

**THE PRESIDENCY:**

**REPUBLIC OF SOUTH AFRICA**

Private Bag X1000, Pretoria, 0001, Tel: 012 300 5200 / Private Bag X 1000, Cape Town, 8000, Tel: 021 464 2100

**NATIONAL ASSEMBLY**

**QUESTION FOR WRITTEN REPLY**

**QUESTION NO.:** **3051**

**Mrs M R Mohlala (EFF) to ask the Minister in The Presidency:**

Whether he has been informed of the rising trend in cybercrime; if not, why not; if so, what steps have been taken to counter it? NW3691E

**REPLY:**

Cybercrime refers to illegal internet-enabled activities that are perpetuated using computers. This is a global problem that transcends national boundaries. The cost to the global economy is estimated at $7 trillion US dollars. South Africa, being a global citizen and with our developed infrastructure – be it in sectors such as financial, communication, transportation, government, health, education or energy – is an attractive target for cybercriminals who use the Internet for extortion, fraud, child sexual exploitation, human trafficking, identity theft, disruption of critical services, selling illicit goods, and so forth.

The Honourable Member will be aware that in 2020, this Parliament passed the Cybercrimes Act to delineate offences that constitute cybercrime. The Act places the South African Police Service at the driving seat to investigate, combat and prosecute cybercrime. The Act bestows specific powers and responsibilities upon the Cabinet member responsible for policing, such as issuing Standard Operating procedures to be observed by the South African Police Service or any Law Enforcement Agency authorised to investigate any offence in terms of the law.

More specific to your question Honourable Member, Chapter 8 of The Act on reporting obligations and capacity building, sections 54(1) and 54(2), is very clear in terms of the reporting of cybercrime, to whom cybercrime must be reported and the role of the Cabinet member responsible for policing in terms of classifying offences to be reported and how reporting must be done.

Of course as the Cabinet member responsible for State Security, I am informed of matters that raise the national risk and threat posture. When malicious activities in cyberspace and anywhere else surpass the threshold of criminality and threaten national security, it is the duty and obligation of the relevant authorities to report such to me. It is my responsibility and obligation to act in a manner that will maintain and ensure peace and stability in our country.

To answer your question about the countering steps that are in place, the State Security Agency, as the leading department looking into cybersecurity in government, has a Government Computer Incident Response Centre, where cybersecurity incidents are reported and responded to. Work is also underway to improve our detection and response capabilities, through capacity building (across multiple government sectors). So, in conclusion Honourable Member, work is underway aimed at improving and enhancing coordination and collaboration within government in order to respond to cybersecurity threats and combat cybercrimes effectively.