CYBERCRIMES AND CYBERSECURITY BILL
Briefing to the Portfolio Committee on Justice and Correctional Services
30-31 May 2017

Bill 6 of 2017

the doj & cd
Department:
Justice and Constitutional Development
REPUBLIC OF SOUTH AFRICA

www.justice.gov.za
DOJCD_ZA DOJCD DOJCD

Background and need for comprehensive legislation

- The need for the Bill arises out of a growing threat to cybersecurity and increasing cybercrimes. In **South Africa** cybercrime is now the fourth most reported economic crime, according to the findings of PwC's 2016 Global Economic Crime Survey.

- Current legislation is utilised, to an extent, to deal with cyber crime offences but is inadequate for the following reasons:
  - ❖ It does not comprehensively and uniformly criminalise conduct which is regarded internationally as cybercrimes;
  - ❖ The common law is used to prosecute some of the offences but needs it grapples with new concepts that have arisen with digital technological advancements;

Background and need for comprehensive legislation

- There is no obligation on electronic communications service providers and financial institutions to report cybercrimes and to preserve evidence of cybercrimes on their systems;
- Cyber harassment is currently not recognised as a specific category of conduct in terms our and it should be criminalised, given increasing use of and access to the internet;
- There is no coherent and organised approach to deal with cybercrime and cybersecurity in South Africa;
- The investigative procedures provided for in the Criminal Procedure Act are object based and do not deal with the specialised procedures which are required to investigate cybercrimes, which involves electronic evidence which is of an incorporeal (cannot be seen or touched) nature;

Background and need for comprehensive legislation

- Inadequate capacity, both in the private and public sector, to deal with cybercrimes and cybersecurity;
- Information sharing about cyber incidents is limited. Information sharing ensures that adequate and timeous measures are implemented against a cyber threat and are therefore essential for the cybersecurity wellness of South Africa and to effectively act against cybercrimes; and
- Critical information infrastructures are not adequately protected.

Background in relation to other countries and international co-operation

- Current laws relating to jurisdiction is inadequate to deal with the transnational dimension of cybercrimes.

- Current legislation is not in line with those of the international community, which is essential for purposes of international cooperation and mutual legal assistance, which is mostly based on reciprocal laws.

Background in relation to other countries and international co-operation

- Many countries, for example Tanzania, Botswana, Nigeria Philippines, Singapore, Malaysia, Thailand, Sri-Lanka , New Zealand, Australia, Canada, United Kingdom, United States, have enacted comprehensive legislation to deal with cyber crimes to address the escalation of cybercrimes and cyber threats.

Policy Framework: National Cybersecurity Policy Framework (the NCPF)

- The development and implementation of a Cyber Security Policy and the development of capacity to combat and investigate cybercrime are acknowledged as measures which will make a substantial and positive impact on the safety of the people of South Africa.
- In this regard the National Cybersecurity Policy Framework (NCPF)was approved by Cabinet in 2012.
- The NCPF is a comprehensive framework which provides for the development, review and updating of existing substantive and procedural laws and measures to:
    - ❖ address national security in cyberspace;
    - ❖ combat cyber warfare, cybercrime and other cyber irregularities; and
    - ❖ build confidence and trust in the secure use of Information Communications Technologies.

This Bill give effect to the policy in relation to the development of substantive and procedural laws.

DEVELOPMENT OF BILL AND CONSULTATION PROCESS PRIOR TO INTRODUCTION

A draft Bill was finalised after consultation with numerous government departments as part of the implementation of the NCPF is concerned. These departments are: Department of Defence, Department of Home Affairs, Department of International Relations and Cooperation, Department of Science and Technology, NPA, the lower courts judiciary, Department of Telecommunications and Postal Services, South African Police Service and the State Security Agency.

In addition to the above, the Department also consulted with the E-commerce Advisory Committee, the Film and Publication Board, major electronic communications service providers, legal fraternity, the Banking Association of South Africa, the South African Reserve Bank, the South Africa Banking Risk Information Centre (SABRIC) and cybersecurity experts.

A draft Bill was also published in the Gazette, the webpage of the DOJ&CD, Lexus Nexus and JUTA. A process of engagement with interested parties was pursued to clarify aspects of the Bill. The Bill, as introduced, is an outcome of this consultation process.

Overview of Bill

- Rationalises the laws of the RSA which deal with cybercrime into a single Bill.
- Creates offences and impose penalties which have a bearing on cybercrime.
- Criminalises the distribution of communications which may adversely affect a person and provide for interim protection measures.
- Regulates jurisdiction to provide for the transnational dimension of cybercrimes.
- Regulates the powers to investigate cybercrimes.
- Regulates mutual assistance to deal with cross-border investigation of cybercrimes.

Overview cont.

- Provides for the establishment of a 24/7 Point of Contact to facilitate mutual assistance in the investigation of cybercrime.
- Regulates the proof of certain facts by affidavit.
- Imposes obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes and to report cybercrimes.
- Provides for the establishment structures to promote cyber security and capacity building.
- Provides for identification and declaration of critical information infrastructures and protection of critical information infrastructures.
- Provides that Executive may enter into agreements with foreign States to promote cybersecurity.
- Provides for the repeal and amendments of certain laws.

Summary of Bill

- Chapter 1: definitions (clause 1)
- Chapter 2: offences (clauses 2 to 15)
- Chapter 3: malicious communications (clauses 16 to 22)
- Chapter 4: Jurisdiction (clause 23)
- Chapter 5: Powers to investigate, search and seize (clauses 24 to 43)
- Chapter 6: mutual assistance (clauses 44 to 49)
- Chapter 7: 24/7 Point of Contact (clause 50)
- Chapter 8:evidence (Clause 51)

Summary of Bill (cont)

- Chapter 9: obligations of electronic communications service providers and financial institutions (clause 52).
- Chapter 10: Structures to deal with cybersecurity (clause 53 to 56)
- Chapter 11: critical information infrastructures protection(Clause 57-58)
- Chapter 12: National executive may enter into agreements with foreign States (clause 59)
- Chapter 13: General provisions (clause 60- 62).

Chapter by chapter discussion

Chapter 1

- Contains various definitions of a technical nature which are relevant to the interpretation of the various clauses of the Bill.

Chapter 2: Offences

- **Chapter 2** creates various offences which can be committed in cyberspace and aspects relating to criminal liability (clauses 2 to 15).
- **Clause 2** criminalises the unauthorised securing of access to data, a computer program, a computer data storage medium or a computer system.
- **Clause 3** criminalises the overcoming of a protection measure which is intended to prevent access to data and the subsequent acquiring of data, within or which is transmitted to or from a computer system.

Chapter 2 cont

- **Clause 4** criminalises –

* the possession, manufacturing, assembling, obtaining, selling, purchasing, making available or advertising of; or

* the use of,

software or hardware tools to commit certain offences provided for in the Bill.

- **Clause 5** criminalises the unlawful interference with data or a computer program.
- **Clause 6** criminalises the unlawful interference with a computer data storage medium or computer system.

Chapter 2 cont.

- **Clause 7** criminalises the unlawful –

* the use of passwords, access codes and similar data or devices in order to commit an offence;
* the possession of passwords, access codes and similar data or devices, with the knowledge that such data was acquired unlawfully; and
* the possession of passwords, access codes and similar data or devices, in regard to which there is a reasonable suspicion that it was acquired unlawfully where the possessor is unable to give a satisfactory account of such possession.

Chapter 2 cont

- **Clause 8** aims to create a statutory offence of cyber fraud to specifically criminalise fraud by means of data or a computer program, or through the interference with data or a computer program.
- **Clause 9** aims to create statutory offences of cyber forgery and cyber uttering.
- **Clause 10** aims to criminalise cyber extortion

Chapter 2 cont.

- **Clause 11(1)** criminalises unlawful conduct in cyberspace which is directed at essential computer systems. **Clause 11(2)** criminalises unlawful conduct in cyberspace which may endanger life, limb, property, essential services, the economy or the interests of the Republic.
- **Clause 12** provides that any attempt, or conspiring with another person, or the aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring of another person, to commit an offence as contemplated in Chapter 2 of the Bill, amounts to an offence.

Chapter 2 cont.

- **Clause 13** provides that the common law offence of theft must be interpreted to include the theft of an incorporeal, for instance the theft of valuable software or trade secrets.
- **Clause 14** prescribes penalties for the offences contemplated in Chapter 2 and circumstances which must be taken into account as aggravating circumstances.
- **Clause 15** deals with competent verdicts in respect of the various offences provided for in Chapter 2.

Chapter 3: Malicious communications

- This Chapter aims to criminalise the distribution of a data message which -

* incites the causing of any damage to any property belonging to, or violence against, a person or a group of persons (**clause 16**);
* is harmful (a data message is harmful if it threatens a person, or another person in a close relationship with that person with damage to property or violence; or intimidates, encourages or harasses a person to harm himself or herself or another person; or which is false in nature and is aimed at causing harm to another person) (**clause 17**); or
* is intimate in nature (eg the affected person is nude), and which is distributed without the consent of the such a person (**clause 18**).

Chapter 3 cont.

- **Clause 19** provides for interim protection orders against the conduct contemplated in clause 16, 17 or 18.
- **Clause 20** compels electronic communications service providers to assist with the identification of any person who has distributed a data message as contemplated in clauses 16, 17 and 18.
- In terms of **clause 21**, a court may on completion of criminal proceedings involving an offence contemplated in clauses 16, 17 and 18 make orders to criminalise the further distribution or availability of a malicious communication.
- **Clause 22** prescribes penalties for the offences provided for in this Chapter.

Chapter 4: Jurisdiction

- This Chapter expands the jurisdiction of courts to deal with the transnational dimension of cybercrimes (**clause 23**).

Chapter 5: Powers of SAPS to investigate cybercrimes

- Clause 24 provides for the issuing of Standard Operating Procedures which must be followed in the investigation of cyber offences or offences which have a cyber element.
- Clause 25 provides that the Criminal Procedure Act, applies in addition to the provisions of this Chapter in so far that it is not inconsistent with the provisions of this Chapter.

Chapter 5 cont.

- **Clause 26** provides that a police official may, in accordance with the provisions of Chapter 5, search for, access or seize any data, computer program, computer data storage medium or a computer system involved in the commission of an offence (hereinafter referred to as an article).
- **Clause 27** provides for the application for and the issuing of a search warrant to search for, access or seize an article. **Clause 28** provides for oral applications for search warrants.
- **Clause 29** provides for the search for, access to, or seizure of an article without a search warrant with the consent of the person who has lawful authority to consent.

Chapter 5 cont.

- **Clause 30** provides for the powers of a police official to search for, access, or seize an article in circumstances where the police official on reasonable grounds believes that a search warrant will be issued to him or her if he or she applies for such warrant and that the delay in obtaining such warrant would defeat the object of the search and seizure.
- **Clause 31** aims to further regulate the search for, access to, or seizure of an article on arrest of a person for an offence contemplated in Chapter 2 or clauses 16, 17 or 18, or under the provisions of section 40 or 43 of the Criminal Procedure Act.

Chapter 5 cont.

- **Clause 32** places obligations on persons, other than the accused person, to assist a police official in an investigation authorised in terms of a search warrant contemplated in clause 27.
- The obstructing or hindering of a police official or non-compliance with a search warrant in terms of clause 27, is criminalised by **clause 33**.
- **Clause 34** provides that the powers conferred upon a police official in terms of clauses 27(2), 29, 30 or 31, must be conducted with strict regard to decency and order and with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence.

Chapter 5 cont.

- Any wrongful search, access or seizure of an article as well as the use of any instrument, device, password or decryption key or information to gain access is criminalised in terms of **clause 35**. The clause also makes provision for civil liability in respect of damage which a person may have suffered as a result of any contravention of this clause.
- **Clause 36** criminalises the giving of false information which results in an investigation and also deals with civil liability as a result of a wrongful investigation.

Chapter 5 cont.

- **Clause 37** prohibits the disclosure of any information which a person has obtained in the exercise of his or her powers or the performance of his or her duties in terms of Chapter 5 or 6 of the Bill.
- **Clause 38** clarifies the operation of the RICA, vis-à-vis the Bill. This is to ensure that indirect communications and real-time communication-related information can only be intercepted or be obtained in terms of the procedures provided for in the RICA.
- **Clause 39** provides for expedited preservation of data which is necessary for the investigation of an offence.

Chapter 5 cont.

- **Clause 40** provides that a judicial officer may issue a preservation of evidence direction which may direct a person, for a time period specified in the direction (which may not exceed 90 days), to preserve an article involved in the commission of an offence. **Clause 41** provides for an oral application for a preservation of evidence direction.
- Where an expedited preservation of data direction or a preservation of evidence direction is in place, or where it is otherwise expedient to obtain data without issuing a search warrant, a judicial officer may, in terms of **clause 42**, issue a disclosure of data direction, directing a person to hand over data to a police official, if it is on reasonable

Chapter 5 cont.

grounds involved in the commission of an offence and that it would be in the interest of justice to issue the disclosure of data direction.

- **Clause 43** provides that a police official may without authorisation receive-

(a) publicly available data regardless of where the data is located geographically; or

(b) non-public available data, if the person, who has the lawful authority to disclose the data voluntarily and on such conditions regarding confidentiality and limitation of use which he or she deems necessary, discloses the data to a police official.

Chapter 6: Mutual Legal Assistance

- This Chapter provides for mutual legal assistance between RSA and foreign countries in the investigation of offences in terms of the Bill.
- **Clause 44** provides that Chapter 6 applies in addition to Chapter 2 of the International Co-operation in Criminal Matters Act, and relates, unless specified otherwise, to the preservation of evidence, pending a request in terms of section 2 or 7 of the International Co-operation in Criminal Matters Act, 1996.
- **Clause 45** provides for the exchange of information between the South African Police Service and foreign countries which may assist in the investigation of cybercrimes.

Chapter 6 cont.

• Requests by a foreign country for assistance and co-operation are regulated by **clause 46** of the Bill which provides that:

* The request must be submitted to the 24/7 Point of Contact which must submit the request to the NDPP for consideration.
* The NDPP must submit the request for assistance, together with his or her recommendations, to the Minister of the DOJ&CD for approval.
* If Minister approves it must be submitted to the designated judge who may, after complying with the provisions of the clause, issue orders to intercept/ preserve/seize the article in question.
* Where a request relates to the expedited disclosure of traffic data, the request must be submitted to the NDPP for consideration who must submit it to the designated judge for an appropriate order in accordance with the provisions of the clause.

Chapter 6 cont.

- **Clause 47** criminalises non-compliance with an order of the designated judge and provides for the amendment or the cancellation of the order concerned.

- **Clause 48** provides that the NDPP must inform the designated judge and a foreign State of the outcome of its request for assistance and cooperation. The clause further provides that any traffic data which is made available on an expedited basis, in terms of an order in terms of clause 46, must be provided to the 24/7 Point of Contact for submission to a foreign State.

Chapter 6 cont.

Clause 49 deals with requests for mutual assistance by South Africa to a foreign State, pending the issuing of a letter of request in terms of section 2(2) of the International Co-operation in Criminal Matters Act, to -

* preserve data or other articles;
* seize data or other articles on an expedited basis;
* disclose traffic data on an expedited basis;
* obtain data which is real-time communication-related information or archived communication-related information; or
* intercept data which is an indirect communication,

within the area of jurisdiction of a foreign State.

Chapter 7: 24/7

Clause 50 provides for the establishment and functions of the 24/7 Point of Contact as part of the South African Police Service.

Chapter 8

Clause 51 aims to further regulate the proof of certain facts by affidavit.

Chapter 9

Clause 52 imposes obligations on electronic communications service providers and financial institutions who are aware of, or become aware of the fact that their computer systems are involved in the commission of any category or class of offences provided for in Chapter 2 which is determined by the Cabinet member responsible for policing, to report such offences to the South African Police Service and to preserve any information which may be of assistance to the South African Police Service to investigate such offences.

Chapter 10

- **Clause 53** establishes the Cyber Response Committee (CRC) as the overseeing body which is responsible for the implementation of the cyber initiative of the Republic.
- **Clause 54** deals with the establishment of structures which support cybersecurity and capacity building. In terms of the clause:

* SSA must establish, equip, operate and maintain a computer security incident response team for Government;
* SAPS must establish 24/7;
* DTPS must establish Cyber Hub
* DOD must obtain cyber offensive/defensive capacity.

Departments involved must, in general, obtain skills and capacity to give effect to their constitutional mandates.

Chapter 10 cont

Clause 55 deals -

* with the establishment of nodal points and the recognition of private sector computer security incident response teams in the private sector; and
* with information sharing.

Clause 56 provides that the Cabinet member responsible for the administration of justice must make regulations to regulate information sharing, for purposes of Chapter 10.

Chapter 11

Clause 57 deals with the protection of critical information infrastructures. In terms of the clause the Cabinet member responsible for State security is empowered, after following an extensive consultation process, to declare certain information infrastructures as critical information infrastructures.

Chapter 11 cont

Clause 58 provides for the auditing of critical information infrastructures to ensure that there is compliance with a directive which is issued by the Cabinet member responsible for State security in terms of clause 57.

Chapter 12

In terms of **clause 59**, the National Executive may enter into agreements with any foreign State regarding mutual assistance and cooperation relating to the investigation and prosecution of offences contemplated in the Bill and various other matters which may impact on cybersecurity.

Chapter 13

- In terms of **clause 60**, the NDPP is obliged to keep statistics of the number of prosecutions instituted in terms of Chapter 2 or clause 16, 17 or 18 of the Bill. These statistics must be included in the report referred to in section 22(4)(g) of the National Prosecuting Authority Act, 1998.
- Clause 61 of the Bill proposes the deletion of section 71 of the South African Police Service Act/section 24B of the Films and Publications Act/sections 40A and 41(4) of the National Prosecuting Authority Act/ section 128 of the Correctional Services Act, 1998/ sections 65, 66 and 67 of the Financial Intelligence Centre Act/ and sections 85, 86, 87, 88 and 90 of the Electronic Communications and Transactions Act, which are superfluous as a result of the provisions of the Bill.

Chapter 13 cont

• Clause 61 of the Bill also proposes amendments to various other laws to facilitate the implementation of the Bill.

•Clause 62 provides for the making of regulations to further regulate aspects provided for in the Bill.

•Clause 63 deals with the Short Title and commencement.

Thank you