**UNREVISED HANSARD**

**MINI PLENARY - NATIONAL ASSEMBLY (VIRTUAL)**

**THURSDAY, 11 MARCH 2021**

**PROCCEEDINGS OF MINI PLENARY SESSION – NATIONAL ASSEMBLY CHAMBER**

Members of mini-plenary session met in National Assembly at 16:00

The HOUSE CHAIRPERSON (Mr M L D Ntombela): Good afternoon hon members. I welcome all members who have logged in to the virtual mini plenary session. There will now be an opportunity for silent prayer or meditation. Thank you very much. Hon members, before we proceed I would like to remind you that the virtual mini plenary is deemed to be in the precinct of Parliament and constitutes a meeting of National Assembly for debating purposes only. In addition to the rules of the virtual sitting, the rules of the National Assembly, including the rules of debate apply. Members enjoy the same powers and privileges that apply in a sitting of the National Assembly.

Members should equally note that anything said in the virtual platform is deemed to have been said to House and maybe ruled upon. All members who have logged in, shall be considered to

be present and are requested to mute their microphones and only unmute when recognised to speak. This is because the mics are very sensitive and will pick up noise which might disturb the attention of other members.

When recognised to speak, please unmute your microphone and connect your video. Members may make use of the icons on the bar, at the bottom of theirs screens which has an option that allows a member to put up his or her hand to raise points of order. The secretariat will assist in alerting the Chairperson to members requesting to speak. When using the virtual system, members are edged to refrain or desist from unnecessary points of order or interjections.

We shall now proceed to the order of this mini plenary session, which is a subject for discussion in the name of the hon M Modise on: *creating a safe and secure cyber environment that protects the nation and the economy backed by appropriate science and innovation strategies*. I now recognise the hon M Modise to take the podium, hon Modise.

**CREATING A SAFE AND SECURE CYBER ENVIRONMENT THAT PROTECTS THE NATION AND THE ECONOMY BACKED BY APPROPRIATE SCIENCE AND INNOVATION STRATEGIES**

Mr K B PILLAY: House Chairperson, the hon Modise has a bereavement and hence I am going to be speaking on her behalf.

The HOUSE CHAIRPERSON (Mr M L D Ntombela): You are welcome, hon member. You can go ahead.

Mr K B PILLAY: House Chairperson, Members of the Executive, Members of the Assembly, fellow compatriots, ladies and gentlemen watching on various platforms. As we commemorate Human Rights Month, we remember the sacrifices that accompanied the struggle for the attainment of freedom and democracy in South Africa. This year, we commemorate Human Rights Month under the theme: *The year of unity, socio- economic renewal and nation-building*.

At the heart of the struggle for liberation was the attainment of human rights and the restoration of human dignity. The period of the 1960s to the 1980s was characterized by systematic defiance and protest against the apartheid regime in the country. On 21 March 1960, the community in Sharpeville, like their fellow compatriots across the country, embarked on a protest march against pass laws. On the 25th anniversary of the Sharpeville Massacre, tragedy struck again KwaLanga in the Eastern Cape which became known as the *Langa*

*Massacre*. These horrific incidents exposed the apartheid government’s deliberate violation of human rights to the world.

The democratic government declared 21, March Human Rights Day to commemorate and honour those who fought for our liberation and the rights we enjoy today.

Our Constitution is hailed across the world as being one of the most progressive in the world. Among others, it is founded on the following principles: Human dignity, the achievement of equality and the advancement of human rights and freedoms. The Constitution is the ultimate protector of our Human Rights.

Among the rights enshrined in our Constitution is the right to privacy. Privacy is a fundamental human right, enshrined in numerous international human rights instruments. It is central to the protection of human dignity and forms the basis of any democratic society. It supports and reinforces these other rights, such as freedom of expression, information and association.

Activities that restrict the right to privacy can only be justified when they are prescribed by law, necessary to

achieve a legitimate aim, and proportionate to the aim pursued.

In terms of Section 7(2) of the Constitution, the state is required to respect, protect, promote and fulfil the rights in the Bill of Rights. Section 14 of the Constitution provides that:

Everyone has the right to privacy, which includes the right not to have:

1. their person or home searched;
2. their property searched;
3. their possessions seized; and
4. the privacy of their communications infringed.

There are various pieces of legislation that relate to the right to privacy. Of particular importance is the Protection of Personal Information Act 4 of 2013, POPIA, which deals with data protection; the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, RICA, which deals with the interception of communications; and the Electronic Communications and Transactions Act 25 of 2002, ECTA, particularly in relation to encryption.

South Africa has ratified two international treaties relevant to the right to privacy: The African Charter on the Rights and Welfare of the Child, article 10 and the International Covenant on Civil and Political Rights, article 17.

Parliament passed the Protection of Personal Information Act, POPIA, to give expression to the right to informational privacy, also known as the right to the protection of personal data.

In order to implement these laws, and in line with

international practice, the Protection of Personal Information, POPI, Act creates the office of the Information Regulator which must ensure respect for and to promote, enforce and fulfil the rights protected by the Act. The Regulator is independent and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers without fear, favour or prejudice. It is accountable to the National Assembly.

The Information Regulator also has duties relating to the Promotion of Access to Information Act, 2000. The POPIA gives the Information Regulator the authority to investigate and fine public and private parties for the violation of the Act.

The operation of POPIA was put into operation incrementally with only some of the sections, including those relating to the establishment of the Regulator, implemented in 2014.

Sections 2 to 38; sections 55 to 109; section 111 and sections 114(a) (b) and (c) commenced on 1 July 2020 and sections 110 and section 114 (4) shall commence on 30 June 2021. Section

114 is of importance in that it states that all forms of processing of personal information, must within one year of the commencement of the section, be made to conform with the Act. The effect of this is that both private and public bodies will have to ensure compliance by 1 July 2021.

With the Fourth Industrial Revolution, 4IR, upon us and the growing use of technology, data is regarded as the most valuable commodity in the digital economy. According to the World Economic Forum, more than 50% of the world’s population is now online; roughly one million more people join the internet each day and two-thirds of humanity own a mobile device. 4IR technologies are already bringing tremendous economic and societal benefits to much of the global population.

With that said, many unintended consequences have also surfaced. Cyberattacks have become a common hazard for individuals and businesses. The safety of people’s data is therefore critical. The right to privacy needs to be respected, protected and promoted.

While South Africa has various laws, which are used to address cyber offences, they do not comprehensively and uniformly criminalise conduct that is regarded internationally as cybercrime. This has rendered us vulnerable to cybercrimes and cyberattacks. Such vulnerability presents serious financial risks and challenges to the economy.

Considering the security of the country, the ANC 54th National Conference resolved that:

There is a need to strengthen capability for cybersecurity to enhance protection of critical databases, systems and critical infrastructure resources, including protecting society against fake news, cybercrime, cyber-attacks and hacking.

South Africa should never have to meet the fate of internet and telecommunication shutdowns that were experienced by our

African brothers in 2020, including Burundi, Chad, Ethiopia, Guinea, Kenya, Mali, Sudan, Tanzania, Togo and Uganda.

In our constitutional democracy, the internet and all telecommunication services, especially those under the cyber environment, should be widespread and fairly accessible to all compatriots irrespective of the political climate of the country.

In 2015, the Department of Justice and Constitutional Development initiated the process to establish decisive policy in the form of the Cybercrimes and Cyber Security Bill, responding to the country’s lack of legislation in this area. The end product of the study culminated with a draft bill called the Cybercrimes and Cybersecurity Bill which would assist in addressing the problem of cybercrime. Subsequent to discussions, changes were made to the Bill, including the removal of some of the security obligations. The 'security' part of the originally named Cyber Crimes and Cyber Security Bill was removed.

The Cybercrimes Bill was passed by Parliament in December 2020 and was sent to the President for signature. Among others, the Bill provides for interim protection orders, further regulates

jurisdiction in respect of cybercrimes, further regulates the powers to investigate cybercrimes, and further regulates aspects relating to mutual assistance in respect of the investigation of cybercrime.

The protection of privacy rests firmly on the constitutional conception of being a human being and a necessary part of a democratic society as a restraint on the power of the state. It must be balanced against the right It must be balanced against the right of freedom of expression which enhances human dignity and autonomy and makes democracy possible. I thank you.

Ms C V KING: Hon House Chairperson, I first rise to say long live the spirit of Mthokozisi Ntumba, who needlessly died yesterday around Wits University. We live in an age in which access to highly sophisticated technologies and almost every social media, economic or military asset has become scrutinised or vulnerable to disruption. Whether temporary or more lasting from an outside attacker or even an inside source. In a globalised but also more confrontational and complex world, resilience will remain and ongoing concern, requiring constant adaptation as new vulnerabilities and threats emerge.

Conventional crimes normally leave a trail of evidence that can be tracked to solve the crime. However, crime that takes place in cyberspace are more complex to trace and therefore to solve.

South Africa like other countries is not immune to this phenomenon. Cyberinsecurity is often under estimated.

Government and individuals do not know the extent of damages that can be caused on the economy or on society by an insecure of cyberenvironment. An insecure cyberenvironment has a direct impact on critical infrastructure that is needed for the economy to run adequately.

In the past the South African government has already experienced direct attacks on infrastructure. In 2017, Telkom was a victim of global cyberattack. This resulted in Telkom experiencing service problems which prevented subscribers from buying data bundles. It took Telkom days to solve the problem which amounted to millions of profits lost during this time.

In 2019, there was an attack on the Johannesburg municipal electricity system which largely affected billing. All the attack on the country’s major critical information infrastructure through to major banks affected.

Early this year, Nedbank experienced a data breach of

1,2 million clients were affected. In August last year, South Africa’s major banking groups including Standard Bank, First National Bank, FNB, and ABSA had a breach of

24 million client’s data. Essentially 793 794 businesses had their details breached by a fraudster.

In the current context of the pandemic since there is a drastic shift towards the digitisation, a focus on cybersecurity should be the main issue on the agenda. As hospitals gear up the technology and the context of the roll out of the vaccine, there is a massive need to protect the systems health information. The entire supply chain of the vaccines, procurement, distribution and manufacturing is being done via cyberspace. This means cyberinsecurity is a major risk to the successful roll out of the vaccination plan.

Interpol Cybercrime Unit has issued a warning on cyber-risk associated with COVID-19 procurements. Interpol stated that over 3 000 websites associated with online pharmacists has been suspected of selling illicit medicine and medical devices. And around 1 700 cyberthreaths, especially fishing and ... [Inaudible.] ... experience.

Before considering science and innovation strategies, the question to be asked is: How capacitated are we to ensure a safe cyber secure environment?

Government responded in 2015 with the National Cybersecurity Policy Framework with implementation led by the Minister of State Security, the Protection of Personal Information Act of 2013 created the information regulator to ensure data privacy.

The Protection of Personal Information regime, POPI, regime is being implemented slowly and has overly widely exemptions for national security. The Information Regulator was not fully operational and the cyberwall strategy is yet to be finalised.

South Africa lacks behind economies in cybersecurity legislation, in government co-ordination and engagement in businesses and citizens and as a pie of skilled labour. Delays have meant it lacks the experience obtained in fast moving countries and the improvements they have made to their policy and especially implementation.

Parliament has neither pressed the government for faster action nor explores areas where powers might have been taken to infringe human rights. Even with the best cyberdefence

organisations remain susceptible to data breaches. If they do not have a strong human fire wall the demand for cybersecurity talent outpace supply.

South Africa high-end demand human capital development in the areas of information and communication technology, ICT, and cybersecurity developers is far outweighed by cadre deployment in South Africa and the emigration of specialised skills. It is impossible to implement Cybercrime and Cybersecurity Bill without a fully capable cyberforce. It is therefore imperative that investments into ICT skills from school level is needed to produce the talent for higher education sector to produce cybersecurity qualification for now and into the future.

Not only would we need investment in better cybersecurity technology, but there is a need for awareness campaigns to be launched in order to educate companies and individuals on how to use technologies safely and securely. We can make South Africa a hub of cyberTeller. We have the people; we just need to rewrite their futures. I thank you.

Ms P MADOKWE: Hon House Chairperson, as far back as 2018, it was reported that South Africans lose as much as R2,2 billion as a result of Internet fraud and fishing attacks.

Cyberthreats are a growing phenomenon. Threatening not only individual levities, but are also a major threat to the country. Cybercriminals have been able to evolve their techniques faster, posing major for cybersecurity measures.

These cyberthreats are only going to be intensify as South Africa and the world transition from office work to doing most of the work and most work and their transactions online as a result of the new reality introduced by COVID-19.

As things stand, South Africa is reported to have the third highest number of cyberattacks in the whole world. The continent as a whole is very vulnerable to cyberattacks.

However, in the entire continent, we only have about 10 000 certified cybersecurity technicians.

While cybercriminals are moving at a very fast pace, and evolving their methods we do not seem to be moving as fast to ensure that personal, state and corporate information is safe from the hands of rogue elements. The Cybersecurity and the Cybercrimes Bill that was passed by this House 2018 is not sufficient to deal with the challenges of cybercrimes faced by this country.

The three-year imprisonment term on people who commit cybercrimes, is not a sufficient enough detergent for offenders. More critically, the country does not have enough capacity to investigate this types of criminal activities. We need to expand our capacity for both cybercrime technicians who must help the state and the banks against these fishing attacks as well as improve the ability of our investigative and prosecutorial services to deal thoroughly with these crimes.

At the moment we are still directing students who may be interested in cybercrimes to doing general information technology, IT, qualifications. Only the cybersecurity institute and the Cape Peninsular University Technology offer courses in cybercrimes and these are very expensive.

The Department of Higher Education, Science, Technology and Innovation have spectacularly failed to appreciate the severity of the threats and have not done what they should have done and can still do to train as many people as possible in order to protect the country from cyberattacks. The department’s own policy framework titled the National Cyber Policy Framework enjoins the department to develop and facilitate cybersecurity research for the country.

In combatting cyberthreats this country must create flexible and dynamic cybersecurity strategies which are in line with high priority national objectives, so as to meet new global threats head on.

Government must also build internal capacity to develop and manufacture information and communication technology, ICT, hardware and software unique to South African and African needs.

Furthermore, the government must use science, technology and innovation to produce the knowledge, information, skills and talent needed to support, facilitate and fuel the development and growth of strategic sectors of the economy and society which are central to the overall independence and sovereignty of South African and African people.

Central to any moves towards development and economic growth Chairperson, is education, and maximise educational opportunities. In this regard as the EFF we reiterate our call for free decolonised education for all, from Grade 1 until one attains first undergraduate qualification.

We further pledge our solidarity with all the students across the country, as they contemplate ways to ensure the government delivers on its promise to free education. Not this arrogant ducking and diving we have been subjected to since the start of this year. Thank you very much, Chairperson.

The DEPUTY MINISTER OF POLICE: Chairperson, let me acknowledge the Minister and Members of Parliament present here, it’s a privilege and honour for me to be part of this debate this afternoon, in the context of the struggle that is currently unfolding in our country for free education by our young people. The 21st century has indeed ushered in unprecedented levels of Information and Communication Technology, ICT, advancement.

These leaps in technological advancement have inevitably brought about drastic changes in the way we live our lives, economically, socially and politically. The world today is more interconnected than ever before. Yet, with all its advantages increased connectivity brings increased risk of theft, fraud and abuse. Ladies and gentlemen, with these enormous technological advancements made in ICT, came an upsurge in technology-based crime and the technologically advanced high tech criminals, using computers and advance

technology to commit crime, protected by the anonymity that this technological advancement offers.

With all the convenience and the advantages of the increased usage and reliance on ICT, subsequent spikes and prevalence of cybercrimes are now demanding law enforcement agencies to refocus their crime combating strategies and interventions to include the policing of the cyber space. Chairperson and members, cybercrime has evolved into distinctive and sophisticated crime phenomenon which requires a highly skilled and specialised law enforcement response.

It calls for a multidisciplinary approach in which actionable intelligence plays a key role. To this effect, the SA Police Service, SAPS, established a Cybercrime Steering Committee in order to address the internal fragmented capacity that existed and also to co-ordinate the operationalisation and implementation of the Legislative Framework, the Interim Cybercrime Strategy Policy Framework and operational co- ordination in general.

One of the unique characteristics relating to cybercrime is that it often takes place across jurisdictional boundaries, with offenders steering cyber-attacks through various

jurisdictions, which can only be countered by cross border and international law enforcement responses. The need for reliable and efficient international co-operation in law enforcement matters has therefore never been more urgent than it is today. Law enforcement agencies and prosecutorial authorities across the globe, are continuously focusing upon developing investigating and forensic methodologies to address the scourge of cybercrime.

We as SAPS are also doing the same. We are also collaborating with the international community to leverage on a number of interventions they have undertaken to facilitate cross border co-operation in criminal matters, including the investigation and prosecution of cybercrime. One such collaboration is with

the International Criminal Police Organisation, Interpol. Not only with Interpol, but we are also interacting and collaborating with other law enforcement agencies across the globe, including the Federal Bureau of Investigation, FBI.

There are instances where they collaborated on a matter that had to do with the cybercrime committed in South Africa, but the proceeds of that criminal activity was a process in Japan. This just shows how these syndicates operates, and this has affected one of our best institutions, whose name I won’t

mention here because the matter is still under investigation. Internally, the SA Justice, Crime Prevention and Security cluster has developed, as part of its mandate and obligations, the National Cybersecurity Policy Framework, NCPF, that seeks measures to do the following:

Address national security threats in terms of cyberspace, promote the combating of cybercrime, build confidence and trust in the secure use of ICT and develop, review and update substantive and procedural laws to ensure alignment. According to the National Cybersecurity Policy Framework, the South African Police Service is accountable for the prevention, investigation, and combating of cybercrime, including: The development of cybercrime policies and strategies; collaboration with appropriate stakeholders; development and maintenance of enforcement capabilities; and improvement of a basic understanding of cybercrime within the South African Police Service.

It is therefore our responsibility as the South African Police Service to develop and implement a Cybercrime Strategy, associated policy or policies and to implement the framework. In this regard, the SAPS, in terms of the back to basic approach, prioritised cybercrime as a priority and part of the

department’s programme of action. Further, in line with the SA National Security Strategy, which was adopted by Cabinet in December 2013, we have been tasked with the development of innovative cybercrime legislation.

To this effect, the Bill has already been drafted and introduced in Parliament in February 2017, and was adopted by this honourable House in November 2018, and referred to the NCOP in 2020. The Cybercrimes Bill is expected to be promulgated into law in the near future. Chairperson, according to the proposed legislative framework the SAPS need to create a strategy, capability, and adequate capacity, including the creation of an institutional framework, to deal with the threats of cybercrime in an integrated and coordinated manner.

As is the case with all crime prevention and crime combating strategies, a co-ordinated approach with all stakeholders is necessary. Strategies and measures against cybercrime would have to follow a criminal justice rationale and should be linked to broader crime prevention and criminal justice policies, aimed at contributing to the rule of law and the promotion of human rights. Other government departments which do not necessarily fall within the Justice cluster have a

crucial role to play in this space, for example, the Department of Communications and Digital Technologies.

In 2018 the SAPS, through the South African and European Union dialogue facility, presented a project proposal for dialogue in order to establish strategic interventions in eradicating the identified cybercrime phenomena and its manifestation within the Southern African regional context. The proposal, recommended by the National Commissioner of the SA Police and approved by the EU included, amongst others, a study visit by

members of the SA Police Service to the European Police Office, EUROPOL, Cybercrime Centre.

The aim of the proposed visit was to identify law enforcement best practices to be included in the development of a unique SA Police Service Cybercrime Policing Framework. In line therewith, SAPS has developed the Cybercrime Strategy proposing a unique policing model on cybercrime, as well as the proposal of a Law Enforcement Operational Implementation Framework ... [Interjections.] [Time expired.]

Ms Z MAJOZI: Hon chairperson, the pandemic has been difficult to navigate in many ways, one of which is digitally. The migration from a physical to a functional digital, virtual

Parliament has not been without its challenges, least of which are the security challenges of engaging via technology. We have witnessed multiple instances of potential breaches while performing our duties. The issue of cyber security is not isolated to our Parliament, and is increasingly becoming an international concern for industries across the board.

It has been apparent for a long time that the state of our country’s cyber security falls short of international best practice. This leaves our people and their interests open to all forms of data breaches and ransomware. The pandemic has only served to exacerbate this problem. According to Mimecast Threat Intel, in the first 100 days of the pandemic, there was a 75% increase in impersonation fraud in the country.

In 2020 alone, South African organisations lost at least R40,2 million per breach on average to data breaches. Cyber criminals are using increasingly sophisticated tools to execute data breaches, and no one is spared, and it is no longer enough to merely require organisations and regulators to inform customers of breaches in terms of POPI.

We must begin to see a concerted effort to prevent such data breaches using up to date technologies and protocols that

reflect the information age in which we live. The institute for security studies has highlighted that as we move to a digital medical world, the cyber security is literally the difference between life and death for many. One place where work must be done to guarantee cyber-security is the Cybercrimes Bill, which has yet to be signed into law.

There remain concerns about over-reach on the government’s part and these objections must be taken seriously. We cannot have critical legislature stalled while the threat level is so high. Further, lending more support to the information regulator to allow the country to keep abreast with international best practice. This will allow the necessary security for economic growth and extend security to people as they navigate an increasingly digital world.

We must ensure that we protect, defend and uphold all the rights pertaining to personal privacy and security of our people. If government fails to do this, it is failing to deliver on its constitutional mandate. Thank you, Chair.

Dr W J BOSHOFF: Hon House Chair, the hon Modise and the ANC want us to discuss creating a safe and secured cyber environment that protects the nation and the economy by

appropriate science and innovation standards. This is a kind of fanciful utopian expression of a wish which covers everything which is proper and good versions to be expected from the ANC.

What appropriate science and innovation strategies would be, is determined by what one wants to protect in the nation and the economy. Does the nation equate the citizens with the government of South Africa? Certainly, many citizens especially corporate ones would regard effective protection against an all-powerful state as safe and secure.

Few models of security exist. Let us call it the western model which protects the people against the state and the Chinese model where laws protect the state against the people. The state would indeed be well-advised to give some sort of private encrypted currencies. This technology may enable citizens to [Inaudible.] income out of the Receiver of Revenue cycle that would convert tax from inescapable duty to a voluntary contribution.

Before citizens rejoice about such a safe and secure cyber environment, they must keep in mind that smugglers of drugs, weapons and humans like this most of all. Who do we, as a

nation, fear most? Other nations? Fellow but malicious citizens? Big business? The big state or some political figure taking control over all of us with our cellphones? In fact, none of these. It’s ridiculous! External security is provided by the country’s security forces and internal security by the police.

Likewise, in cyber terms, the state has to protect its own systems and South Africa’s infrastructure against possible threats. However, a cyberattack happens too fast to respond to. This means that emphasis needs to be placed on prevention and in the event of a successful attack, to know exactly what the perpetrators have done – what they have laid their hands on. Only when that is known, the consequences can be managed.

In [Inaudible.] like the citizens are protected against the abuses of the police, the law should protect the citizens’ cyber rights. It is with this mind that the UN formulated global data protection rights, GDPR. It provides citizens with the assurance that the state acts in the interest of the citizens and if it does not do, it can be challenged.

To make this discussion even more complex, we should remember that with the internet of things every globe, every geyser,

every fridge and coffee machine, every mower, every power saw and every lift join our computers, radios, cellphones and cars in the cyber environment. So, first of all, who do we distrust most? I believe for many in South Africa the answer is, the state. Not only does the state have a nasty reputation of meddling in private matters, but it is also increasingly incompetent. The reality is that whatever we discuss here in Parliament and whatever the government thinks, corporate and private citizenship should take the responsibility of cyber security upon themselves while hoping that government will look after its own affairs and leave law-abiding citizens alone. I thank you.

Mr W M THRING: Hon House Chair, it is the belief of the ACDP that the international scope of the internet, the fast technological advances and the increase in cyberattacks require the South African administrative and legislative system to both intersect largely with the application and implementation of international legislation, as well as to take timeous precautionary measures and stay updated on trends and developments.

The ACDP is of the view that one of the problems associated with technological revolution is that the cyberspace is full

of complex and dynamic technological innovations that are not well-suited to any lagging administrative and legal systems. Additionally, we realise that there is a lack of comprehensive and enforceable treaties facilitating international cooperation with regard to cyberdefence, resulting in many developing countries like South Africa in particular, not being properly aware, prepared, or adequately protected in the event of a cyberattack on a national level. Often, when these attacks are realised, the time to react is of such a long nature, due to consultation and legislative processes, that the legal systems provide little support to ensure timeous and necessary countermeasures.

On many levels, cyberwarfare brings the battle closer to home since more people can potentially be affected. In many cases the enemy is difficult to identify, since any piece of equipment that uses technology is a potential battlefield or medium that can be used by enemy forces. Cyberterrorists have the capability to shut down South Africa’s power, disrupt financial transactions and commit crimes to finance their physical operations. Organised crime is also increasingly making use of the internet as a means of communication and financial gain. Therefore, South Africa needs a national cyberdefence system to which everybody must comply.

Cybercrime has emerged as a significant contributor to economic crime losses in South Africa and is considered to be the fourth most common economic crime after the misappropriation of assets, bribery and corruption, and financial statement fraud.

The Systemics, Cybernetics and Informatics Journal states that, if South Africa is to create a safe and secure cyber environment, we must focus on: The public sector, where the security of all state departments and their systems and sensitive information must be protected; the private sector to curb economic losses; the military or national security sector to negate external cyberattacks on our country; and citizen education at schools, FET’s and universities to capacitate citizens in identifying and fighting cybercrime.

The ACDP supports these interventions. Thank you, hon House Chair.

Ms M C DIKGALE: Chairperson and hon members, the preamble of the Report of the Presidential Commission on the Fourth Industrial Revolution says that throughout human history, the search for human well-being has been an enduring and foundational concern. In response to this fundamental human

conundrum, in 2013 South Africans articulated a developmental Vision 2030 as encapsulated in the National Development Plan, NDP as the latest iteration in the continued course to ensure security and welfare for all, explicitly aimed at removing the triple scourge of poverty, inequality and unemployment by 2030. This Vision 2030 ...

The HOUSE CHAIRPERSON (Mr M L D Ntombela): Hon Dikgale ... Hon Dikgale, we have lost you.

Ms M C DIKGALE: ... the country’s socioeconomic transformation in which all South Africans can meaningfully and ... Hello!

The HOUSE CHAIRPERSON (Mr M L D Ntombela): Hello! Hon Dikgale, go ahead, please. You still have ... [Interjections.]

Ms M C DIKGALE: Thank you very much, Chairperson. The 2018 state of the nation address directed that the digital industrial revolution would respond to rapid technological advances and ensure the nation’s prosperity. The Presidential Commission on the Fourth Industrial Revolution included the private sector and civil society to ensure that the country is in a better position to seize opportunities and manage the

challenges of rapid advances in information and communications technology.

The [Inaudible.] solution on the Fourth Industrial Revolution made eight key recommendations that are considered game changers within the Fourth Industrial Revolution will have to implemented by the relevant stakeholders. The following constitute part of the recommendations: one, invest in human capacity related to the Fourth Industrial Revolution; two, build Fourth Industrial Revolution infrastructure; three, establish an artificial intelligence institute; four, establish a platform for advanced manufacturing and new materials; five, secure and avail data and enable innovation; six, incentivise future industries; seven, review and amend policy and legislation ...

The HOUSE CHAIRPERSON (Mr M L D Ntombela): Your line is terrible, hon member. Hon Dikgale, you are gone. Hon Dikgale

... Hon Dikgale. I think we shall have to move. Hon Dikgale is gone.

Ms M C DIKGALE: My apology, Chairperson. Can you hear me?

The HOUSE CHAIRPERSON (Mr M L D Ntombela): You are left with four minutes, hon member. Sorry, you line is very bad, hon member. Let’s call it a day. You are totally inaudible. Hon member, we shall have to move.

Ms M C DIKGALE: Hon House Chairperson, within the aforementioned technology in the cyberspace ...

*Sesotho:*

MODULASETULO WA NTLO (Mong M L D Ntombela): Nako ya hao e a lahleha, mme.

*English:*

Ms M C DIKGALE: Chairperson, can you hear me?

The HOUSE CHAIRPERSON (Mr M L D Ntombela): You were totally inaudible. I can hear you now. You are left with a few minutes. [Interjections.]

Mr W F FABER: Chairperson, point of order.

The HOUSE CHAIRPERSON (Mr M L D Ntombela): We cannot go on, sorry. I do not ... maybe we can somehow ... [Interjections.]

Ms M C DIKGALE: ... for economic and ...

The HOUSE CHAIRPERSON (Mr M L D Ntombela): What’s your point

of order, hon member?

Mr W F FABER: Hon Chair, I think there was a cyberattack. Maybe she must ...

The HOUSE CHAIRPERSON (Mr M L D Ntombela): Hon member, you are exacerbating the problem. [Interjections.]

Ms M C DIKGALE: ... of information and communication technology. Hello Chair, can I go on?

The HOUSE CHAIRPERSON (Mr M L D Ntombela): Go ahead, hon member. I think you left with two minutes. You better move away from where you are. Hon Dikgale ... Hon Dikgale.

Ms M C DIKGALE: The Fourth Industrial Revolution obliges this government to align ...

*Sesotho:*

MODULASETULO WA NTLO (Mong M L D Ntombela): Dithapo tsa hao di a hana, mme.

*English:*

Hon Dikgale, I think your time will be compensated somehow.

Ms M C DIKGALE: Chairperson ... Chair.

The HOUSE CHAIRPERSON (Mr M L D Ntombela): Hon member, you are left with one minute now.

Ms M C DIKGALE: Yoh, yoh, the ANC-led government continues to invest in human capital. South Africa’s greatest opportunity and greatest resources is her people. The Fourth Industrial Revolution gives us a relaying point of urgency and opportunity to redesign, streamline and align the education system through a coordinated, robust multi-stakeholder process. The purpose of version 2,0 of our skills ecosystem leapfrogs our youth into productive work and reskill current workers for job retention and ongoing productive work in the economy.

The ANC-led government continues to use amongst others, ICTs to play an enabling role in addressing the challenges related to inequalities in the standard of living, life expectancy, etc. ITC sector in South Africa is characterised by exponential growth of the whole sector. The ability of South

Africa to compete in the global economy is dependent to a large extent on its ITC sector and in particular, the country’s ability to facilitate and grow the sector to meet the citizens’ needs for affordable and accessible broadband.

The rapid deployment of fast and affordable broadband infrastructure remains a powerful lever to create an internationally-competitive knowledge economy, improve productivity and expand access to new markets.

House Chairperson, artificial intelligence involving the theory and development of computer system to perform tasks usually requiring human intelligence which is a bedrock technology of the Fourth Industrial Revolution underpins the growing connections in cyber, physical and biological system. To be successful in the context of the Fourth Industrial Revolution it is imperative that the manufacturing sector is supported by a state-led research initiative focused on advanced manufacturing of new materials.

The ANC-led government continues to ... [Time expired.] Thank you, Chairperson.

Mr M G E HENDRICKS: Hon House Chair, the amount of cyber- attacks and scams has increased in recent years. In creating a safe and secure cyber environment for the nation the user needs to be educated and the risks understood. But how can we overcome this?

There is a need for a basic level of understanding and education. Too many of our end users are falling prey and victims to attacks. I personally fell prey when my Parliament email was used to invite advocates and judges to a meeting to discuss a matter between the Speaker and the Public Protector which everyone knows is a hot potato.

We must not underestimate the hackers from other foreign countries. I don’t think our Parliament email department, for example, makes the cut to outsmart them. I know because I am a victim. So, Parliament email cyber security will tell you that according to their logs you have not been compromised or their systems have not been compromised but will blame it on the device but we all know for example that Apple products are the most secured devices in the world.

Parliament and the nation needs to be protected but just watching the logs is not enough. We will never be able to be

100% secure but all we can to is to lessen the risks. I think, hon Speaker, that is what you must tell the nation.

We do need South African youth to step up and become more innovative. The technological advances made in South Africa and around the world have been phenomenal but we can improve. As we know the advances so too is the threat of a breach in cyber security.

Large corporations should encourage white hat persons. That is the legal hacking of a company’s system. How can you prevent hacking if you don’t know how to hack yourself? Also, an emphasis should be made on the ability ... [Inaudible.] ... by hosting events which can focus at talent pool for those without the necessary qualifications will enable us to create a broader and wider talent pool which we can harness to become leaders in the world.

Studies in science, technology, engineering and mathematics education should be further encouraged to bring forth the future leaders and the roles they play.

In conclusion, for the safeguarding of our nation, we need to establish a platform whereby we can provide for the

advancement of our next cyber generation regardless of their background. Everyone in this field can put together to create and develop our technological advances as a whole. The following are just some of the ways to add in limiting the risk, Notifactor, authentication, audit security, penetration testing and scanning tools. [Time expired.] Thank you very much.

Dr A LOTRIET: Chairperson, the South African government cybersecurity efforts are like the government itself — stuck in the early 2000s with only few efforts being made here and there to address major issues. If one looks at the efforts made to date, one would not say that we are the third most targeted country in the world. Yet, because most people cannot see cybercrimes and most people cannot see the effect of proper cyber policy, it never seems to make it to the top of the ANC’s priority list. Yet, these crimes cost our economy billions every year. Small and medium-size businesses and municipalities being among the hardest hit of all. Personal information and finances being the biggest targets.

In order for us to get South Africa cybersecurity to keep up with ever evolving technology and innovation, and to safeguard our citizens against a useable but very real threat, we need

to focus on the three Cs: Capacity, co-operation and community.

Capacity focuses on ensuring that the right entities can deal with cyber threats effectively. Right now at station level, the South African Police Service, Saps, does not know how to deal with cybercrimes despite the new Cybercrimes Bill that will soon be promulgated. Once it eventually reaches the Hawks specialised unit you will find that this unit is staffed with a handful of very capable but overworked people who do their job to the best of their abilities but they don’t have enough people with specialised skills in cyber forensics to effectively and speedily deal with the workload. A module on cybercrime is not sufficient, Deputy Minister.

They also serve as a training sector but because of public sector cannot compete with the private sector, there is no way in which they can retain the skills they build. Apart from this they are kept busy investigating parody Twitter accounts that perked the ego of the Minister of Police rather than to focus on municipalities and small businesses who fall victim amounting to millions of rands a month, leading to job losses and less funds for proper service delivery.

We can also not leave the country’s cybersecurity policy in the hands of the State Security Agency, SSA. There is a very good reason there is distrust for the SSA. It is time for us to establish a specialised unit or entity to safeguard our cyber rights and to ensure effective policy informed by specialists in the field.

The second factor is co-operation. We cannot do this alone; we need the private sector. There are currently but a handful of efforts between government, businesses and universities to address the shortcomings in our cyber industry. We applaud the effort that has been made but it is time for us to increase these efforts so that meaningful co-operation can take place.

For instance, universities can play a key role in planning the capacity that we need if the state is willing to nurture those graduates. In return, the government could help such academic institutions with a necessary funding to ensure that we develop world class cyber technology that will not only generate revenue but give the ability to deal with such threats.

Finally, we need to focus on the community. We need a nationwide cybersecurity campaign that will be understood, not

by cyber experts, by every person who owns the most basic cellular device. A number of 22 million people now in this country own a cell phone. We need to inform the public how to live about responsibly with it. It is so basic an idea, yet it is the only thing that probably displace the most effectively the ANC’s lack of meaningful efforts to address the threats.

We need to form meaningful partnerships internationally. We still await a better excuse from the government as to why the Budapest Convention was never ratified whilst it has become a convention ratified not only by the European Union but by 64 countries worldwide. Or rather, just be honest, our partners in BRICS, most notably Russia and China, are opposed to it.

Chair, this is our best bet at having meaningful co-operation in fighting cybercrimes. Indeed, we will need an international agreement to defect that will be more acceptable to a broader scope of the international community. But in the meantime, we cannot be stuck in the early 2000s whilst the world is advancing and co-operating at a much faster speed and technology that is advancing at a rate with which no one can keep up, and decreasing budgets for science and innovation is not helping.

Chair, it is one thing to talk about cybersecurity is a topic, it is another thing to do the right thing even when no one can see it. Thank you.

The DEPUTY MINISTER OF JUSTICE AND CORRECTIONAL SERVICES RESPONSIBLE FOR CONSTITUTIONAL DEVELOPMENT: Hon Chairperson

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 and I quote:

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. So hon Lotriet, we are not stuck in the early 2000s.

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 police and provides for capacity building by the police 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 is 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 Cybercrime Act will provide that the National Executive may enter into agreements with any foreign State regarding the provision of mutual assistance and co-operation 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 cyberspace 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. Be mindful of how much personal information you share on social media. Always set the privacy settings of your social media profiles to the highest level possible.

Never log in to your online banking through a link in an email. Monitor your bank accounts to ensure 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.

The National Cybersecurity Policy Framework for South Africa promotes coordination and consultation between the Justice Crimes Prevention Security, 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 – that is the banking body, 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 cyberspace a safer place for everyone.

In closing, just to respond to certain issues. Firstly, to welcome the fact that the protection of personal information remaining sections will come into effect at the end of June. Those will be the sections dealing with access to information which will now resort under the information regulator and the year’s grace period for compliance with the [Inaudible] will be up.

It’s been good that debaters largely had consensus on a number of issues, but I just want to focus on three hon members. Hon Lotriet from DA, it’s ironic that you speak about how important cybercrime, cybersecurity is but the DA tried to prevent the passing of the Cybercrimes Bill in the NA in the last Parliament by depriving the House of a quorum. You luckily did vote for the same Bill when it was returned by the NCOP, but that was not particularly helpful.

Hon Boshoef, I can find it particularly ironic that you can tell us about human rights given your party’s history and your own ancestry.

Lastly, to the hon Madokwe, the FF Plus opposed the Bill for both times in the House because it thought it was passing the Cybersecurity and Cybercrime Bill. It was all in the

Cybercrime Bill and it was passed; you however still refer to it being the Cybersecurity Bill.

You then complain that the sentences are too little and you spoke about three years. Hon member and other members from the EFF, please read the Bill. Please read clause 19, which is on sentences. The three years is only for the minor offences such as voucher message, inciting violence or threatening a person or disclosing intimate message. The other crimes are faced sentences of up to five, ten years and even fifteen years.

Chairperson, and hon members, I think it has been a good debate but I think it is something we need to work together on to ensure that the scourge attacks and cyber-attacks and cybercrime is dealt with. I thank you.

Mr K B PILLAY: Chairperson, firstly let me acknowledge all

the hon members and their input that there is indeed a need to strengthen the capacity to curb cybercrime. There is also indeed a very big need for public awareness of cybercrime.

It’s a devastating impact on people and businesses, unsuspecting individuals and most vulnerable. There is definitely a need for that.

With the losses running up to millions of rands annually due to cybercrime, we have established closer institutional relations with the South African Banking Risk Information Centre, SABRIC. SABRIC shares best practices and reports of intrusions among its members to mitigate the risk of data being stolen, access denied of processes being meddle with. I think it is important for me to highlight that. That we have started this relationship.

One of the members alluded that SA Police Service, SAPS, does not know how to deal with cybercrimes. Let me just give you something factually, hon Chairperson. In 2019-20 financial- years the National Prosecuting Authority, NPA, placed special focus on curbing the international phenomenon of cybercrime. Prosecutors maintained the high conviction rate by 320 convictions in 325 cases with their verdicts. Let me repeat that; 320 out of 325 cases with a verdict also – and you can just do this by Google.

South Africans can report cybercrimes anonymously by calling the Crime Stop call centre. Crime is a national contact centre that is staffed with the well-trained, investigative interviewers who all have at least basic detective training and they are able to advice accordingly.

Chairperson, I must emphasize the importance of supporting the work of the Information Regulator which is an independent institution subject to the constitution and law. The Presidential Commission on the Fourth Industrial Revolution, 4IR, which was set up, the commission which made recommendations on strategic areas such as the country’s investments, inhuman capital, artificial intelligence, advance manufacturing and new materials.

The provision of data to enable innovation, future industries and the 4IR infrastructure. It is evident that there is a need for more education and training and to strengthen the capabilities of South Africans.

Let me close by saying; let us not lose sight of our Constitution. The claim is that an applause for our constitution goes beyond our borders and esteemed Harvard Law School, Professor Cass Sunstein said that “Our constitution is the most admirable constitution in the history of the world.” While a US Supreme Court Justice showered praise on it as a great piece of work that embraces basic human rights. Thank you.

The Mini-Plenary adjourned at 17:16.