Comments on the Cybercrimes and Cybersecurity Bill

Prof Basie von Solms

Director: Centre for Cyber Security

University of Johannesburg

November 2015

1. Introduction

This set of comments is very general and do not go into detail. Detailed inputs on the general comments in this document can be provided if these general comments are seen as valuable. The comments provided will all be on the Structures described in Chapter 6 and also in Chapter 5. Such comments are all on technical aspects, and do not refer at all to the legal components of the Bill as I am not a legal expert in any way. Comments will also be in terms of the major problems I envisage with the implementation of the Bill although there are many smaller comments on certain aspects.

Comments will cover the following aspects:

- The lack of Cyber Security capacity to implement the Structures
    - a proposal to develop more capacity
    - ignoring existing cyber capacity expertize capacity in the private sector
- The 'silo-based' approach of the Structures described in the Bill

2. The lack of Cyber Security capacity to implement the Structures

2.1 A proposal to develop more capacity

It is totally unrealistic to think that the Structures as described in the Bill can be implemented with the present level of Cyber Security capacity in SA – the country simply do not have sufficient capacity to implement the tasks assigned to many, if not all of these structures.

An example is the Cyber Security Hub. The activities listed is 56 (5) (a) to (m) will need a significant number of experienced and skilled staff members – a conservative estimate will be at least 20 full time staff members. It is well known that there is a lack of such experienced and skilled capacity in SA, and internationally.

Without such capacity, the Hub will become a structure on paper and will cause extreme frustration amongst citizens and other stakeholders as their complaints and problems will not be addressed properly and in time.

The situation can of course be addressed by developing such capacity by Upskilling, Reskilling and Initial Skilling.

Doing this using the traditional and existing avenues will not produce enough expertise fast enough. Innovative and out-of-the-box ways of fast tracking the development of totally new capacity must be investigated, defined and implemented.

Such innovative ways do exist but the political will to quickly implement such solutions will make or break the success of the implementation of the Bill.

The present formulation of the Bill does not address this problem in any way.

Proposal: Create and implement new ways to fast track the development of Cyber Security capacity

2.2 Ignoring existing cyber capacity expertise in the private sector

It is clear that the Bill was drafted without thorough consultations with the private sector.
Generally it is accepted that most of Critical Information Infrastructures are managed by the private sector. Because of that factor, private industry has substantial knowledge and skills, as well as experience in managing different structures related to Critical Information Infrastructures.
This fact had been totally ignored by the Bill.

Proposal: Create a wider discussion with private industry to determine how existing structures in the private industry can used by and integrated with the Structures proposed in the Bill.

3. The 'silo-based' approach of the Structures described in the Bill

The Bill is especially guilty of this problem which is related to paragraph 2 above. With the present lack of experienced and skilled capacity in SA, the Bill creates at least 5 Structures which have an immense overlap of activities. As an example, the activity of incident response and investigation is present in some form or the other in all these structures.

It is short sighted to dilute and distribute the available expertise in this country is such an unnecessary and strategically risky way.

If these Structures could have been combined in some way, physically or virtually, and the skills consolidated, much better service would have been possible and unnecessary overlap and duplication would have been eliminated or at least minimalized.

SA is a developing country and such overlapping Structures, which would surely be possible a developed countries, is a luxury this country cannot afford.

Correcting this problem will be difficult as political infighting will not allow the Structures to be combined – in fact, it is my opinion that such infighting actually led to this silo-based Structures. However consolidation and coordination of some sort is essential as without that SA will not effectively secure its Cyber Space.

The easiest way to address that is to establish a National Cyber Coordinator whose responsibility will be to oversee the effectiveness of and cooperation between the proposed Structures. Such a National Coordinator's role is also advised by the UN's International Telecommunications Union.

Such a Coordinator should be a full time dedicated expert in the cyber field, not reporting to any of the Government Departments who are involved in the present Structures. The most logical line will be reporting directly to the President's Office. The fact that the Coordinator must be an expert in the cyber field is that a major part of the Coordinator's role will be technically oriented.

The Bill does create the Cyber Response Committee (CRC) who has amongst other, the following responsibility:

' to coordinate cybersecurity activities …' and 'to oversee and guide the functioning of the 24/7 PoC, Cyber Security Centre, GSIRT, Cyber Crime Centre, Cyber Command, the Cyber Hub etc..'

The CRC cannot perform the role envisaged by the proposed National Cyber Coordinator for the following reasons:

- The CRC is not a dedicated full time facility which is essential for this role
- The CRC is a committee and not a dedicated resource
- The CRC is not made up of cyber experts but are all persons occupying other Government roles
- The CRC does not report outside the Government departments in which the Structures are hosted.

The proposed National Cyber Coordinator should not replace the CRC but should be intensely and full time be involved with the operational aspects of the Structures as far as coordination and effectiveness are concerned.

Proposal : Establish the position of National Cyber Coordinator along the lines as indicated above.

4. Summary

As stated above, I have several other aspects of criticism, but the two discussed above are those that I see as essential to ensure that the Bill, if enacted, does not become ‘just another piece of paper’.