# The Impact of Cybercrimes and Cybersecurity Bill on South African National Cybersecurity: An Institutional Theory Analytic Perspective

J Phahlamohlaka[1] , J Hefer[2]

[1] Defence Peace Safety and Security: CSIR, Pretoria, South Africa

[2] Department of Defence, Pretoria, South Africa

jphahlamohlaka@csir.co.za

Johan.hefer@sita.co.za

***Special Note**: This analysis was done in 2016 before the Cybersecurity was separated from Cybercrime in the Bill. The power point version of this paper was presented to the 2016 Military Information and Communication Symposium of Southern Africa (MICSSA) conference but there were no published proceedings for MICSSA. After considering public comments, the RSA Parliament has amended the Bill with effect from 07 November 2018 and it is now called the Cybercrimes Bill, with all the Institutional structures previously included except the South African Police Services, removed from the Bill. The concepts from Institutional Theory used for the analysis remains unchanged and valid. It is expected that several cyber related Bills will in future be promulgated with each of the institutions mentioned in the previous Bill taking the lead. It is envisaged that when that happens, the analysis given in this paper could provide some special insights*

## Abstract

Our aim in this paper is to analyse the possible impact of the Cybercrimes and Cybersecurity Bill on the institutions charged with the responsibility to enforce it as outlined in chapter 6 of the Bill. The analysis is conducted using selected concepts from Institutional Theory. Assuming that the Bill has been passed and that all current fears and concerns from the various institutions and stakeholders have been addressed; we trust that our analysis will provide some insight on how from an institutional theoretic perspective, the bill will, at least from an enforcement point of view; impact Industry, Civil Society, Government and ultimately the ordinary South African citizens.

**Keywords:** Cybercrime; Cybersecurity; Institutional Theory; National Cybersecurity, National Security

## 1. Introduction

Nation States around the globe, whether developed or developing, are faced with an equal challenge of how to protect themselves and their citizens against ongoing cyber-attacks. Although these happened several years ago; attacks such as those which disrupted on-line banking in Estonia and defaced government websites in Georgia, as well as the infamous Stuxnet worm that temporarily shut down Iran's nuclear programme, are vivid examples of what may be possible within this new strategic domain (Betz D.J & Stevens T , 2011).

In October 2009, the United States of America established the Cyber Command on the basis that their current capabilities to operate in cyberspace have outpaced the development of policy, law and precedent to guide and control their operations in cyberspace. Just over six

years later, and following approval in 2012 of the National Cybersecurity Policy Framework by Cabinet of the South African Government; South Africa released for public comment the Cybercrimes and Cybersecurity Bill in June 2015. Chapter 6 of the Bill outlines institutional arrangements on how South Africa would position itself to deal with the cybercrime and cybersecurity challenges facing the country.

Our aim in this paper is to analyse the possible impact of the Cybercrimes and Cybersecurity Bill on the institutions charged with the responsibility to enforce it as outlined in chapter 6 of the Bill. The analysis is conducted using selected concepts from Institutional Theory. Assuming that the Bill has been passed and that all current fears and concerns from the various institutions and stakeholders have been addressed; we trust that our analysis will provide some insight on how from an institutional theoretic perspective, the bill will, at least from an enforcement point of view; impact Industry, Civil Society, Government and ultimately the ordinary South African citizens.

The paper is organised as follows: In the next section, we give a brief description of Institutional Theory together with a few concepts we use in our analysis borrowed from its repertoire. In sections 3, 4, 5 and 6 we list, briefly describe and analyse the relevant objects and functions of the respective *cyber centres* (cyber security centre, cybercrimes centre, cybersecurity Hub, cyber command, See Figure 1) as outlined in the bill; which for purposes of this paper are referred to as the *key institutions* (institutional arrangements).

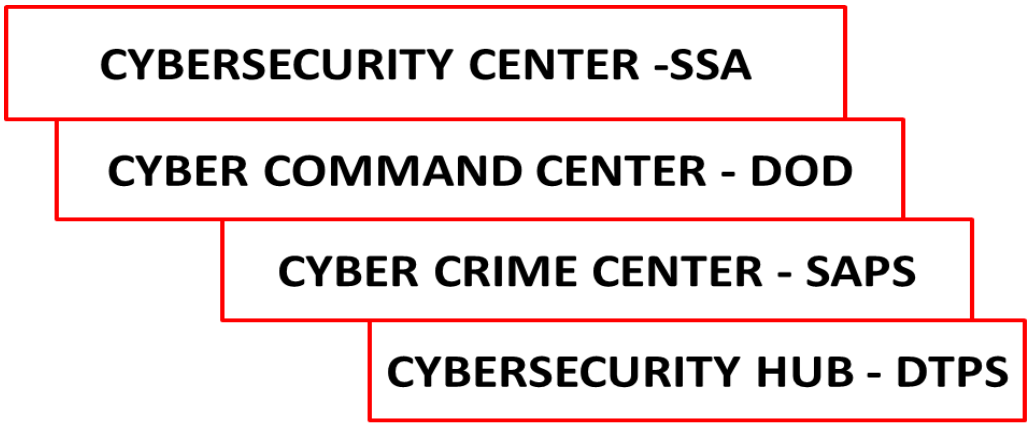


**Figure1**: The four key cyber centres outlined in the Bill

The impact of the bill on the institutions, stakeholders and the broader society drawn from the analysis are discussed in section 7. Lastly, conclusions are drawn in section 8.

## 2. Institutional Theory and selected concepts

With space limiting, we confine ourselves to (Madon et al, 2007) who pointed out that institutional theory has developed over a long period of time, and offers a wide range of concepts and approaches to analyse institutional persistence and institutional change. They indicate further that the potential value of institutional theory in the Information Systems (IS) field has been recognised for some time, pointing out that a number of authors have applied institutional theory with a focus on IS in developing countries, reflecting an interest in the relationship between ICTs and the institutional contexts in which they are embedded. We align ourselves with Madon et al (op cit.) and likewise locate our paper within this genre, drawing on selected elements from institutional theory in order to analyse the functional

attributes assigned to each cyber centre. Similarly we build on the following definition of institutions from one of its principle theorists:

'Institutions are multi-faceted, durable social structures, made up of symbolic elements, social activities, and material resources (Scott R.W, 2001)

Drawing from this definition, we wish to analyse the different interpretations by the various institutions and stakeholders which we have become aware of through our interactions with them, to assess how the process of institutionalising some of these objects and functions would impact these institutions through *symbolic acceptance by the community*; *stimulating viable social activities, enrolling public-private partnerships* and the *resources impact on the institutions*.

We turn now to the objects and functions of our four institutions, each of which we analyse through the theoretical perspective introduced here. The objects and functions items associate with each centre (institution) found relevant for analysis through the institutional theory lens are in *italics* in the description lists

## 3. Cyber Security Centre

### 3.1 Description

Looking at the ten (10) objects and functions of the Cyber Security Centre through the four Institutional Theory lens, only three (3) are clearly visible and are thus analysed in section 3.2. These are:

(*c*) *facilitate the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange on national security and threats in order to improve technical response coordination;*
*(g) develop response protocols in order to guide coordinated responses to cyber security incidents and interaction with the various stakeholders;*
*(h) ensure the conducting of cyber security audits, assessments and readiness exercises and provide advice on the development of national response plans;*

### 3.2 Analysis

*Symbolic acceptance by the community*: response protocols developed by the Cyber Security Centre for other organs of state and established CSIRTs are relatively easy to conceptualise. Developing and obtaining symbolic acceptance by the broader communities outside government and corporate would need some innovative approaches (g) as communities may not even be aware that an incident in their locality may be requiring a coordinated response.

*Stimulating viable social activities*: analysis of cyber security incidents, trends, and vulnerabilities, information-sharing, technology exchange on national security and threats in order to improve technical response coordination could stimulate viable social activities (c). Information sharing platforms could be arranged at different corporate levels and society using specialised non-disclosure agreements

*Enrolling public-private partnerships (PPP)*: PPPs are easily envisaged to conduct cybersecurity audits, assessments and readiness exercises. To facilitate this and to avoid criminalising the work of researchers, those involved in research, development, capacity building and professional services must be enabled to develop, possess and use software and

hardware tools, access computers and networks etc. with the aim to understand, test and protect organisations and/or our national security. Some accreditation and or licensing mechanisms may need to be put in place to effect this.

*Resources impact on the institution*: the other 7 functions (a, b, d, e, f, i, j) suggest huge resource impact on the institution, both in human and material resources.

# 4. Cybersecurity Hub

## 4.1 Description

A look at the thirteen (13) objects and functions of the Cyber Security Hub as outlined in the bill through the four lenses make five (5) of them clearly visible. The five are the following and are analysed in section 4.2:

(*a*) *coordinate general cyber security activities in the private sector;*
*(b) inform Private Sector Security Incident Response Teams, electronic communications service providers, vendors and other persons or entities who may have an interest in cyber security, of cyber security developments;*
(*d) initiate cyber security awareness campaigns;*
(*f) encourage and facilitate the development of Private Sector Security Incident Response Teams;*
(*k*) *conduct cyber security audits, assessments and readiness exercises on request;*

## 4.2 Analysis

*Symbolic acceptance by the community*: symbolic acceptance by the community would be achieved when the hub initiates cyber security awareness campaigns (d); and when it coordinates general cyber security activities in the private sector (a). Although still in its infancy, the cybersecurity hub is in operation and its official opening represented symbolic acceptance by the community.

*Stimulating viable social activities*: cyber security awareness campaigns (b) as well as coordination of general cyber security activities in the private sector (a) will stimulate viable social activities. The hub is very well positioned to initiate cyber security campaigns and activities for both civil society and the private sector and thus stimulating viable social activities.

*Enrolling public-private partnerships*: By encouraging and facilitating development of Private Sector CSIRTs and informing them, electronic communications service providers, vendors and other persons or entities who may have an interest in cyber security, the cybersecurity hub would be enrolling PPPs. This will also be achieved when the hub conducts cyber security audits, assessments and readiness exercises on request.

*Resources impact on the institution*: The other 8 functions (c, e, g, h, i, j, l, m) suggest huge resources impact on the institution.

# 5. Cyber Crimes Centre

## 5.1 Description

Again subjecting the ten (10) objects and functions of the National Cybercrime Centre to the four Institutional Theory lens, five (5) are found to be visible and are analysed in section 5.2. These are:

(*c*) *facilitate the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange on law enforcement and threats in order to improve technical response coordination;*
(*f*) *develop response protocols in order to guide coordinated responses to cyber security incidents and interact with the various stakeholders;*
*(g) develop and maintain cross-border law enforcement cooperation in respect of cybercrime;*
*(h) promote, establish and maintain public-private cooperation in order to fight cybercrime;*
*(i) promote, establish and maintain international cooperation in order to fight cybercrime;* and

### 5.2 Analysis

*Symbolic acceptance by the community*: Symbolic acceptance by the community will follow when the cybercrime centre develop response protocols in order to guide coordinated responses to cybersecurity incidents and interact with the various stakeholders (f). Unlike conventional crime incidents, cybercrime incidents may happen all at once in one location, making it almost impossible for the community to report observed incidents to the police and thus difficult to build the acceptable symbolism between the police service and the community.

*Stimulating viable social activities:* the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange on law enforcement and threats in order to improve technical response coordination will stimulate viable social activities (c).

*Enrolling public-private partnerships:* to promote, establish and maintain international cooperation in order to fight cybercrime (i) as well as to develop and maintain cross-border law enforcement cooperation in respect of cybercrime requires enrolment of effective PPPs (g). Again, to facilitate this and to avoid criminalising the work of researchers, those involved in research, development, capacity building and professional services must be enabled to develop, possess and use software and hardware tools, access computers and networks etc with the aim to understand, test and protect organisations and/or our national security.

*Resources impact on the institutions:* The other 5 functions (a, b, d, e, j) suggest high impact on resources for the institution.

## 6. Cyber Command

### 6.1 Description

Similarly and lastly, subjecting the eight (8) objects and functions of the Cyber Command to the four Institutional Theory lenses, four (4) are visible and are analysed in section 6.2. They are the following:

(a*) facilitate the operational coordination of cyber security incident response activities regarding national defence;*
*(b) develop measures to deal with cyber security matters impacting on national defence;*
*(c) facilitate the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange and threats on national defence in*

*order to improve technical response coordination;*
(f*) ensure the conducting of cyber security audits, assessments and readiness exercises and provide advice on the development of national response plans in so far as they relate to national defence;*

### 6.2 Analysis

*Symbolic acceptance by the community*: symbolic acceptance by the defence community would be achieved through operational coordination of cyber security incident response activities regarding national defence (a) as well as development of measures to deal with cyber security matters impacting on national defence (b)

*Stimulating viable social activities:* the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange and threats on national defence in order to improve technical response coordination (c) as well as development of measures to deal with cyber security matters impacting on national defence (b) would stimulate viable social activities within the defence community

*Enrolling public-private partnerships:* the conduct of cyber security audits, assessments and readiness exercises and provision of advice on the development of national response plans in so far as they relate to national defence (f) requires enrolment of appropriate technical PPPs. Similarly, to facilitate this and to avoid criminalising the work of researchers, those involved in research, development, capacity building and professional services to support the department of defence must be enabled to develop, possess and use software and hardware tools, access computers and networks etc with the aim to understand, test and protect organisations and/or our national security. Acceptable levels of security classification would need to be put in place to enable the required R&D work.

*Resources impact on the institutions:* The other 4 functions (d, e, g, h) suggest high impact on the resources of the institution

## 7. Discussion

Taken together, the Institutional Theory analysis le could be summarised as follows:

*Symbolic acceptance by the community*: development of response protocols in order to guide coordinated responses to cybersecurity incidents and interact with the various stakeholders. Unlike conventional crime incidents, cybercrime incidents may happen all at once in one location, making it almost impossible for the community to report observed incidents to the police and thus difficult to build the acceptable symbolism between the police service and the community. The cybersecurity hub is in operation and its official opening represented symbolic acceptance by the community.

*Stimulating viable social activities:* analysis of cyber security incidents, trends, and vulnerabilities, information-sharing, technology exchange on national security and threats in order to improve technical response coordination could stimulate viable social activities. Information sharing platforms could be arranged at different corporate levels and society using specialised non-disclosure agreements

*Enrolling public-private partnerships:* PPPs are easily envisaged to conduct cybersecurity audits, assessments and readiness exercises. To facilitate this and to avoid criminalising the work of researchers, those involved in research, development, capacity building and professional services must be enabled to develop, possess and use software and hardware tools, access computers and networks etc. with the aim to understand, test and

protect organisations and our national security. Some accreditation and or licensing mechanisms may need to be put in place to effect this.

*Resources impact on the institutions:* It is very clear that there are huge resources impact, both human and financial, on all four institutions charged with the responsibility of enforcing the bill.

## 8. Conclusions

It is our conclusion that the use of the four concepts borrowed from Institutional Theory enabled us to gain some insight on the implications the bill has on the institutions charged with the responsibility of enforcing it.

Out of a total of 41 objects and functions assigned to the four centres (10 cyber security centre, 13 cybersecurity hub, 10 cybercrime centre, 8 cyber command), the analysis assisted us in gaining some insight on a total of 17 of them. For the 24, our conclusion is that they will have much higher resource impact

What this indicates is that analyses such as these, borrowed from the social sciences are needed to give us some insight in dealing with the challenges we face in the cyber domain.

## 9. References

Betz D.J, Stevens T. (2011). Cyberspace and the State: Towards a Strategy for Cyber-power. London: Routledge.

Draft Cyber Crimes and Cybersecurity Bill. 2015.

Madon, S., Reinhard, N., Roode, D., Walsham, G. (2007). Proceedings of the 9th International Conference on Social Implications of Computers in Developing Countries, São Paulo, Brazil, May 2007

Scott, R.W. (2001), Institutions and Organizations, (2nd edition), Sage, London.