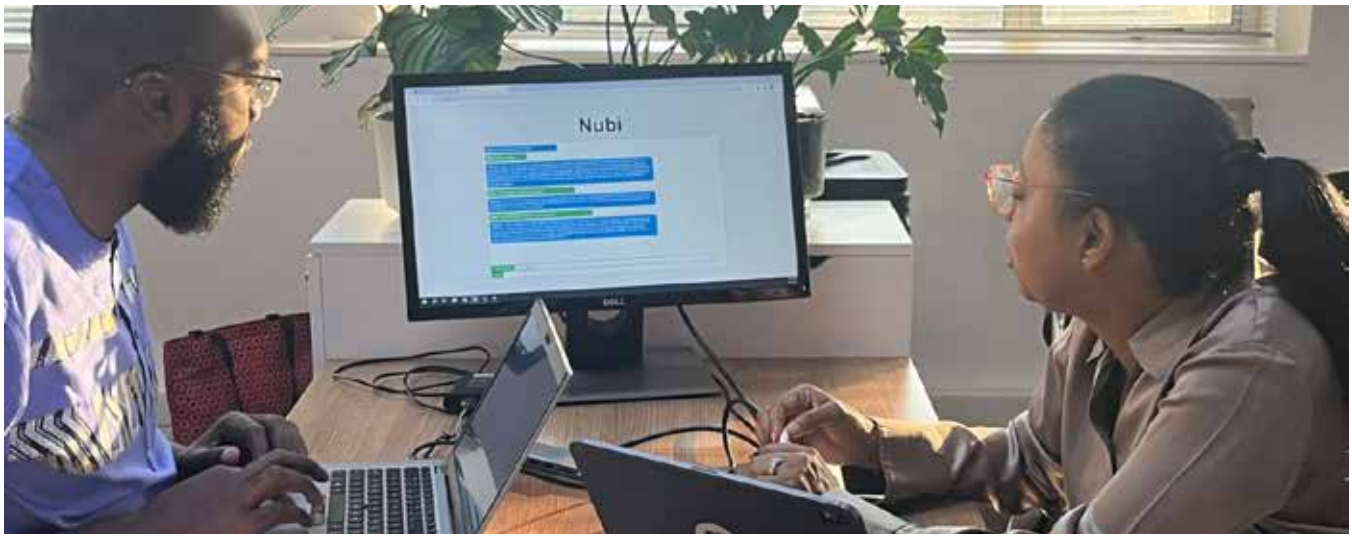
Threat2023 Conference:

Navigating cyber threats and AI opportunities for a brighter digital future



The recent THREAT2023 Cybersecurity Conference held in Stellenbosch in November gathered global experts from government, academia and industry to explore the cutting edge of cybersecurity, emphasising emerging technologies such as AI that are shaping Africa's digital security future. Themed "CyberFuture", the conference addressed a wide range of topics, from quantum-resilient algorithms to the ethical dimensions of AI in cybersecurity and unique challenges faced by developing nations.

The conference was attended by top cyber security and AI experts from across the country and abroad.

Key takeaways from the conference:

1. Security is not just about cyber – it's about human behaviour and managing how we interact with technology.
2. AI will not only find its way into our job markets but will play a crucial role in keeping us secure. At the same time, it presents a potential threat, as hackers seek to use AI to their advantage.
3. Quantum computing is coming – and it will be a threat to some of the encryption and certificates that we currently use. There are solutions, but they will also take time to roll out and include in our business processes, so the time to begin is now.
4. Africa has tremendous potential for building AI solutions that suit our own needs and drive not only upliftment but also entrepreneurship.
5. Developing countries often lack resources to combat cyber threats, making them vulnerable targets. Building cybersecurity resilience in these countries is a strategic necessity for global cybersecurity.
6. International collaboration is of paramount importance in successfully combating cyberthreats. A cybersecurity vulnerability in one nation poses a threat to others. We must foster international collaboration, share resources, and provide technical support to build robust global defences.
7. Cybersecurity is not just a technical challenge but a societal one. It is about protecting our way of life in an increasingly interconnected world.

Digital paradox

The opening address by Deputy Minister Philly Mapulane of the Department of Communications and Digital Technologies underscored the South African government's commitment to advancing cybersecurity. The Deputy Minister noted the rapid evolution of our world and the integral role of the digital landscape in our lives, and how this integration offers opportunities but also poses significant challenges in cybersecurity and digital governance, especially for developing countries.

Mapulane emphasised the dual role of technical advances as enablers for development and as sources of new threats in information societies. Acknowledging this "digital paradox", he pointed out that while governments and organisations can provide services more efficiently, cybercrime poses a significant limitation, particularly for South Africans, with the highest screen time globally.

He highlighted the heightened priority of cybersecurity for African governments, citing comprehensive cybersecurity laws and policies in Nigeria, Kenya and South Africa, and stressed the growing complexity of cybersecurity threats, emphasising the need for cyber resilience and protective measures against financial losses and reputational damage.

Mapulane further noted that recent malware attacks in the region have put organisations on high alert, leading to significant growth in the network security market 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."

Addressing AI, the Deputy Minister acknowledged its potential to enhance cybersecurity defences but cautioned against risks, including the development of sophisticated malware and automated cyber-attacks. He emphasised the importance of ethical AI use, addressing biases, and ensuring transparency and accountability.

Building global inclusivity and resilience

The THREAT2023 Conference illustrated the importance of international collaboration and global inclusivity in cybersecurity. As noted by the Deputy Minister, developing nations frequently face resource constraints in tackling cyber threats, rendering them vulnerable targets. It becomes imperative to strategically enhance cybersecurity resilience in these countries for the sake of global cybersecurity. The solution lies in promoting international collaboration, resource-sharing, and offering technical support to fortify global defences.

"Cybersecurity is not just a technical challenge but a societal one. It is about protecting our way of life in an increasingly interconnected world," Mapulane said.

This sentiment was echoed by Jennifer Bachus, Principal Deputy Assistant Secretary at the US State Department's Bureau of Cyberspace and Digital Policy, who highlighted the interconnected nature of cybersecurity vulnerabilities. Bachus underscored the collaborative goal to address these vulnerabilities and create deterrents against exploitation, citing the UN's framework for responsible state behaviour in cyberspace as a significant initiative outlining acceptable and unacceptable actions in peacetime.

Bridging the digital divide through international collaboration

With the ever-increasing cybersecurity threats, there is a growing demand for experienced and knowledgeable cybersecurity professionals in government and industry alike. With the widening digital divide and within the shared notion of the need for an open cyberspace, it is imperative that we also collaborate on building such a high-level cybersecurity workforce in Southern Africa.

Initiatives such as the 3-day cybersecurity summer school held in conjunction with the THREAT2023 conference, as well as international collaboration initiatives such as the South Africa–Netherlands Cyber Security School (SANCS), as

announced at the THREAT2023 conference, aim to address this divide.

SANCS will bring together experts, institutions and the private sector from both the Netherlands and South Africa to deliver South Africa's first international online Cyber Security School starting in March 2024. This free online course is aimed at honour's students and early- to mid-career professionals in Southern Africa and the Netherlands with an interest in cyber security.

Through SANCS, students from various disciplines will be encouraged to use their respective competencies while working together as a team to address challenges, as they would in the workplace. The central goal of this school is to give students the opportunity to grow professionally and academically in the sphere of cybersecurity. Course work includes challenges set by government agencies and companies to engage students in real-life problem solving.

Offering a qualification in cybersecurity studies, the school promises to be a game changer for South African cyber skills development.

Within Africa's challenges lie immense opportunities

During THREAT2023, Abdul-Hakeem Ajijola, Chair of the African Union Cyber Security Expert Group, highlighted that amid the distinctive cybersecurity challenges in Africa – such as technological gaps, skills and awareness deficiencies, economic constraints, governance issues, social engineering risks and geopolitical complexities – significant opportunities also emerge. Projections indicate that the African cybersecurity market is set to reach 15 to 30 billion US dollars in the next decade.

"We must transform cybersecurity from an organisational cost centre to a societal profit centre, creating jobs, generating wealth, and enhancing tax revenue," Ajijola said.

Although another major cybersecurity conference in Germany recently signalled an awareness of a kind of "digital colonialism", where it is assumed that the Global South is not contributing valuable R&D in AI, Africa has tremendous potential for building AI solutions that suit our own needs and drive not only upliftment but also entrepreneurship.

According to Prof Bruce Watson, founder of the Computational Thinking for AI research group, AI offers many innovative solutions to address challenges that are unique to the African context, not only in the field of cybersecurity, but ranging from applications in wine science and fish farming, to genome comparison and techniques for comparing the variants of tuberculosis, which remains a serious problem in Africa. Various such research projects have resulted in real-life impactful applications.

A bright future

While major AI solutions are often crafted by tech giants such as Google and Microsoft, there is enormous potential to harness these technologies for the creation of indigenous AI solutions within Africa. These locally developed solutions can be tailor-made to address challenges unique to the African context.

In fact, the very challenges that exist in Africa at the same time shape the opportunities for emerging technologies. A key factor in this is a rising (youth) population. By 2030, African youth will constitute 42% of the world's youth population, and by 2050, under 35s will constitute 60% of Africa's 2.5 billion people.

Typically, young people in Africa are enthusiastic and early adopters of new technology and tend to be very entrepreneurial by necessity, despite the slow rate of economic and educational transformation. Over and above that, Africa can leap-frog technologies and has demonstrated this on various occasions in the past, such as with respect to mobile phone technology and online banking.

An example of such homegrown AI innovation is Nubi. Nubi, an innovative platform named after the combination of the Swahili and Amharic words for "light", leverages Large Language Models (LLMs) to unlock Africa's human potential. It addresses challenges in setting up businesses by providing a mobile-first platform for learning, earning and conducting business in multiple African languages. Founder Mike Mpanya envisions Nubi as a daily go-to platform for young Africans with a mobile phone and internet access. Nubi transforms static information into interactive learning tools, supports various languages, and streamlines funding processes for businesses. It coaches on effective presentations for investment readiness and offers on-demand mentorship dialogues from global leaders.

Additionally, Nubi plans to introduce a payment platform, incorporating LLM-powered tracking for seamless payments, revenue, taxes and invoices. This automation will empower small businesses, spaza shops and services, allowing them to professionalise operations at minimal cost, democratising essential business elements for over 300 million Africans with smartphones and internet access.

Should solutions such as Nubi meet their anticipated outcomes, the future of AI in Africa appears exceptionally bright indeed.

Article written by Nanette Watson-Saes, an independent international communications professional specialised in the application of ICT to support communication, and decision making. Nanette's research interest is in the application of emerging technologies such as AI, and how these can be applied to improve the efficacy and efficiency of communication and language solutions even further as well as make them more secure. She is a Research Fellow at Stellenbosch University, where she also guest-lectures.