



**REMARKS
BY
HON. TJEKERO TWEYA**

MINISTER OF INFORMATION AND COMMUNICATION TECHNOLOGY

AT THE CYBER SECURITY WORKSHOP

HILTON HOTEL

28 SEPTEMBER 2017

- Director of Ceremonies
- Permanent Secretaries Present
- Generals of Industries
- Distinguished Invited guest
- Members of the Media

All protocol observed

Good Morning , I am humbled for the honour bestowed upon me to be in your midst this morning as we bring heads together to address issues related to cyber security.

The global threat posed by cybercrime every second is upon us at an alarming rate, therefore we cannot stand idle, and we need to be proactive .This very important event organized by New Point Electronic Solutions, a leading local IT software development company could not have come at a better time.

Since the turn of the century we have witnessed an extraordinary growth in internet and communication technology. It has transformed the way we communicate and ultimately the fundamental way we live. We might think Namibia is separate- a paradise amidst all the war, chaos and atrocities of this world- but the global threat of cybercrime is here. We have our very own examples of cybercrime, from the modest ego-centric and relatively harmless hacking of several Namibian websites to our localized version of FNB Ewallet message scam with real life financial consequences.

As we inevitably move towards a digital economy, we will be faced with increasing risks of exposure. As a government we are hard at work to put legal frame work in place through the development of the Cyber Security Bill which recently concluded its consultative phase .

Cyber security is an important and complex subject, therefore we need to apply a motto of constant vigilance to ensure our data sovereignty. Digital developments are rapid and far-reaching. Our lives increasingly rely on mobile devices, big data and the Internet of Things. And the internet itself is driving social and economic innovation in ever changing ways.

These developments give rise to players who challenge the status quo. Uber and Airbnb, for example, are stirring up the taxi and rental market. We want to leverage those innovations. We want to foster and replicate an era of unparalleled customer service tied with strong operational efficiencies. A key component of ensuring such investment is to carefully plan and deliver a strong, dependable cybercrime safe zone.

This is very visible in our country. Namibia has been a frontrunner in the adoption of mobile technology and the internet. Every young Namibian today knows how to operate aweh aweh. They will give me a run for my money.

In this age of hyper-connectivity, our digital infrastructure is both an opportunity and a risk. Banks are experiencing DDos (denial of service) attacks that undermine the underlying financial infrastructure. And the software that runs the devices that we rely on, is vulnerable. If aweh aweh were hacked today, it would be catastrophic for the country. We need to have the proper infrastructure, laws and institutions working in both a preventive and a punitive manner to prevent the occurrence of serious incidents.

The security and resilience of our infrastructure should grow at the same rate as our digital dependency. This is especially the case for critical infrastructure in telecommunication, energy and finance. We need to have a secure environment hence the concept of cyber security.

One of the key issues any government faces is the gap between awareness and action. Our aim is help businesses to grow the economy and encourage them to understand their cyber risks and manage them appropriately. To this end, we will create the Namibia National Cyber Security Centre, which will aim to propel Namibia into the safest place to live and do business whether online or offline. Yesterday I launched a NAMIGF, becoming the 6th country to have such a forum under SADC support.

As well as protecting Namibia at a national level, we need to support the socio-economic foundation - that is, the parts of industry and society the security services have not traditionally engaged with - including small and medium-sized businesses, charities and educational institutions.

Analysis shows that the vast majority of cyber-attacks exploit basic, known vulnerabilities, like passwords and admin access policies. Cyber Essentials is aimed to engage the most vulnerable parts of our economy to help them address some of the issues that they might or will be facing. It's simple, low cost and specifically designed for SMEs and individuals.

The next step is to require all government suppliers which handle sensitive data to hold a Cyber Essentials certificate. This is about taking an organizational approach to cyber security and managing cyber risk as you would any other business risk. This is a board level issue, not one to delegate to the IT department. We want directors and board members to engage and frontline this issue. We also want to develop our national capability to deal with the cyber threat.

This final piece in the jigsaw is a crucial one for tackling the skills shortage. We need to put measures, interventions to improve cyber security skills at every level of education.

A Cyber Schools Programme to identify talented and motivated 14-18 year olds and help them become future cyber security professionals;

Cyber Security Apprenticeships, to establish apprenticeships as a viable route into the cyber security profession

And, a Cyber Retraining Programme to address the skills gap more immediately. This will help those already in the labour market change careers and become cyber security professionals in a short timeframe.

The next challenge for the ministry is to come out with a coherent National cyber security strategy for Namibia. But ultimately this is something which can only be done through partnership between business and Government and capitalizing on the dynamism shown by Namibian companies as we have seen today. So I look forward to continued efforts between the private sector and the Government, to help deliver our shared mission of making Namibia one of the safest places to do business online in Africa and globally.

Director of Ceremonies

I have outlined my plan for Namibia. I say my plan but in the spirit of our Namibian House, in the spirit of this country, it is our plan, one we are all torchbearers to.

There is growing awareness that Government coordinated efforts – regulation as much as cooperation – can make a real difference to the resilience of Namibia's network and information systems.

I believe you will find this workshop a valuable and helpful exercise in educating and creating awareness on the threats of cyber security. I also encourage all of you to take this opportunity to network with your fellow workshop participants in order to deepen your understanding of the critical role you play in safeguarding your cyber space. I will rely on your unwavering support for the cybercrime Bill I will table soon in parliament for debate and eventual passing into law.

I now declare this Cyber Security workshop officially open.

I thank you