Address by the Deputy Minister of Justice and Constitutional Development, the Hon JH Jeffery, MP,
in a Subject for Discussion on *Cyber Security: Creating a safe and secure cyber environment that protects the Nation and the Economy backed by appropriate science & innovation strategies,*
National Assembly,
11 March 2020

Deputy Speaker/Chairperson
Honourable Members

Cybercrime is a reality of the world we live in.

More and more criminals are exploiting the internet and online means to commit a diverse range of crimes. We know that highly complex cybercriminal networks bring together individuals from across the world to commit these crimes.

New trends in cybercrime are emerging all the time, with estimated costs to the global economy ever increasing.

In 2018, when I addressed this House on the Cybercrimes Bill, I said that –

> "*most, if not all of us, have some form of an online presence – we email, we WhatsApp, we shop online, we're on Facebook and Twitter and Instagram, we buy our electricity online and we do our banking via cellphone, online or an app.*
>
> *It would be naïve to think that criminals would not seize the opportunity to operate in the sphere. It would be equally naïve to think that cybercrime is something that could never happen to us.*"

Covid-19 has forced us to live our lives even more online than before – so the risk is an ever increasing one.

We therefore need to make cyber space safer and more secure.

Parliament recently passed the Cybercrimes Bill in order to improve and rationalise our laws which deal with cybercrime into a single law.

Cybercrimes differ from many other crimes in fundamental ways - for example, in most instances they have a transnational dimension, meaning that they span the borders of many countries. Due to their transnational nature, international co-operation in law enforcement is essential and also urgent due to the transient nature of evidence.

From a law enforcement point of view, it requires the laws of evidence to provide for the admissibility of electronic evidence and the circumstances under which it may be admitted and it needs co-operation with service providers as they often have essential information at their disposal to assist with the investigation of cybercrimes.

It was necessary to align our law with international trends and best practices, as dual criminality and adherence to general accepted standards and practices to investigate cybercrimes are essential for international co-operation.

Another factor is the evolving nature of cybercrime. The methods of committing cybercrimes change rapidly and our laws need to keep pace with the more intrusive and complex investigative measures which are needed to investigate cybercrime.

Various countries, including other countries on our continent have enacted cyber-specific laws to deal with cybercrimes and various other countries are in the process of enacting specific laws to come to terms with the escalation of cybercrimes.

The new Cybercrimes Act, once assented to, will rationalize the laws of South Africa which deal with cybercrime into a single law which criminalizes conduct considered to be cybercrime and criminalizes the distribution of data messages which are harmful. It also provides for protection orders to protect victims against harm.

The Act will impose obligations on electronic communications service providers and financial institutions to report cybercrimes to the SAPS and provides for capacity building by the SAPS to detect, prevent and investigate cybercrimes.

Various acts can take place in cyberspace or the virtual world which enhance the ability of any person, entity or organisation to engage in computer terrorist activities.

With regards to information, sensitive or confidential information that is not adequately protected from search-robots or hacking attempts can be easily accessed. Considerable information can be obtained about possible targets through legal as well as illegal access.

Criminal and terrorist activities can be planned and preparations of how to carry out an attack can take place over the Internet. By using encryption technology and anonymous communication technologies, unwanted access to such communications may be limited.

The internet can also be used to receive funds or move funds around with a degree of anonymity.

The new Act will provide for expanded jurisdiction in respect of these offences so as to cater for the transnational dimension of cybercrime. The procedures to investigate cybercrimes and the extensive mutual assistance mechanism in the legislation are also applicable to terrorism and terrorism-related investigations.

There are also other legislative considerations to strengthen our response to cybercrime. Amendments to the Protection of Constitutional Democracy against Terrorist and Related Activities Act have been proposed to deal with cyber terrorism.

The Regulation of Interception of Communications and Provision of Communication-related Information Act is essential for the investigation of cyber-related offences, while the Financial Intelligence Centre Act provides for control measures and reporting obligations in respect of money laundering and financing of terrorist and related activities.

The new Act will provide that the National Executive may enter into agreements with any foreign State regarding the provision of mutual assistance and cooperation relating to the investigation and prosecution of offences and the implementation of cybercrime response activities.

It allows for training, research, information and technology-sharing and the exchange of information on the detection, prevention, mitigation and investigation of cybercrime. It also allows for the implementation of emergency cross-border response mechanisms to mitigate the effect of cybercrimes.

This provision can be used to forge the necessary relations with other States to combat cybercrime.

We all need to be vigilant and protect ourselves within the cyber space and when we are transacting online. There are steps we can all take, for example, be careful of clicking on links and opening documents from sources that you do not recognize. Be aware of things like phishing. There is a saying that passwords, ideally, should be used in the same way as underwear – don't show it to anyone, and change it frequently.

The South African Banking Risk Information Centre (SABRIC) has said that one should never list one's main email address publicly anywhere. This includes online advertisements, blogs or any place where your information can be harvested by spammers. Use strong passwords for all accounts. Be wary of email attachments and free software from unknown sources.

Be mindful of how much personal information you share on social media. Always set the privacy settings on your social media profiles to the highest level possible.

If you use a public webmail service, ensure that you enable two factor authentication services. Don't ignore reports from friends about mysterious emails coming from your accounts.

Never log in to your online banking through a link in an email. Either type the address into your browser or use your bookmarks and register for SMS notifications so that you are notified of any transaction on your bank account.

Monitor your bank accounts to check that no irregular activity has taken place and don't respond to emails that claim to be from your bank or any other company requesting your account details.

Honourable Members,

The National Cybersecurity Policy Framework for South Africa promotes coordination and consultation between the JCPS cluster departments, the private sector and civil society regarding cybersecurity matters through the establishment of a Cybersecurity Hub within the Department of Communications and Digital Technologies.

The Hub has been established and is largely responsible for public education.

The Hub works closely with SABRIC and various electronic communications service providers on initiatives to make information regarding threats in cyberspace available to the public as well as to educate the public on measures that can be taken to protect themselves against such threats.

The new legislation, coupled with the work of the Hub, will ensure that we make cyber space a safer place for everyone.

I thank you.