Cybersecurity Policy finally published

By Ahmed Areff

14 Dec 2015

The State Security Department's National Cybersecurity Policy Framework, which was approved by Cabinet in 2012, has finally been published.

©Herman Lumanog via 123RF

The Right2Know (R2K) campaign said recently that, until October, the document was regarded as classified. The policy framework was published in last week's Government Gazette. It comes on the heels of the closure of public comments by the State Security Department on its controversial draft Cybercrimes and Cybersecurity Bill on 30 November.

R2K said in a statement on 30 November that parts of the draft bill were basically "a copy-and-paste of the worst parts of the secrecy bill". The bill seeks to create offences and impose penalties on cybercrime. It also seeks to impose obligations on electronic communication service providers regarding aspects that may affect cybersecurity.

R2K's media freedom and diversity organiser, Micah Reddy, told News24 that the bill was too broad in its current form and that a lot of it undermined privacy. Should it come into law, it would be bad news for investigative journalists, as it not only penalised those who leaked classified documents, but also those in possession of them, he said.

In its submission to the department against the bill, the group said penalties ranged from a maximum of five to 15 years in jail, depending on whether the information was classified confidential, secret or top secret. "There is no public interest

defence and no whistleblower protection. Even the limited and flawed exemptions contained in the protection of state information bill are missing."

"Effectively, even more so than the secrecy bill, the draft cybercrimes bill cannot tell the difference between an act of espionage and an act of journalism."

All-encompassing approach

The policy framework, defines "cyber espionage" as "the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature) from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage". The policy framework is "intended to implement an all-encompassing approach pertaining to all the role players (state, public, private sector, civil society and special interest groups) in relation to cybersecurity".

The National Cybersecurity Advisory Council was inaugurated in October 2013. It was established in terms of the policy framework, which was passed by Cabinet in March 2012.

State security minister David Mahlobo spoke about the framework policy at a cybersecurity symposium in March this year and in a speech that mentioned the fourth movie in the Die Hard franchise, Live Free or Die Hard, in which hackers bring down parts of the US infrastructure.

He mentioned several things the framework policy sought to do, including:

- Centralise coordination of cybersecurity activities within South Africa so as to have a coordinated approach to cybercrime, national security imperatives and to enhance the information society and knowledge-based economy;

- Strengthen intelligence collection, investigation, prosecution and judicial processes in respect of preventing and addressing cybercrime, cyber terrorism and cyber warfare;

- Anticipate and confront emerging cyber threats, in particular threats to the National Critical Information Infrastructure and to coordinate responses thereto; and

- Foster cooperation and coordination between government, the private sector and civil society, including ensuring that South Africa becomes a critical contributor to international cooperation on cybersecurity matters.

Source: News24