170530PC Justice

1

TERMINOLOGY USED IN THE CONTEXT OF THE CYBER BILL

1. **Cyberspace** means a physical and non-physical domain created by or composed of some or all of the following: computers, computer systems, networks and their computer programs, computer data, content data, traffic data and users.

2. **Cybersecurity** is the practice of making the networks that constitute cyberspace secure against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them.

3. **Cybercrime** means illegal acts, the commission of which involves the use of information and communication technologies.

4. **National Critical Information Infrastructure** means all Information Communication Technology (ICT) systems, data systems, data bases, networks (including people, buildings, facilities and processes) that are fundamental to the effective operation of the Republic.

5. **Transnational** means operating or extending across borders or beyond national boundaries. Cyberspace and cybercrime by its very nature transcends boundaries.

6. **Mutual legal assistance** is an agreement or arrangement between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws. This is particularly important by virtue of the transnational nature of cybercrime.

7. **Computer** (defined in the Bill) means any electronic programmable device used, whether by itself or as part of a computer system to perform predetermined operations in accordance with set instructions which include input devices, output devices, processing devices, computer data storage mediums and other equipment and devices that are related to , connected or used with such a device.

8. **Computer system** (defined in Bill) means one computer or two interconnected or related computers which allow these interconnected computers to exchange data or any function with each other or with another computer system.

9. **Data** (defined in Bill) is information stored on a computer.

10. **Restricted computer system** (defined in the Bill) means any data, computer programme, computer data storage medium or computer system under the control of or exclusive use by any financial institution, organ of state or critical information infrastructure.

Mr Mangena

11. **Malicious communications** is uttering, sending or delivering letters or other articles for the purpose of causing distress or anxiety.

12. **Seizure of data** includes making and retaining a copy of data or a computer programme and seizing a computer includes removing a computer data storage medium or any part of a computer system, rendering inaccessible data, a computer programme in order to preserve evidence.

13. **Expedited preservation** is prompt preservation of any form of data which is relevant to and which may afford evidence of the commission or intended commission of an offence.

14. **Expedited preservation of data direction** is an incidence where a specifically designated police official may, if he, on reasonable grounds believes that any person or service provider is in possession of or in control of data which is relevant to and which may afford evidence of the commission of or intended commission of an offence, issue an *expedited preservation of data direction* to that person or service provider.

15. **24/7 point of contact** is a structure under the direction of SAPS aimed at ensuring the provision of immediate expedited assistance for the purposes of proceedings or investigations regarding the commission of offences.

16. **Nodal points** are structures that assist with the distribution of information regarding cyber incidents within a sector (clusters of businesses (mobile cellular operators, banking etc...)which utilise ICT), receiving and distribution of information about cybersecurity incidents, reporting cybersecurity incidents, and receiving information about cybersecurity incidents.

17. **Computer Security Incident Response Team** is a team of dedicated information security officials that prepare for and responds to cybersecurity breaches or incidents.