REPUBLIC OF NAMIBIA

MINISTERIAL STATEMENT ON SCAMS AND CYBER ATTACKS ON CITIZENS AND THE MEASURES BEING UNDERTAKEN TO MITIGATE THE EFFECTS

BY HON. EMMA THEOFELUS

MINISTER OF INFORMATION AND COMMUNICATION TECHNOLOGY

NATIONAL ASSEMBLY, PARLIAMENT

9 APRIL 2025

WINDHOEK, NAMIBIA

Honourable Speaker,
Honourable Members,

I rise to address this august House on a matter of growing concern to our nation around the escalating incidents of scams and cyberattacks on our citizens, many of which are being conducted through telecommunication and digital platforms.

With the increasing integration of Artificial Intelligence (AI) technologies into everyday communication systems, we have witnessed a sharp uptick in scams, synthetic media, deepfakes, and other forms of digital deception targeting unsuspecting Namibians. These cyber incidents pose a serious threat not only to individuals' privacy and financial security, but also to our national trust and social cohesion.

Namibia, like many nations across the world, is yet to establish specific legislation governing the use and regulation of AI technologies. As a result, we currently rely on existing legal instruments, including the Electronic Transactions Act, the Communications Act, and provisions under our penal code to investigate and prosecute AI-related crimes. However, the dynamic nature of emerging technologies necessitates a more tailored and forward-looking regulatory approach.

It is this reason that for the last six months, the Ministers of ICT on the African continent have been meeting regularly, both physically and virtually to take bold decisions on this phenomenon. Our position is clear, AI should be for Public Good. This is why we have resolved to create an AI Council that will foster a regional position and enact a regional legal instrument that will cascade down to every member state in the African Union, Namibia included.

Honourable Members,

In the meantime, The Ministry of Information and Communication Technology, in collaboration with law enforcement agencies, is actively investigating recent incidents of scams perpetrated through telecommunications. We are working closely with service providers in telecommunications and the banking sectors to trace malicious actors and to strengthen cybersecurity protocols across our digital infrastructure.

Notably, the widespread usage of social media in Namibia has further amplified the reach and impact of such scams. According to recent statistics as of 2024, over **703,900 Namibians** are active users on platforms such as Facebook, Twitter (now X), WhatsApp, Instagram, and TikTok. While these platforms have revolutionized how we communicate, share information, and participate in democratic processes, they have also unfortunately become tools for malicious actors, including those leveraging generative AI to create and spread disinformation and fake news.

Content generated or manipulated using AI which is known as Synthetic Media has made it easier, faster, and more cost-effective for scammers to produce highly convincing fake videos, images, and messages. This presents a significant risk to public trust, especially when fake news is circulated under the guise of legitimate institutions or public figures.

[Deepfake video of the President, Deepfake video of the Governor of the Bank of Namibia]

In response to this, the Ministry is:

1. Considering the introduction of a national system for authentication of information sources. This will enable citizens to validate the credibility of any information they receive by cross-checking it against a database of verified institutional accounts and communication channels. These lessons were learned during election periods that there is a need for citizens to actively fact check information and data given to them by media houses, public figures or any other political actors.
2. Developing a comprehensive public campaign to sensitize citizens on the dangers of misinformation, disinformation, and misinformation. This campaign will include:
    - Multimedia content in indigenous languages,
    - Community workshops,
    - Social media engagement using trusted influencers and public figures. I therefore ask of the MPs of this August House to pass vote 29 with no reservation when the time comes. I am lobbying on the floor Hon Speaker.
3. MICT has rolled out a digital literacy program throughout the country, which will now also educate participants on the responsible use of AI and empower them with skills to reduce the negative impact of AI as part of the course material.
4. Through our 2-year digital literacy-training programme, we have now started piecing together a National Digital Literacy Framework that will guide the delivery of various digital literacy initiatives to ensure that citizens are empowered to navigate the digital space and fight against misinformation and disinformation**.**
5. Launching the Namibia Cyber Incidence Response Team and its Website on 14 April 2025 which will create an avenue to fight cybercrimes.
6. Continuing to implement the National Cybersecurity awareness creation plan, which aims to empower citizens with information to ensure their safety online. Every Friday, MICT and Salt Essential IT have a one-hour online cybersecurity training (10am – 11am) for anyone and everyone who has access to the internet to learn how to be safe online. This is one avenue. Those who do not have this access are being catered in the avenues I have outlined before.
7. The Ministry regularly encourages members of the public to engage the Ministry for tailor-made awareness raising sessions to understand the danger of cybercrimes and the importance of cybersecurity. The Ministry encourages the public to be vigilant when online, avoid clicking on unauthorised links, and not entertain those tricking them into providing their information, especially their banking details.
8. Finally, MICT Launched the National Reporting Portal for Child Sexual Abuse Material. The portal allows anyone to anonymously report digitally abusive materials affecting children with the view of combating cybercrimes towards them. This is implemented in partnership with the Internet Watch Foundation, UNICEF and Lifeline/ChildLine Namibia. As a Ministry, along with our partners, we are monitoring the age at which children are increasingly going online. And although social media platforms have an age restriction, many children are still going online and violating those various age restrictions, some U/13 and others u/16. We therefore call on parents, who at many times are the ones who own these gadgets that enable children to go online or who buy these gadgets for their children to actively monitor their use. How many stories have we heard of children buying stuff online without consent through their parents' gadgets and using their parents' financial details to do so. Both parents and children become at risk for scams and sexual exploitation online. Parents we call on you to step up your supervisory role.

From a regulatory standpoint, in collaboration with other Ministries, we are in the process of developing the following laws; some are at advanced stages while others are still at initiation:

- Cybercrime Bill
- Data Protection Bill
- Artificial Intelligence Bill and Process Guiding Principles in line with the UNESCO Recommendation on the Ethics of Artificial Intelligence and Continental Artificial Intelligence Strategy
- Content Credentials Legislations

This is a fast-evolving industry, and just when you think you have caught up with today's innovation, an emerging technology springs up. I therefore also implore my fellow MPs that once these legislations come to Parliament, let us attempt to pass them in good time. We know the law-making process can be cumbersome, for good measure, but technology waits for nobody, not even elected Honourable members of the National Assembly. We do not want to be left behind as a country because the impact will be immeasurable.

Furthermore, we emphasize that citizens should verify any public announcements, news, or social media posts from the government through the official communication channels of the government spokesperson, who is the Minister of ICT, before acting upon them.

Honourable Speaker,

We are in the midst of an exciting digital revolution. While the opportunities are vast, so too are the risks. As a Government, we have the responsibility to protect our people from the evolving threats of the digital age. This includes ensuring that our citizens are informed, our policies are robust, and our regulatory frameworks are future-proof.

I, therefore, call on all Namibians to remain vigilant, verify information before sharing it, and report any suspicious digital activity to the relevant authorities. The fight against scams and cyberattacks is not just a government responsibility. I would not be telling the truth if I were to claim that the government can overcome this alone because we cannot. It is a national imperative that requires all our collective action.

Thank you.