**NATIONAL ASSEMBLY**

**QUESTION FOR WRITTEN REPLY**

**PARLIAMENTARY QUESTION NO: 3497**

**DATE OF QUESTION PAPER: 03 NOVEMBER 2017**

**DATE OF SUBMISSION IN PARLIAMENT: 17 NOVEMBER 2017**

**Ms C King (DA) to ask the Minister of Justice and Correctional Services:**

What measures has his department put in place to mitigate the impact of cyber-attacks in the country?

**NW3924E**

**REPLY:**

In terms of the National Cybersecurity Policy Framework (NCPF) for South Africa, the Department of Justice and Constitutional Development is obliged to review the cybersecurity laws of the Republic to ensure that these laws are aligned with the NCPF, and provide for a coherent and integrated cybersecurity legal framework for the Republic. In accordance with the mandate of the Department, the Cybercrimes and Cybersecurity Bill (the Bill) was developed and introduced in Parliament as Bill 6 -2017 after a protracted consultation process. The Bill aims, amongst others, to put measures in place to deal with cybersecurity, capacity building and, as a subdivision of cybersecurity, also with cybercrimes.

Chapter 11 of the Bill provides for the declaration of essential information infrastructures as critical information infrastructures and provide for the implementation of special measures, amongst others, to regulate minimum security standards relating to:

1. the classification of data held by the critical information infrastructure;
2. the protection of, the storing of, and archiving of data held by the critical information infrastructure;
3. cybersecurity incident management by the critical information infrastructure;
4. disaster contingency and recovery measures which must be put in place by the critical information infrastructure;
5. minimum physical and technical security measures that must be implemented in order to protect the critical information infrastructure; and
6. other relevant matters that are necessary or expedient in order to promote cybersecurity in respect of the critical information infrastructure.

Cyber attacks are criminalized by various offences provided for in Chapter 2 of the Bill. Clause 11 of the Bill provides for specific offences that can be committed in respect of critical information infrastructures that are punishable with appropriate and proportional sentences.

The Bill further amends the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act 33 of 2004), in order to criminalize cyber- terrorist activities. Amendments are also affected to the Disaster Management Act, 2002 (Act 57 of 2002), to specifically make that Act applicable to disasters that may involve critical information infrastructures.

The Department also actively participates in initiatives of the interim Cyber Response Committee, which consists of various Departments, that is tasked to implement the NCPF. The NCPF makes provision for the development and implementation of various initiatives and measures by different Departments that are aimed at securing South Africa’s Information Communication Technologies.