



08 April 2022

Quantum computing risk is an opportunity for South African defence innovation

TABLE OF CONTENTS

Introduction	2
Turn risk into opportunity	2
Collaboration, not competition	3
Less imitation, more innovation	3
About Snode Technologies	4
Author	4

Introduction

Quantum processors are poised to revolutionise computing as the world currently knows it. It offers the capability of current high-end devices in a fraction of the time it takes us today to perform highly complex mathematical computations and other common tasks, including big data searches. This is achieved by using quantum bits (known as 'qubits'). It differs from the usual binary system of 1 or 0, in that it can exist in multiple states. For instance, it can be both 1 and 0 simultaneously - which means they have the potential to process exponentially more data compared to classic computers. Qubits are the undefined properties of an object before they've yet been detected, such as the spin of an electron.

However, what is currently hindering the development of quantum computing is an unacceptably high error rate. This means the first company or nation to build a high-fidelity processor will ultimately lead the international race for quantum supremacy.

That this will be achieved at some point is undoubted given the scale of research underway - but it remains impossible to predict when. Every major quantum protagonist is playing a key role in various disputes such as the Russia-Ukraine war and China-Taiwan dispute. Given the nationalistic character of these conflicts, the race for quantum supremacy now has the flavour of a race for sovereign security and military dominance, much like the race to be first to land on the moon once had. Such conflicts will ultimately catalyse quantum research and expedite processor development. This is because any unforeseen rapid breakthrough in quantum processor research will be perceived as negatively impacting the sovereign security of other countries and their national cyber defence. South Africa needs to prepare itself for any such significant technological advancement or find itself exposed and vulnerable to more advanced nation states.

Turn risk into opportunity

Even before quantum computing becomes ubiquitous, the threat to sovereignty and military security will at least equal the impact of the Enigma decoding (first used in World War II to encrypt radio messages, the decoding of which helped turn the tide of the war). This is because many of the encryption algorithms in use today are vulnerable to attack by any country having access to the exponentially-increased speed of quantum computing. The design and development of local quantum resistant encryption technology will not only mitigate this risk but provide an opportunity to propel South African defence solutions into the growing global cyber defence market.

Collaboration, not competition

South Africa boasts a wealth of thought leadership and intellectual capital within its cybersecurity community. Our export capability should be a lot greater than is currently the case. Recently we at Snode spent some time in other flourishing global cybersecurity markets, primarily in Southeast Asia. We were interested to observe there that vendors, professional services, and consulting firms collaborated a lot more than we do locally. This changed our view: although we find competition stimulating and healthy, we recognise the urgency for a similar collaborative culture in South Africa. As a country, we need to share intelligence, create centres of excellence, focus on deep skills development and establish creative monopolies. I call on our community to partner in order to grow our new innovations into underserved global markets. Such a dynamic approach will produce higher customer value and ultimately realize greater returns for local cybersecurity players.

Less imitation, more innovation

Snode is following in the wake of excellent South African cybersecurity brands like Sensepost, Thinkst, Telspace and Paterva. Our model is to build locally and serve globally, thereby underscoring the hypothesis that homegrown cyber talent could dominate in the global arena. Emerging trends in the global technology landscape, like quantum, 6G and homomorphic encryption provide the perfect opportunity to achieve these goals. However, for this to be achieved at scale, we first need to stimulate, support and promote South African cyber defence engineering.

About Snode Technologies

Snode Technologies is a cyber defense company, operating out of Centurion, South Africa. Snode's defense model consists of people, processes, and expert technologies to provide superior real-time threat detection.

Snode's Guardian platform offers cyber threat intelligence empowering informed, data-driven, risk-based decision-making. It encompasses:

- Breach intelligence - insight into what attackers do once inside, how customer security controls fail
- Machine intelligence - with 80 global points of presence, thousands of malicious events per hour are collated
- Operational intelligence - experts validate alerts, and the continuous monitoring provides a unique perspective on identifying emerging global threats within specific industry verticals
- Adversary intelligence - intelligence analysts are entrenched within the mindset of an attacker and offer clients visibility into motives and trends

Our technology is next generation breach detection, offering real-time, contextual behavioural analytics to monitor and identify suspicious behaviour.

Author



Nithen Naidoo

CEO and Founder of Snode Technologies

Nithen Naidoo is the CEO and founder of Snode Technologies. As a cyber security evangelist, with over 20 years of experience, Nithen provides cyber defence solutions globally, and most recently was recognised by the prestigious AfricArena tech accelerator as an Emerg-ing Entrepreneur of 2021. Nithen is also a sought-after public speaker.



www.snode.com

info@snode.com

+27 12 880 0989