becoming a reality.

As we blend our physical and digital lives, we create new virtual spaces that are ripe for exploration but also vulnerable to exploitation.

Cybersecurity in the Metaverse goes beyond protecting data; it's about ensuring the safety and integrity of virtual experiences.

This includes safeguarding personal identities, protecting virtual assets, and preventing malicious activities in virtual environments.

We must anticipate the evolution of cyber threats in these spaces and develop innovative security solutions.

As we protect these new virtual frontiers, we are not just guarding bits and bytes, but the very essence of human interaction and experience in the digital age.

Department's response

Against the backdrop of the National Cybersecurity Policy Framework (NCPF) 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 at coordinating the cybersecurity domain in the private sector and civil society.

"Cybersecurity Hub" means a CSIRT established to pool public and private sector threat information for the purposes of processing and disseminating such information to relevant stakeholders including the Cybersecurity centre.

The Hub was established and operationalised in 2016, with the specific mandate to act as the national CSIRT responsible for the private sector and citizens.

The Cybersecurity Hub successfully became a member of the Forum of Incident Response and Security Teams (FIRST) in March 2022, which make the Hub the second state institution to be a FIRST member

As a result of the Hub's FIRST membership there has been an increased level of engagement with other national CSIRTs globally, which allows the Hub access to credible cybersecurity threat information which ideally should be shared with the Hub's strategic partners including sector-CSIRTs and other state institutions.

The Cybersecurity Hub has cultivated strong relationships with various sector-CSIRTs including:

- The South African Banking Risk Information Centre (SABRIC), which represents the commercial banks.
- The Communications Risk Information Centre (COMRIC) which represents the mobile operators.
- The Internet Services Providers Association (ISPA) which represents internet service providers.

The roles of sector-CSIRTs are among others to:

- be a point of contact for that specific sector on Cybersecurity matters;
- coordinate Cybersecurity incident response activities within the sector;
- facilitate information and technology sharing within the sector;
- facilitate information sharing and technology exchange with other sector CSIRTs;
- establish national security standards and best practices for the sector; and
- conduct cybersecurity audits, assessments and readiness exercises for the sector and provide sector entities with best practice guidance on ICT security.

The Hub has formal relationship with the sector-CSIRTs in order to better exchange threat information, collaborate on awareness and other initiatives and in so doing improve the overall threat posture of the country.

One of the primary mandates of the Hub is for the development and implementation of national awareness programs. The following programs have been developed together with associated artefacts:

- SMME Toolkit
    - successfully developed a Cybersecurity and Data Protection Toolkit for Small, Medium, Micro-sized Enterprises (SMMEs), which provides the tools and knowledge to better guard against cybersecurity risks and drive better compliance with the Protection of Personal Information (POPI) Act and international data protection legislation. Partnered with the Information Regulator.
- Schools Toolkit and Schools Awareness programs
    - Successfully developed a Cybersecurity Awareness Toolkit includes workbooks, videos, games, posters etc., aimed at school learners, teachers and parents.
    - The workbooks that were developed have been translated into 11 languages (English, Afrikaans, isiZulu, isiXhosa, isiVenda and SeSotho, Sepedi, Tswana, Tsonga, Swati and Ndebele).
    - The Cybersecurity Awareness Schools' toolkit targets school learners, teachers and care givers and includes workbooks, videos, posters. It is being rolled out to all Schools in collaboration with DBE

Conclusion

As we delve into these critical themes, let us remember that cybersecurity is not just a technical challenge but a societal one. It is about protecting our way of life in an increasingly interconnected world. The conversations we have and the decisions we make at this conference will echo beyond these walls, shaping the future of cybersecurity not just in Africa but across the globe.

I thank you.