**PORTFOLIO COMMITTEE ON POLICE**

**14 March 2018**

**CRITICAL INFRASTRUCTURE PROTECTION BILL AND CYBERCRIMES AND CYBERSECURITY BILL: DISCUSSION OF OVERLAP BETWEEN THE TWO BILLS?**

**1. Introduction**

1.1 **Critical Infrastructure Protection Bill, 2017 (‘‘the Infrastructure Protection Bill’’)**

1.1.1 The **Infrastructure Protection Bill, seeks to replace the National Key Points Act, 1980** (Act 102 of 1980), and corresponding laws of the former TBVC States as is set out in the Schedule to that Bill. The **primary aims** of the Infrastructure Protection Bill are to -

(a) secure critical infrastructure against threats through the implementation of measures aimed at securing critical infrastructures and by mitigating risks to critical infrastructures through assessment of vulnerabilities and the implementation of appropriate measures[[1]](#footnote-1);

(b) provide for the confidentiality of information pertaining to certain critical infrastructure subject to the Promotion of Access to Information Act, 2000 (Act 2 of 2002)[[2]](#footnote-2);and

(c) provide for the identification and declaration of critical infrastructure and critical infrastructure complexes[[3]](#footnote-3).

1.1.2 In terms of clause 1 (the **definition clause**) of the Infrastructure Protection Bill -

(a) ‘‘**critical infrastructure**’’ is defined as any infrastructure which is declared as such in terms of clause 20(4);

(b) ‘‘**critical infrastructure complex**’’ is defined as more than one critical infrastructure grouped together for practical or administrative reasons, which is determined as such in terms of section 16(3);

(c) ‘‘**infrastructure**’’ is defined as any building, centre, establishment, facility, installation, pipeline, premises or systems needed for the functioning of society, the Government or enterprises of the Republic, and includes any transport network or network for the delivery of electricity or water;

(d) ‘‘**security**’’ is defined to includes, but is not limited to -

(i) physical security of critical infrastructure;

(ii) personnel security at critical infrastructure;

 (iii) contingency plans applicable to critical infrastructure; and

 (iv) measures aimed at protecting critical infrastructure; and

(e) ‘‘**security measures**’’ is defined as any physical security measure to preserve the availability, integrity or confidentiality of a critical infrastructure, and includes, but is not limited to, physical security measures to protect -

(i) any part or component of a critical infrastructure;

 (ii) any physical structure that partly consists of, incorporates or houses

 information infrastructure; or

 (iii) personnel or other persons at or nearby a critical infrastructure; and

(f) ‘‘**threat**’’ is defined to include any action or omission of a criminal, terrorist or accidental nature which may potentially cause damage, harm or loss to critical infrastructure or interfere with the ability or availability of critical infrastructure to deliver basic public services, and may involve any natural hazard which is likely to increase the vulnerability of critical infrastructure to such action or omission.

1.1.3 Clause 16 of the Infrastructure Protection Bill empowers the Cabinet member responsible for policing (the Minister) to declare critical infrastructure and critical infrastructure complexes after considering the conditions provided for in clauses 16(2) and 17. For purposes of the current discussion **clause 16(4), (5) and (6)** is important and is quoted hereunder:

 **“(4) In the event where any infrastructure partly consists of, incorporates or houses, any information and communications infrastructure as contemplated in any legislation on cybersecurity, the Minister must consult with the Cabinet member responsible for State Security before exercising any power contemplated in subsection (1).**

 **(5) The Cabinet member responsible for State Security must—**

**(*a*) consider whether the information and communications infrastructure referred**

**to in subsection (4) must be dealt with in terms of any legislation on cybersecurity; and**

**(*b*) inform the Minister, in writing, of his or her decision.**

 **(6) Where the Cabinet member responsible for State Security decides that the information and communication infrastructure referred to in subsection (4) must not be dealt with in terms of any legislation on cybersecurity, the Minister must deal with the application contemplated in subsection (1), in terms of this Act.”.**

A **proposed amendment to clause 30** of the infrastructure Protection Bill was brought to my attention in terms of which the following subclause is added to clause 30:

 **“(9) In the event that no legislation on cybersecurity is in operation when this Act comes into operation, the Minister must, in consultation with the Cabinet member responsible for State Security, determine interim guidelines on the manner in which an application referred to in section 16(4) must be dealt with by any person performing a function in terms of this Act.”.**

1.2 **Cybercrimes and Cybersecurity Bill (“the Cyber Bill”)**

1.2.1 The **National Cybersecurity Policy Framework for South Africa** (the NCPF) was approved by Cabinet in 2012 and provides for measures to address national security in cyberspace; measures to combat cyber warfare, cybercrime and other cyber irregularities; the development, review and updating of existing substantive and procedural laws; and measures to build confidence and trust in the secure use of Information Communications Technologies. In terms of paragraph 16.1 of the NCPF, the Department of Justice and Constitutional Development (the DOJ&CD) must review and align the cybersecurity laws of the Republic to ensure that these laws are aligned with the NCPF and in order to provide for a coherent and integrated cybersecurity legal framework for the Republic. The Bill gives effect to this mandate of the DOJ&CD.

1.2.2 The Bill aims to rationalise the laws of South Africa which deal with cybercrime and cybersecurity into a single Bill and to that extent the **Bill seeks to** -

(a) create offences and impose penalties which have a bearing on cybercrime (Chapter 2);

(b) criminalise the distribution of malicious communications and to provide for interim protection measures (Chapter 3);

(c) regulate jurisdiction to provide for the transnational dimension of cybercrimes (Chapter 4);

(d) regulate the power to investigate cybercrimes (Chapter 5);

(e) regulates mutual assistance to deal with cross-border investigation of cybercrimes (Chapter 6);

(f) provide for the establishment of a 24/7 Point of Contact to facilitate mutual assistance in the investigation of cybercrime (Chapter 7);

(g) regulate the proof of certain facts by means of affidavit (Chapter 8);

(h) Impose obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes and to report cybercrimes (Chapter 9);

(i) provide for the establishment of structures to promote cybersecurity and capacity building (Chapter 10);

(j) provide for the identification and declaration of critical information infrastructures and the implementation of measures to protect critical information infrastructures (Chapter 11);

(k) provide that the Executive may enter into agreements with foreign States to promote cybersecurity (Chapter 12); and

(l) provide for the repeal and amendments of certain laws (Chapter 13).

1.2.3 For the present discussion it is only necessary to deal with **Chapter 11** (clauses 57 and 58) that provide for the identification and declaration of critical information infrastructures, the implementation of measures to protect critical information infrastructures and auditing requirements in order to evaluate compliance with the protection measures. In terms of **clause 57** of the Cyber Bill:

 **“(1) The State Security Agency—**

***(a)* in consultation with the Cyber Response Committee; and**

***(b)* after consultation with the owner of, or the person in control of any information infrastructure which is identified as a potential critical information infrastructure,**

**must within 12 months of the fixed date, submit to the Cabinet member responsible for State security, information and recommendations regarding information infrastructures which need to be declared as critical information infrastructures.**

 **(2) The Cabinet member responsible for State security may, subject to subsection (3), after considering any information and recommendations made to him or her in terms of subsection (1), by notice in the *Gazette*, declare any information infrastructure, or category or class of information infrastructures or any part thereof, as critical information infrastructures if such information infrastructure or information infrastructures are of such a strategic nature that any interference with them or their loss, damage, disruption or immobilisation may—**

***(a)* substantially prejudice the security, the defence, law enforcement or international relations of the Republic;**

***(b)* substantially prejudice the health or safety of the public;**

***(c)* cause a major interference with or disruption of, an essential service;**

***(d)* cause any major economic loss;**

***(e)* cause destabilisation of the economy of the Republic; or**

***(f)* create a major public emergency situation.**

 **(3) …….. .**

**(4) The Cabinet member responsible for State security must, within six months of the declaration of any information infrastructure, or category or class of information infrastructure or any part thereof, as a critical information infrastructure, in consultation with the relevant Cabinet members, issue directives to the critical information infrastructure in order to regulate minimum standards relating to—**

***(a)* the classification of data held by the critical information infrastructure;**

***(b)* the protection of, the storing of, and archiving of data held by the critical information infrastructure;**

***(c)* cybersecurity incident management by the critical information infrastructure;**

***(d)* disaster contingency and recovery measures which must be put in place by the critical information infrastructure;**

***(e)* minimum physical and technical security measures that must be implemented in order to protect the critical information infrastructure;**

***(f)* the period within which the owner of, or person in control of a critical information infrastructure must comply with the directives; and**

**(*g*) any other relevant matter which is necessary or expedient in order to promote cybersecurity in respect of the critical information infrastructure.**

 **(5) ...... .**

 **(6) ....... .**

 **(7) ....... .**

 **(8) The owner of, or person in control of a critical information infrastructure must in consultation with the Cabinet member responsible for State security, at own cost, take steps to the satisfaction of the Cabinet member for purposes of complying with the directives contemplated in subsection (4).**

 **(9) If the owner of, or person in control of a critical information infrastructure fails to take the steps referred to in subsection (8), the Cabinet member responsible for State security may, by written notice, order him or her to take such steps in respect of the critical information infrastructure as may be specified in the notice, within the period specified in the notice.**

 **(10) An owner of, or person in control of the critical information infrastructure who without reasonable cause refuses or fails to take the steps specified in the notice referred to in subsection (9), within the period specified therein, is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.**

 **(11) (*a*) If the owner of, or person in control of, the critical information infrastructure fails or refuses to take the steps specified in the notice referred to in subsection (9), within the period specified therein, the Cabinet member responsible for State security may take or cause to be taken those steps which the owner or person failed or refused to take, irrespective of whether the owner or person has been charged or convicted in connection with that failure or refusal, and the Cabinet member may recover the costs of those steps from the owner or person on whose behalf they were taken.**

 **(*b*) A failure by a provincial government to take the steps specified in the notice referred to in subsection (9), within the period specified therein, must be dealt with in accordance with section 100 of the Constitution.**

 **(12) For purposes of this section—**

***(a)* ''classification of data'', for purposes of subsection (4)*(a)*, means to assign a level of sensitivity, value and criticality to the data for purposes of security controls for the protection of the data;**

***(b)* …… .**

***(c)* …… .**

***(d)* ''information infrastructure'' means any data, computer program, computer data storage medium, computer system or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto; and**

***(e)* "relevant Cabinet members" means the Cabinet members responsible for defence, telecommunications and postal services, the administration of justice, policing and State security.**

**Clause 58** of the Cyber Bill provides for the auditing of critical information infrastructures to ensure compliance with a directive which is issued by the Cabinet member responsible for State security in terms of clause 57(4). The owner or person in control of a critical information infrastructure must, once every 24 months, at own cost cause an audit to be performed on the critical information infrastructure by an independent auditor in order to evaluate compliance with the directive. The critical information infrastructure must notify the Director-General: State Security of the date on which an audit is to be performed whereupon the Director-General: State Security may designate any member of the State Security Agency or any other person to monitor, evaluate and report on the adequacy and effectiveness of the audit. The owner or person in control of a critical information infrastructure must, upon completion of the audit, report in the prescribed form and manner to the Director-General: State Security regarding the outcome of the audit in order to enable the Director-General to evaluate compliance with the directive. The failure to perform an audit or to comply with the various regulatory provisions of the clause is criminalised. The Cabinet member responsible for State security must, by notice in the *Gazette*, prescribe the persons or the category or class of persons who are competent to be appointed to perform an audit as contemplated in the clause.

**2. Discussion**

2.1 The Infrastructure Protection Bill and the Cyber Bill must be considered in light of the fact that many **traditional critical infrastructures rely on information and communication technologies to function**. Such information infrastructures may be localised at a specific critical infrastructure, may extend to critical infrastructure complexes by means of local area networks or networks that do not belong to such an infrastructure and which may be used to transfer data from one destination to another or as a means of communication. Information infrastructure may further either be contained at a specific place at an infrastructure or may be incorporated to various degrees in other physical components at an infrastructure.

2.2 As already pointed out, the Infrastructure Protection Bill, seeks to **replace the National Key Points Act**, 1980 and corresponding laws of the former TBVC States. Similarly, the **Cyber Bill aims to renew current legislation** on the Statute Book. In the Schedule to the Cyber Bill, the Electronic Communications and Transactions Act, 2002 (Act 25 of 2002) (“the **ECTA**”) is amended by the deletion in section 1 of the definitions of ''critical data'', ''critical database'' and ''critical database administrator'' and the deletion of Chapter IX. Chapter IX (sections 52 to 58) of the ECTA deals with the protection of critical databases. A “critical database” is defined in section 1 of the ECTA as “a collection of critical data in electronic form where it may be accessed, reproduced or extracted”. Critical data is in turn defined as “data that is declared by the Minister in terms of section 53 to be of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens”. From the wording of sections 52[[4]](#footnote-4), 54(2)(*b*) and (*c*)[[5]](#footnote-5) and 55, one may conclude that a critical database comprises of physical elements, in other words, information infrastructure. Chapter IX of the ECTA co-exits with the National Key Points Act, 1980 on the Statute Book in that the National Key Points Act, 1980 provided for the protection of physical infrastructure[[6]](#footnote-6) and the ECTA provides for the protection of information infrastructures.

2.3 Critical **infrastructure and critical infrastructure complex is defined** in the Infrastructure Protection Bill with reference to the definition of ‘‘infrastructure’’. Infrastructure is in turn defined as “any building, centre, establishment, facility, installation, pipeline, premises or systems needed for the functioning of society, the Government or enterprises of the Republic, and includes any transport network or network for the delivery of electricity or water”. This **broad definition may include information infrastructure** by virtue of the words “facility”, “installation”, “system”, “network for the delivery of water” etc. In terms of the Cyber Bill, **critical information infrastructures would be** information infrastructures that are of such “a strategic nature that any interference with them or their loss, damage, disruption or immobilisation may—

(a) substantially prejudice the security, the defence, law enforcement or international relations of the Republic;

(b) substantially prejudice the health or safety of the public;

(c) cause a major interference with or disruption of, an essential service;

(d) cause any major economic loss;

(e) cause destabilisation of the economy of the Republic; or

(f) create a major public emergency situation”.[[7]](#footnote-7)

Clause 57(12)(*d*) of the Cyber Bill defines ''**information infrastructure**'' as any data, computer program, computer data storage medium, computer system or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto”. This definition may equally include some structures that may resort under the Infrastructure Protection Bill.

2.4 There are **important differences between critical infrastructure protection and critical information infrastructure protection**. Some of these differences are discussed below:

(a) Threats

The *threats against critical infrastructure* in general and as contemplated in the Infrastructure Protection Bill are mainly of a physical nature (for instance unauthorised access, publication of essential information about an infrastructure, sabotage, terrorism or a natural hazard), that is committed against physical infrastructure (such as a dam, an airport, a power station etc) that affects the physical security of an infrastructure. *Threats against critical information infrastructures* are of a non-physical nature. It can be committed without a physical presence at the affected infrastructure and a single perpetrator can simultaneously lodge multiple attacks on multiple infrastructures. It is difficult to detect a threat unless special protocols are in place. Special technical solutions are necessary to prevent threats and to deal with the effect of such threats. The aim of such threats is to affect computer programs, which in turn will have an adverse effect on physical infrastructure or to gain access to protected data. Examples of threats against information infrastructures include denial of service attacks, unauthorised access to data, the distribution of malware such as worms, viruses, and Trojans that can copy data and sending it to another address, manipulate data, hinder the operation of information infrastructure, delete, suppress or block access to data. One of the legendary attacks on a critical infrastructure took place at Bushehr nuclear power plant in Iran, where the Stuxnet worm adjusted equipment at the plant to self-destruct.

(b) Protection measures

The protection measures which need to be implemented for the protection of critical infrastructure and critical information infrastructure differ. *Protection measures at critical infrastructure* are aimed at access control and measures to protect the physical infrastructure and persons at the infrastructure. These protection measures are in the form of persons that must enforce prescribe measures to protect an infrastructure. *Protection measures that relate to critical information infrastructures* are more complex and include, among others:

(i) Access control protocols and measures that restricts access to data at a critical information infrastructure to authorised users.

(ii) The role-players involved in critical information infrastructure protection is not limited to a specific location and may include various other role-players that renders complementary services, such as network services, software or hardware that is utilised at an information infrastructure.

(iii) Specialised expertise and knowledge is required to safeguard information infrastructures and to deal with different threats that evolve on almost a daily basis.

(iv) Special technical solutions are needed to prevent and detect threats such as firewalls, antivirus software etc. These technical solutions must regularly be updated and sometimes be developed due to the ever-changing nature of possible threats.

(v) Specialised knowledge and or technical solutions are necessary to effectively deal with the result of threats.

(c) Enforcement of protection measures

Prescribed measures to protect critical infrastructure protection are *enforced by persons* at a critical infrastructure that must ensure compliance with these measures. Protection of critical information infrastructures against threats are *largely based on technical solutions* that must detect, prevent and mitigate threats against information infrastructures.

(d) Offences

Specific offences are necessary to criminalise contraventions. In respect of critical infrastructure, unauthorised access, conduct that may damage the infrastructure, conduct that may threaten the safety of persons at the infrastructure, the making available of sensitive information regarding an infrastructure and non-compliance with enforcement mechanisms, are criminalised. Offences that aims to criminalise conduct in respect of critical information infrastructures are aimed at protecting devices, programmes and data by means of specific offences such as unlawful securing of access to an information infrastructure, unlawful conduct that may interfere with an information infrastructure (such as computer systems, data and programmes) and unauthorised obtaining and using of access codes.

**3. Overlapping issues**

3.1 The **distinction between critical infrastructure and critical information infrastructures already existed** **before** the promotion of the Infrastructure Protection Bill and the Cyber Bill as a result of the co-existence of National Key Points Act, and the ECTA on the Statute Book[[8]](#footnote-8). Various **countries** deal with the protection of physical infrastructures and information infrastructures. In terms of their regulatory measures different agencies have mandates to deal with infrastructure protection and information infrastructure protection.

3.2 It must be admitted that there is a **measure of overlap between the Infrastructure Protection Bill and the Cyber Bill**.[[9]](#footnote-9) The overlap in protection measures that must be implemented at the respective infrastructures, is found in **clause 57(4)(*e***) of the Cyber Bill that provides for “minimum physical …… measures that must be implemented in order to protect the critical information infrastructure” and paragraph (*b*) of the **definition of “security measure”** **in clause 1** of the Infrastructure Protection Bill that provides for physical security measures to preserve and to protect “any physical structure that partly consists of, incorporates or houses information infrastructure”.[[10]](#footnote-10) It is clear that the Infrastructure Protection Bill does not aim to extend protection to the information infrastructure, itself, but only a structure that houses such information infrastructure. On the other hand clause 57(4)(*e*) of the Cyber Bill also aims to extend to physical security of an information infrastructure that may include “any building, structure, facility” (in other words physical components that need to be protected). It is submitted that these **provisions are necessary** for the following reasons:

(a) Protection measures that may be implemented to protect the physical structure in so far as it relates to infrastructure protection and information infrastructure protection may differ. Protection measures that relate to infrastructure protection are aimed at securing the physical structure itself. Protection measures in respect of information infrastructure are aimed at securing data, programmes, networks and devices at a physical infrastructure.

(b) There may be instances where critical infrastructure house **information infrastructure that is not regarded as critical**. In such instances the Infrastructure Protection Bill will provide protection at physical structures that partly consist of, incorporates or houses information infrastructure. Furthermore, there may also be instances where **an infrastructure may not be considered as critical but house information infrastructure that may be critical**, and it is submitted that clause 57(4)(*e*), read with the definition of information infrastructure in clause 57(12)(*d*) of the Cyber Bill, may be used to protect any “building, structure, facility” that house such an infrastructure.

3.3 In order to deal with this overlap clause 16(4), (5) and (6) and the proposed clause 30(9) of the Infrastructure Protection Bill provides for a consultation process between the Minister and the Cabinet member responsible for State security in order to decide the appropriate law under which the infrastructure should be dealt with. If the Cabinet member responsible for State security decides that the infrastructure that houses an information infrastructure should be dealt with in terms of the provisions of the Cyber Bill, clause 57(4) obliges the said Cabinet member to consult, among others with the Minister on the directive that should be issued to regulate standards that should be implemented at such infrastructure. This double consultation requirement will ensure that no contradictory or overlapping security measures are prescribed in respect of the same physical structure that houses an information infrastructure.

**4. Conclusion**

4.1 There is an overlap between the Infrastructure Protection Bill and the Cyber Bill as a result of clause 57(4)(*e*) of the Cyber Bill.

4.2 Clause 57(4)(*e*) of the Cyber Bill can only be used to regulate security measures at a physical infrastructure if an information infrastructure is declared a critical information infrastructure and there is a building, structure, facility, system or equipment associated therewith. If an information infrastructure is not considered critical, it must be dealt with in terms of the Infrastructure Protection Bill. The fact that a critical information infrastructure exists at an infrastructure does not imply that the infrastructure in question will become a critical information infrastructure.

4.3 In practice, the two Bills will complement each other. The Infrastructure Protection Bill that provides for physical security measures addresses unlawful physical actions against information infrastructures or their components at a critical infrastructure that may affect their availability and integrity. The Infrastructure Protection Bill, however, does not primarily deal with the protection of information infrastructure that may have an adverse effect on the critical infrastructure itself. The Cyber Bill aims to put in place measures that are primarily aimed at securing information infrastructure against mostly non-physical attacks that may have an adverse effect on a critical information infrastructure which in turn will adversely affect a critical infrastructure.

4.4 Clause 16(4), (5) and (6) and the proposed clause 30(9) of the Infrastructure Protection Bill and Clause 57(4) aim to ensure that the respective Cabinet members that are tasked to make regulatory measures for critical infrastructure must consult with one another. This will ensure that only one of the functionaries must deal with an identified infrastructure or a component or portion of such infrastructure. The practical effect of the integration of computer technology in critical infrastructures is that the Cyber Bill and the Infrastructure Protection Bill will, more usually than not, simultaneously apply to an identified infrastructure. In such an instance the respective components of the infrastructure must be evaluated to determine whether they are physical infrastructure or information infrastructure to determine the application of the respective Bills.

4.5 If there is a need to further clarify this aspect, amendments to the Cyber Bill may be proposed.

1. Clause 2(*a*) and (*e*). [↑](#footnote-ref-1)
2. Clause 2(*b*) [↑](#footnote-ref-2)
3. Clause 3 [↑](#footnote-ref-3)
4. “critical databases or parts thereof”. [↑](#footnote-ref-4)
5. “(b) the location of the critical database, including the locations of component parts thereof where a critical database is not stored at a single location; and

 (c) a general description of the categories or types of information stored in the critical database excluding the contents of such critical database”. [↑](#footnote-ref-5)
6. In terms of section 1 of the National Key Points Act, 1980, 'National Key Point' is defined as any “place or area which has under section 2 been declared a National Key Point”. Section 1 further defines “area” as soil or water surface, whether with a building, installation or structure thereon or not, and includes any place; and “place” as “any premises, building, installation or industrial complex”. It must be pointed out that the word “installation” may include components of information infrastructure at such a place, but this must be read with Chapter IX of the ECTA that specifically provides that information infrastructure that is considered as a “critical database” must be dealt with in terms of the ECTA. [↑](#footnote-ref-6)
7. Clause 57(2) of the Cyber Bill. [↑](#footnote-ref-7)
8. Paragraph 2.2, above. [↑](#footnote-ref-8)
9. See paragraph 1.1.2(a), (b) and (c), above where the definitions of “critical infrastructure”, “critical infrastructure complex” and “infrastructure” are discussed and paragraph 2.3, above and clause 57(12)(*d*) of the Cyber Bill. [↑](#footnote-ref-9)
10. See paragraph 1.1.2(d) and (e) where the definitions of “security” and “security measures” are discussed and paragraph 1.2.3 where section 57(4) of the Cyber Bill is quoted. [↑](#footnote-ref-10)