Comments on the Cybercrimes and Cybersecurity Bill (B-6, 2017)

Prof Basie von Solms

Director: Centre for Cyber Security

University of Johannesburg

March 2017

1. Introduction

As an academic deeply involved with capacity building in the (technical) area of Cybersecurity, my comments will be limited to cybersecurity capacity building.

It is a well-accepted fact internationally that cybersecurity capacity is at a premium, and that there are large numbers of vacancies in relevant cyber related fields.

The following two papers emphasize this aspect on an international level.

Cybersecurity Skills Shortage: A State of Emergency
(We) has been researching, writing about, and addressing the cybersecurity skills shortage for a number of years.
Unfortunately, this situation continues to deteriorate. In a disquieting development, nearly half of organizations now claim to have a problematic shortage of cybersecurity skills.
Additionally, a vast majority of organizations acknowledge that it is difficult to recruit and hire cybersecurity talent. (We) believe that this trend represents a national security risk demanding a comprehensive strategy from national governments.
http://www.esg-global.com/hubfs/ESG-Brief-Cybersecurity-Skills-Shortage-Feb-2016.pdf

Hacking the Skills Shortage - A study of the international shortage in cybersecurity skills
A secure cybersecurity environment requires a robust workforce, yet currently there are not enough cybersecurity professionals to adequately defend computer networks. Countries and companies have to act quickly to fix this problem by facilitating the entry of more people into this profession through improvements in education, workforce diversity, training opportunities, security technology, and data collection. These concurrent efforts are vital to defeating cybersecurity threats and creating a more secure network environment.
https://www.mcafee.com/in/resources/reports/rp-hacking-skills-shortage.pdf

The next comments zoom into this aspect as far as SA is concerned.

SA faces ICT skills crisis
South Africa still has a massive skills shortage in ICT, with a concerted effort from industry and academia required to help the country build the capacity needed to develop a digital economy.
https://it-online.co.za/2016/07/19/sa-faces-ict-skills-crisis/

The real worrying aspect is whether the Draft Bill takes these aspects of shortages into account. The clear impression is that it is not! This will be elaborated on later.

2. Addressing Capacity

The draft Bill suggests at least 3 forms of Incident Response Teams – the 24/7 Point of Contact, The Government Incident Response Team (Government CSIRT) and the Cybersecurity Hub (National CSIRT).

The skills and needed for a CSIRT is comprehensive.

What Skills Are Needed When Staffing Your CSIRT?

If you want to build a computer security incident response team (CSIRT) with capable incident handlers, you need people with a certain set of skills and technical expertise, and with abilities that enable them to respond to incidents, perform analysis tasks, and communicate effectively with your constituency and other external contacts. They must also be competent problem solvers, must easily adapt to change, and must be effective in their daily activities. It is not often easy to find such qualified staff, so sometimes CSIRTs nurture and train internal staff members to advance into these incident handling roles.

http://www.cert.org/incident-management/csirt-development/csirt-staffing.cfm

The real question as far as this Bill is concerned, should be - does SA presently have the cybersecurity capacity to populate 3 such CSIRTs at the effective operational level to really deliver the services to their constituency as specified in the Bill?

From my view, the answer is a categorc NO!

We will just dilute the little capacity we have and nobody will be able to provide a comprehensive service as specified by the Bill.

The Bill is therefore on an extremely risky (and irresponsible) path to suggest such separate structures which will create expectations from constituents which will not be able to be delivered. At this stage SA does not have the luxury to operate 3 different structures basically doing the same thing.

The chances are big that if enacted in its present piece-meal form, the Bill will become a document on paper with little added value for the ordinary citizen

The silo-based approach by dividing 'the cybersecurity cake' is irresponsible and goes against the established norm of optimizing available resources.

3. Proposal

In the light of the discussion above, the following should seriously be considered:

1. At this point in time, merge the 3 (or more) structures suggested into one, and consolidate all the available skills which would have been deployed in the 3 structures, into one national CSIRT structure providing services to all constituents mentioned.
2. Immediately create a national cybersecurity capacity program on national level and grow more skills.
3. In time, when more skills become available, progressively split/divide the one national CSIRT structure into more as required.

Finally, I see the omission of establishing the position of a National Cyber Coordinator, as suggested in my November 2015 Comments, as a serious deficiency in a national Cyber Strategy in SA.