5-2018

Evaluating Factors Contributing to Misalignment of the South African National Cybeersecurity Policy Framework

Joel Chigada
University of Cape Town, chigadajm@gmail.com

Michael Eddie Kyobe Prof.
University of Cape Town, Michael.Kyobe@uct.ac.za

EVALUATING FACTORS CONTRIBUTING TO MISALIGNMENT OF THE SOUTH AFRICAN NATIONAL CYBEERSECURITY POLICY FRAMEWORK

Joel Chigada
University of Cape Town
chigadajm@gmail.com

Michael Kyobe
University of Cape Town
michael.kyobe@uct.ac.za

Abstract:

This paper evaluates factors contributing to misalignment of the South African National Cybersecurity Framework (SA-NCPF) and suggest better ways to align the national policy framework to national, regional and global cyberlaws. The SA-NCPF is designed to mitigate, address and provide the regulatory guidelines relating to escalating cybercrimes, however, the complexity and interplays of factors contributing to misalignment make it difficult to achieve and measure alignment of national cyberlaws. The SA-NCPF recognises the complexities, inconsistencies, fragmentation and poor coordination of e-legislation, thus, it is imperative to recommend the removal of hindrances. By reviewing various literature, we were able to discuss and integrate a number of theoretical works that explain inconsistencies/misalignments in law. We synthesised literature to produce an integrated theoretical framework, which is a major innovation of this study. The integrated theoretical framework provides a broader perspective of the influencing factors and their interplay resulting in complex relationships which are difficult to understand. The researchers used the integrative theoretical framework and the configuration approach to develop a conceptual model. This model guides the measurement of the extent of alignment of the influencing factors and the identification of that combinations of these factors that yields an effective Cybersecurity Policy Framework. The conceptual model will be validated in a later study.

Keywords:

Alignment, Configuration Theory, Cybercrime, Cybersecurity, Conceptual Model, Integrative Theoretical Framework, Law-Making Process, South Africa

1. Introduction

Information Communication Technology (ICT) applications, such as e-government, e-commerce, e-education, e-health and e-environment are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas (ITU, 2012). In addition, ICT applications can facilitate the achievement of millennium development targets, reducing poverty and improving health and environmental conditions in developing countries. However, the growth of the information society is accompanied by new and serious cyber-attacks and threats. The recent surge in the cyberattacks on critical public and private sector technology infrastructures and services in different parts of the world has made cybersecurity an important policy issue for many governments. The scourge of cyber-attacks and threats has created a challenge for many governments on how to provide the necessary legal and regulatory framework and instruments to protect citizen rights from threats posed by pervasive use of digital technologies in society.

Deterring cybercrime is an integral component of a national cybersecurity and critical information infrastructure protection strategy. In particular, this includes the development and adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes

and activities intended to affect the integrity of national critical infrastructures (Tembo, 2013). The researchers argue that at national level, development of an information infrastructure protection strategy is a shared responsibility that requires coordinated action related to prevention, response and recovery from cyber-attacks and threats on the part of civil society, government authorities and private sector. At the regional and international level, this entails cooperation and coordination with relevant partners (ITU, 2012:10). The formulation and implementation of a national cybersecurity policy framework requires a comprehensive approach which can only be addressed through a coherent strategy that takes into account the role of different stakeholders and existing initiatives within a framework of international cooperation (ITU, 2012). The development of adequate legislation and within this approach, the development of a cyber-crime-related legal framework is an essential part of South Africa's cybersecurity strategy. In order to address cybercrimes, a host of e-legislation has been developed and implemented in South Africa. However, research illustrates that civil society, public and private sector organisations do not understand and fail to interpret these laws resulting in failure to comply with them (Pokwana & Kyobe, 2016:1). The various pieces of e-legislation are also fraught with inconsistencies, fragmentation, information asymmetries and poorly coordinated by different government agencies with overlapping mandates resulting in misalignment to national and global cyberlaw standards (Mahlobo, 2015).

A thorough analysis of current national laws is vital to identify any possible gaps and if the substantive criminal law provisions criminalise all cyber-related crimes. We state that substantive criminal law provisions alone are not adequate to criminalise cybercrimes, law-enforcement agencies need necessary tools and instruments to investigate and prosecute cybercrimes. The existing mutual legal agreements in South Africa, are based on formal, complex, time-consuming procedures and difficult to understand resulting in misalignment and non-compliance with e-legislation (Kyobe, 2010). The South African government acknowledges these challenges and calls have been made to civil society, public and private sector organisations to work closely together to improve alignment of e-legislation, whilst removing any obstacles in e-legislation development processes, at national, regional and international levels (Mahlobo, 2015). In order to understand the concept of alignment, we review literature to identify inconsistencies, fragmentation and misalignment of national cyberlaws. An integrated conceptual framework will be developed and proposed to guide alignment of e-legislation in South Africa. We discuss the interplays of constructs in the proposed alignment framework through the configuration theory lens. We will use the configuration theory to identify and tease out combinations/patterns of constructs that would ensure appropriate alignment of national cybersecurity policy framework.

2. Literature Review

The alarming escalation rate of cybercrimes has culminated in the development of the SA-NCPF, whose strategic goals are aimed at addressing illegal computer related activities.

2.1 Cybercrime

Warren (2012) defines cybercrime as illegal computer-mediated activities designed to access information, data or cause damage to information systems. The Council of Europe Convention on Cybercrime (2012) states that cybercrime entails all offences against the confidentiality, integrity and availability of computer data and systems. Criminals illegally access, retrieve, steal and misuse that data and information for their gains. Marco (2009) posits that cybercrime entail all criminal acts involving elements of information, data and ICTs. Colangelo (2016:2) states that escalation of cybercrimes is attributable to lack of understanding of cybercrime;

fragmentation of cyberlaws and information asymmetries. However, cybercrime and cybersecurity are inseparable issues in an interconnected environment.

2.2 Cybersecurity

The International Telecommunication Union (ITU) (2012) states that enhancing cybersecurity and protecting critical information infrastructures are essential to a country's security and economic well-being. Orji (2012) states that the word "cybersecurity" is a culmination of the prefix "cyber" and the concept "security". Cybersecurity entails the multi-disciplinary aspect of legal, regulatory, technological and non-technological mechanisms put in place to mitigate, combat, minimise and protect cyber-attacks and threats. Oltramari, Cranor, Walls and McDaniel (2015) report that there has been more than half a billion security breaches in the first semester of 2014, an indication that cyber criminals continue to wreak havoc and instil fear in cyberspace.

2.3 South Africa Cybersecurity Regulatory Environment

The South African Parliament has enacted various pieces of e-legislation designed to address cybercrime and other computer-related illegal activities. The Constitution of the Republic of South Africa, 1996, is the supreme law of the country that informs all other forms of legislation which should conform to the entrenched norms (Classen, Cupido, Etsebeth, Klopper, Van der Walt, Ncube, Nel, Papadopoulos, Snail, Taylor & Watney, 2012). The Parliament of South Africa passes national reform policies into law or Acts, while the National Council of Provinces (NCOP) is responsible for ensuring that provincial legislative issues are taken into account in the national sphere of government, but both legal bodies are expected to bring various legal systems to work together towards a unity of purpose.

2.3.1 Electronic Law

The legislation regulating the use of ICT in South Africa includes: **Common Law:** which is law that exists and applied to a group of people on the basis of customs and legal precedents developed a period of time (Classen et al., 2012). Common law is used to cater for the arrest and successful prosecution of online offenders committing online crimes such as cyber-smearing, child pornography, defamation, defeating ends of justice, contempt of court, theft or cyber-fraud (Hannah, 2015). **The Electronic Communications & Transactions Act (ECTA) (2002).** The ECTA gives legal recognition to electronic transactions whilst preventing the abuse of information systems (Classen et al, 2012 and Orji, 2012). All cybercrimes are addressed in Chapter XIII of the ECTA, 2002. Other Regulatory Mechanisms (Cyber Inspectors or Cyber Police) are established through Chapter XIII of the ECTA, 2002 to carry-out functions of the Cyber Inspection.

The **Interception and Monitoring Prohibition Act (IMPA) 77** of 1995 highlights that it is a criminal offence for any person to intentionally intercept, authorise or procure other people's communication without their knowledge and approval. (Snail, 2009). **Financial Intelligence Centre Act (FICA)** compels financial institutions to obtain proof of identity, proof of residence which is less than 3 months old issued by a reputable authority. FICA provides that institutions should access original documents and make copies which are certified as a true copy of the original with a FICA endorsement. Chapter 4, principle 5.7) of **King Code IV** addresses IT governance issues where the board is required to operate, report IT security and policy issues within the auspices of Corporate Governance (Control Objectives for Information and Related Technology) [COBIT] 4.1 and audit committees. **SA National Cybersecurity Policy Framework** was designed to promote the establishment of the National Cybersecurity Advisory Council (NCAC) which oversees the implementation of national cybersecurity

strategies and National Computer Security Incident Response Team (CSRIT). These pieces of legislation focus on different aspects of cybersecurity, resulting in inconsistencies and complex legal environment. In addition, the jurisdiction of each of these laws rests with different agencies creating legal incoherence. In order to understand the causes of inconsistencies and incoherencies of legislation, a discussion of the law-making process in South Africa suffices.

3. Law-Making Process in South Africa

The Parliament of South Africa is the national legislature (law-making body), whose major functions are to pass new laws, amend existing laws and repeal or abolish (cancel) old laws (Classen et al., 2012). The law-making process in South Africa is similar to the United States of America (US) and United Kingdom (UK) processes (Selebalo, 2014) The US Congress which is an equivalent of the Parliament of South Africa, makes federal laws. Its two legislative bodies- US Senate and House of Representatives) present Bills for public reviews and debates (Sullivan, 2010). In the UK, two legislative bodies- House of Commons and House of Lords develop and present Bills to Parliament (Telegraph, 2014). The law-making processes in all three countries (South Africa, United States of America and United Kingdom) follow the steps illustrated in Figure 1. The steps are: ***1)*** Introduction of the Bill in the National Assembly (NA) or National Council of Provinces (NCOPs). The National Council of Provinces (NCOP) is responsible for ensuring that provincial legislative issues are taken into account in the national sphere of government, but both legal bodies are expected to bring various legal systems to work together towards a unity of purpose (Classen et al., 2012***). 2)*** the Bill is referred to relevant Portfolio Committees and published in the government Gazette for public comments; ***3)*** Committees debate and amend the Bill; ***4)*** Bill submitted to a sitting House for further debates; ***5)*** Bill transmitted to the other house for concurrence; ***6)*** President of the republic assents the Bill; ***7)*** and the signed Bill becomes an Act of Parliament/law of the land (Parliament, 2017). We examine each step in more detail, where we identify areas of inconsistencies/misalignment and the theoretical works that explain these inconsistencies.

3.1 Introduction of Bill in the National Assembly or National Council of Provinces

Resource-based theory contends that possession of strategic resources provides an organisation with a golden opportunity to develop competitive advantage over its competitors (Barney, 1991). Mislaignment arises when an organisation's resources are not jointly exploited to achieve competitive advantage. In addition, the resources-based view (Penrose, 1959) explains that misalignment occurs if a country's IT and legal expertise and skills are scarce because these human resources help understand, interpret cybersecurity terminology and other concepts. For example, NCOPs cannot work without national frameworks that act as standards for alignment, therefore, IT and legal expertise and skills are required. Provincial leadership that makes laws without national standards, results in misalignment and inconsistencies (Selebalo, 2014). Most provincial governments have very little understanding of their law-making powers and responsibilities are, resulting in an array of inconsistences. Inequitable distribution and use of resources also creates conflicts between agencies resulting in confusion between systems elements in the law-making process (Lorenz, 1961). Misalignment also arises if a country's political decsions are not fairly and reasonably debated amongst citizens (Eagan, 2007). Political theory (Eagan, 2007) explains the nature, authority, structure and relationship of the state and its environment. The interactions of different elements should be in harmony to achieve alignment (Lorenz, 1961).

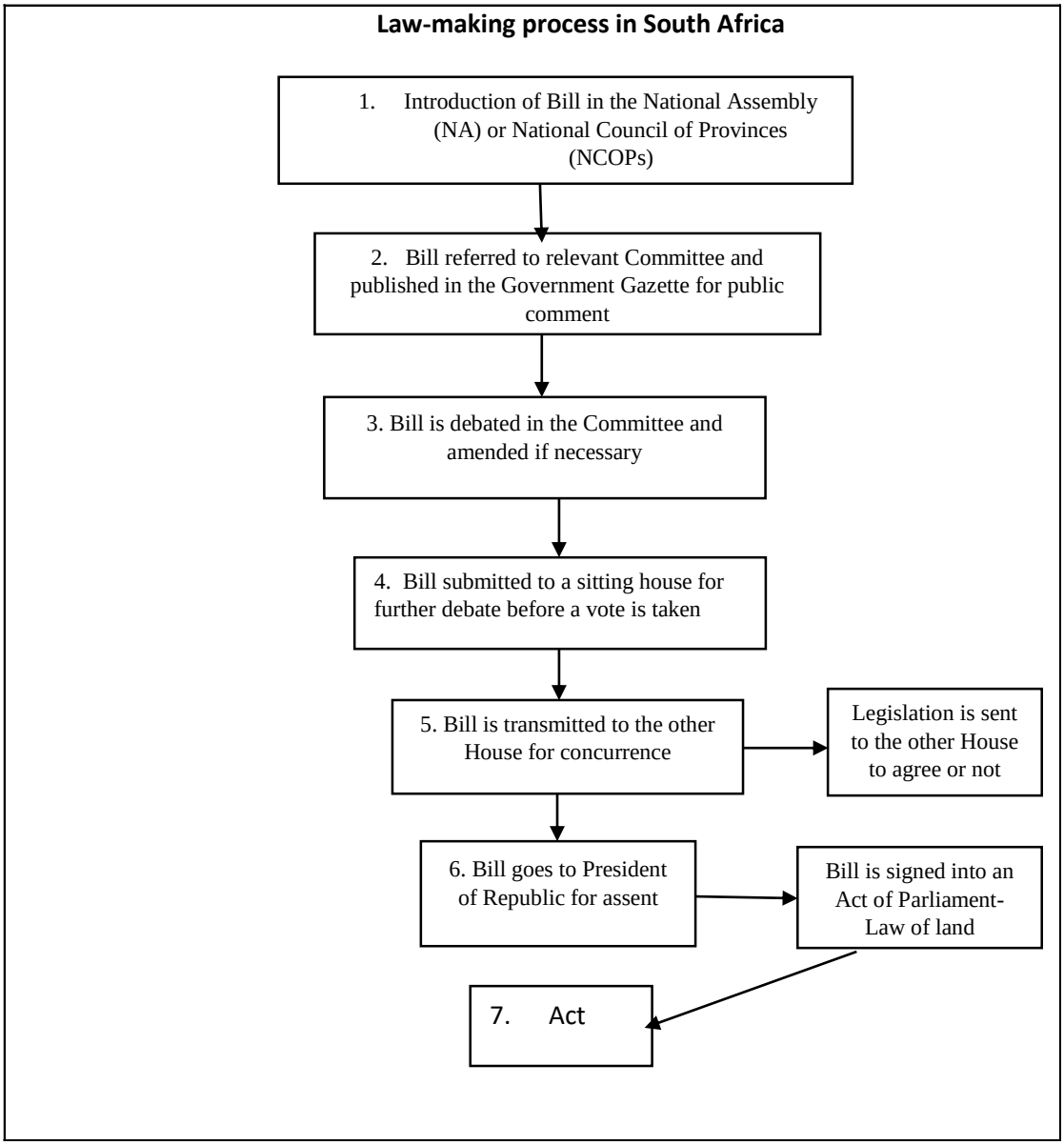

Figure 1: Law-making Process in South Africa (www.parliament.gov.za)

3.2 Bill referred to relevant Portfolio Committees

In this paper, the organisational knowledge conversion theory helps us to understand how Portfolio Committees, civil society and other stakeholders share and convert information to create new knowledge during debates on Bills (Nonaka & Takeuchi, 1995). During the interactions between Portfolio Committees conflicts and disagreements are highly likely to occur resulting in considerable time and resources spent on wrong things. Social conflict theorists (Marx, 1871) posit that conflicts arise as a result of social inequality and existence of bad relations between dorminant groups versus minority groups. The interactions between NCOPs, NA, public and other government agencies create collaborative platforms where organisational knowledge is created. However, we observed that, communities' limited access to media, impacts negatively to access Parliament related information, thus the law making process excludes other members of society whose contribution may be invaluable (Selebalo, 2014). With reference to the deliberative democracy school of thought in political theory, exclusion of civil society from the law-making process, is viewed as unfair and unreasonable,

therefore, it creates conflicts and inconsistencies (Eagan, 2007). Due to poorly advertised Parliamentary events such as public hearings, the public will not have sufficient time to participate and debate Bills resulting in low organisational knowledge conversion rate (Selebalo, 2014). Organisational knowledge conversion theorists (Nonaka, 1986; Nonaka & Takeuchi, 1995) posit that if there are shorter window periods of time to give the public opportunities to make submissions, this is viewed as a deliberate strategy to exclude the public from participating in the law-making process. The exclusion or little input from civil society hinders information and knowledge sharing regarding new Bills (Selebalo, 2014).

3.3 Bill is debated in Committees and Amended

The resources-based theory explains that the Parliament is a representation of an organisation with a set of resources that should be utilised to produce new legislation (Penrose, 1959). Optimally exploited resources require human coordination to yield the desired results. We noted that processes in steps one, two and three have repetitions, resulting in time-wasting, lack of harmonisation and hindrance of the pace of implementation of law (Isasi, 2009), which is supported by chaos theorists who assert confusion arises if there is an apparent lack of order in a system (Lorenz, 1961). In its general term, chaos theory refers to an apparent lack of order in a system because systems rely upon an underlying order and any system and events can cause very complex behaviours to happen (Lorenz, 1961). Misalignment arises through poor coordination, repetition and lack of order in the three steps. If processes are properly coordinated, existence of multiple agencies is eliminated, the cooperation of legislation across jurisdictions and portfolio committees would enhance alignment of laws (Weber, 2014). With frayed, pixilated and existence of incoherent laws, the cyberspace environment is a complex system which makes it difficult for the global village to conceive global laws (Weber, 2014; Colangelo, 2016).

3.4 Bill is submitted to the House for further debate

Chaos theory literature (Lorenz, 1961) contends that chaos arises if there is lack of order and or confusion exists. In this paper, chaos will arise because of a repetitive step four where the Bill if submitted to the House for further debates. The absence of a logical flow in the law-making process between the first and fourth step stifles coherence resulting in a complex law-making process which is misaligned The existence of this system appears to be exhibiting ‘disorder, irregularities and unpredictability’ and cannot be understood scientifically, resulting in inconsistencies (Anderson, 1999; Jackson, 2003). Chaos will arise because of the involvement of many departments, Potfolio Committes and further debates, resulting in interactions and conlficts (Marx, 1871) or disgareements regarding the Bills. The behaviour of a complex system is never linear, therefore, the various interactions and debates occurring during this step, might result in the loss of the original theme of the Bill-resulting in misalignment or rejection of the Bill.

3.5 Bill is transmitted to the other House for Concurrence

Chaos and social conflict theories explain the likelihood of disagreements and conflicts arising when the Bill is referred to the other House for Concurrence(Marx, 187; Lorenz, 1961). If the Bill is not agreed upon, disagreements will arise. The dorminant House (wielding more power) will subdue the viewpoints of the other House (Eagan, 2007). We posit that where Committees are involved, the probability of conflicts arising is very high (Marx, 1871), resulting in confusion or lack of harmony (Lorenz, 1961). Differing viewpoints, one group dorminating the discussions, lack of resources, overlapping roles and responsibilities and diversity can cause rifts and conflicts amongst Portfolio Committee members. We posit that Portofolio Committee members should embrace diversity and work as unity to achieve the desired objectives of

developing legislation. Harmony is not about uniformity rather it entails diversity, but when elements are in harmony, even though their individual attributes remain, they form a completely fresh feature (Isasi, 2009).

3.6 President of the Republic Signs the Bill into an Act

Deliberative democracy school of thought in political theory contends that the enforcement of a legal code by authority illustrates the legitimacy of an Act (Eagan, 2007). The President of the Republic is empowered by the Constitution of South Africa to sign Bills into Acts of Parliament. Literature suggests that the exercise of power is accepted as endemic to human beings as social beings (Wilson, 1999). By signing or rejecting to sign the Bill into law, the President would be exercising legitimate power. We also posit that the President is not a human being who knows it all, therefore, he has to learn and consult legal expertise regarding each Bill which is in line with the assertions of Social Learning Theorists who posit that that learning is a cognitive process that takes place in a social context (Bandura, 1971). Failure to learn and or understand the Bill, harphazard decision-making might be unfavourable and unfair to all citizens (Eagan, 2007). The President has the prerogative to seek legal opinion and advise to gain an understanding as well as acquisition of knowledge of the Bill (Bandura, 1971). The President's actions will inform and determine the future of the country's laws (Colangelo, 2016) which is aptly explained by structuration theory that fosters informing the public about how to act, based around rules which are about the right and wrong way to do things (Giddens, 1984). Laws passed without consultations and involvement of all staekholders, will not address what they are designed to do, therefore, a disjoint/misalignment arises (Giddens, 1984).

3.7 Act

The configurations theory (Miller, 1986: Venkatraman, 1989) explain the importance of various constructs interacting with each over a sustained period of time achieving a strategic fit. As shown in Figure 1, the law-making process is a complex system formed by diverse steps, agencies, people and departments whose diverse viewpoints potentially cause chaos and conflicts. A system that lacks order creates challenges for teams working on development of legislation (Lorenz, 1961). The resource-based theory (Penrose, 1959) and Giddens' (1984) structuration theory help us explain that the Act/Law of the Land comes into being as a result of interactions between different constructs, optimum utilisation of resources and relationships between individuals and society.

With reference to analysis of literature on cybercrime, cybersecurity and the law-making process we have idenitified some gaps which should be addressed . The gaps are shown in Table 1 below.

Table 1 Gaps Identified in Literature

Author/study	Cumberso me law-making	Lack of IT capacity and	Slow pace of	Lack of collaborati	Fast-paced technologi cal	Multiplicit y of agencies &	Cybersecur ity IT &	Cybersecur ity culture	Framewor k of internation
ITU (2012)	X	X	X				X		
ITU (2012)	X	X	X		X		X		
Canhoto (2010);	X	X	X			X	X	X	

Mahlobo (2015)									
Classen et al. (2012); Chigada (2014)		X		X		X			
Selebalo, (2014);De (2016)			X		X	X	X		
Classen et al (2012); Mahlobo (2015)						X	X	X	
Selebalo (2014);JCSE (2016)		X			X		X		

* X represents what has been covered in the study

4. Integrative Theoretical Framework, Alignment, Conceptual Model and Propositions

Having discussed the stages in the law making process, the inconsistencies/misalignment and the theories explaining them, an integrative theoretical framework (see Figure 2) has been developed. The law-making process model illustrated in Figure 1, was used as a template to develop the integrative theoretical framework. The South African law-making process model (www.parliament.gov.za) shown in Figure 1, was modified to include information and knowledge sharing; multiple agencies and systems; legal and IT expertise and control variables to reflect an integrative theoretical framework (Figure 2). Each of the theories discussed looks at certain components of alignment, may overlap and complement each other in some cases. The variables in the integrated theoretical framework interplay and influence each other over a sustained period of time (Venkatraman, 1989). The factors identified by the theories interplay and result incomplex relationships. While the **structuration theory** (Giddens', 1979 & 1984) focuses on the relationships between individuals and society (Jones & Karsten, 2008:129). The law-making process is a responsibility of everyone in South Africa, therefore the relationships between public, private sector organisations, civil society and Parliament are paramount. The purpose of the developed integrative theoretical framework is to bring together the gaps in the theoretical work and literature into one comprehensive framework that explains all the potential factors.

The structuration theory states that social structures are socially constructed by social agents who determine social properties on human institutions (Giddens (1984). Particular behaviour on interaction of social agents, knowledge is created **(Organisational knowledge conversion theory**) about possible interventions that may be applied to limit inhibiting behaviour and facilitate creative behaviour. Literature suggests that structuration theory entails rules and resources organised as properties of social systems (Giddens, 1984). Therefore, the existence of structuration theory is complemented by the **resource-based theory(RBV)** (Penrose, 1959) which looks at an organisation as a set of broader resources that should be utilised to produce products and services.

The **organisation knowledge conversion (OKC) theory** overalps and complements the RBV by looking at information and knowledge sharing as resources that arise out of interactions occurs during interactions between agencies, civil society, Portofolio Committees and legislative bodies. These theories are complemented by **chaos theory** which refers to an apparent lack of order in a system because systems rely upon an underlying order and any system and events can cause very complex behaviours to happen (Lorenz, 1961). Whereas, **complexity theory** (Kauffman, 1969) looks at the behaviour of large and complex systems that might be lacking order. Disparate constructs of a system are expected to work together to shape the system and its outcomes (Kauffman, 1969). Legitimate **political power** and authority should exercise fairness and reasonableness during the decision-making process (Eagan, 2007) for all citizens. All these theories help us explain that the Parliament of South Africa represents an organisation with sets of human, financial, information, information technologies, knowledge, multiple government agencies and time resources which should be jointly and optimally exploited to produce new legislation (Penrose, 1959). With reference to the complex relationships built through the interplay of different constructs explained in the integrated theoretical framework, we propose a conceptual model that helps us to understand the concept of alignment. The proposed conceptual model is guided by two things- an integrative theoretical framework (which broadly covers the influencing factors) and the interplay between the influencing factors, therefore, we need to bring them into alignment.

4.1 Alignment of Legislation

Most studies conducted to date, focus on compliance or non-compliance of legislation. The few studies focusing on misalignment reveal that there are three representations of misalignment in legislation namely: lack of Coherence; Interoperability and Harmonization (Lipton, 2010; Pokwana & Kyobe, 2016). Hsiao and Omrod (1998) define alignment as the synergy and coherence between various components in an organisational system to achieve competitive advantage. Whereas, Maes, Rijsenbrij, Truijens and Goedvolk (2000) define alignment as "a continuous conscious and coherent interrelation between all organisation components, human resources and IT to achieve specific objectives over time". We posit that the interplays among various constructs must be balanced over a sustained period of time to achieve an effective system (Maes et al., 2000). Strategic business continue to use the concept of alignment to develop solutions to various complex organisational challenges (Portee & Siggelkow, 2008). There are six perspectives that explain alignment (Venkatraman, 1989) and these are: (1) **Fit as Moderation** is premised on the relationship between two variables which predict an outcome (Venkatraman, 1989). In moderation terms, the interaction between the predictor and criterion variables depends on the third variable (moderator). (2) **Fit as Mediation** has some similarity to fit as moderation. Venkatraman (1989) asserts that fit as mediation concerns the relationship between two variables (antecedent and consequent variables) by which there exist a third variable (mediator variable) which produces an intervening effect on both variables. (3) **Fit as Matching** is different from fit as mediation and moderation because it does not involve a reference criterion. Fit as matching is defined as a match between two related variables (Venkatraman, 1989). Therefore; the effect of fit between two variables can be estimated.

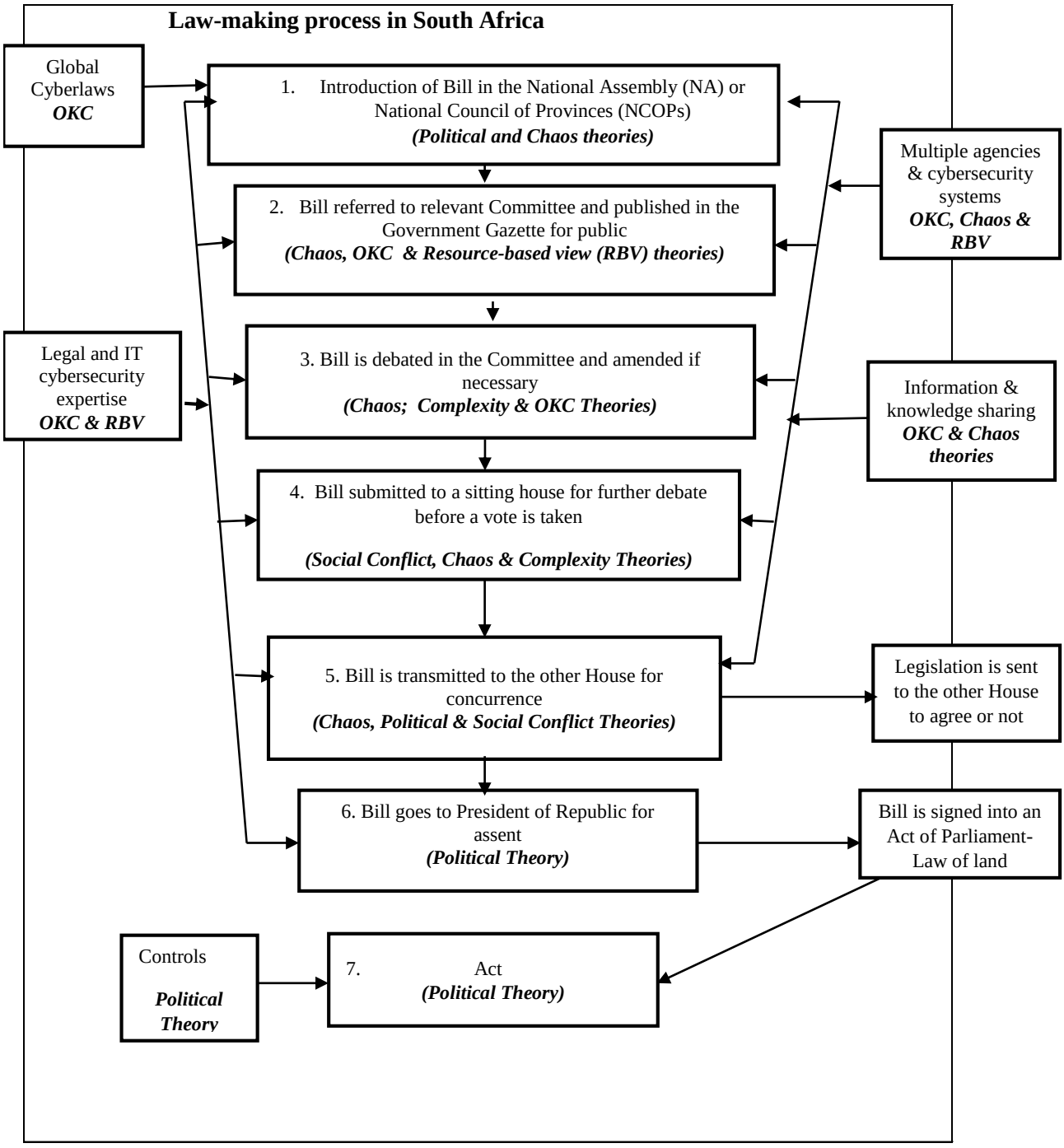

Figure 2: Integrated Theoretical Framework (Parliament, 2017; Chigada, 2017)

The fourth perspective: **Fit as Profile Deviation** entails the degree of adherence to external factors (Venkatraman and Prescott, 1990). Thus, profile deviation is the degree of adherence to the external profile. For instance, a firm's strategy may be specified for a particular environment. Deviations occur when the ideal profile is not achieved, resulting in lower performance. (5) **Fit as Co-variation** is modelled using factor analysis. Alignment can be viewed as a pattern of internal consistency among a set of variables related to a common objective (Venkatraman, 1989). (6) **Fit as Gestalts/Configuration Theory**: Venkatraman

(1989) defines Gestalts as configurations or patterns of organisational elements, constructs or variables that have attained adequate level of coherence, fit or unity with one another over a sustained period of time. Ajumobi and Kyobe (2017) highlight and emphasise that when constructs interplay and interact and coherence is achieved, there is success/effectiveness. In their study, Ajumobi & Kyobe (2017) illustrate that the interplay among human competencies, mobile technology and business strategy achieved coherence, resulting in the attainmenet of optimum benefits and high perfoemence in small-to-medium businesses. Literature also suggests that where constructs are integrated/coherent (complement each other), there will be success or improved performance (Venkatraman, 1989; Van de Ven & Robert, 1985).

4.1.1 The Concept of Effectiveness

Drucker (1987) defines effectiveness as doing the right things, whereas Nyarko (2014) defines effectivess as the capability of producing the desired result. In this paper, the intended outcome is to produce a successful/aligned national cybersecurity policy framework. We do not know which combination/patterns of interactions produce this desired outcome, therefore, the configuration approach will help us identify and measure that pattern/combination of constrcuts that provides effectiveness (Miller, 1986; Venkatraman, 1989). If we identify these constructs, their combined influences and determine their degree of coherence, we should be able to tell how and when we can achieve/aligned the national cybersecurity policy framework (Ventaktraman, 1989). Coherent/aligned constructs help us to achieve a successful/effective national cybersecurity policy framework, attain optimum benefits and value from them as well as gain high performance. The various constructs would enable configurations to be fairly unique, tightly integrated and stable for a sustainable period of time (Ajumobi & Kyobe, 2017). With reference to the perspective of alignment (Gestalts), the adequate level of alignment will be determined using cluster analysis to reveal the patterns and configurations of variables as well as their level of effectiveness. Those constructs that have attained alignment will have high level of effectiveness (Van de Ven & Robert, 1985; Ajumobi & Kyobe, 2017), while, in unlikely scenarios, it would be inferred that constructs not achieving coherence, have not attained alignment.

4.2 Conceptual Model

The proposed conceptual model incorporates, the law-making process (see Figure 1), various theories that explain inconsistencies, gaps identified in literature (Table 1) and the integrative theroretical framework (Figure 2). The proposed conceptual model (Figure 3 below) will help us measure the degree of influence by teasing out the configurations between constructs. The constructs for the proposed conceptual model are: Law-making process; multiplicity of agencies & cybersecurity systems; Monitoring and Evaluation (Controls); Cybersecurity IT and legal expertise, Information and knowledge sharing; Pace of implementation of law; Cybersecurity Culture and global cyberlaws. The seven constructs converge/interact in the circle, creating complex and difficult to understand combinations. Each construct points to the circle (which represents a **combined influence** of activities), thus, configurations or patterns are expected to be tightly interdependent and their significance is best understood as a unity (Miller, 1986; Venkatraman, 1989). The circle represents a continuous interplay which is complex to understand from a human perspective. Given the complexity of interplay between the factors, it is impossible to achieve alignment using the linear approach if the matching, moderation, co-variation and mediation alignment perspectives are considered, therefore, the **configuration theory** helps us to tease out the combinations which would achieve alignment of the national cybersecurity policy framework (Ajumobi & Kyobe, 2017:7).

The various combinations arising from interplay (combined influence) are hidden inside the circle. Therefore, the circle illustrates the combined influence that is required to achieve an aligned regulatory policy framework. If we identify these factors, their **combined influences and determine the degree to which they are coherent/aligned**, we should be able to tell how and when we can achieve a better/aligned National Cybersecurity Policy Framework (Venkatraman, 1989). To determine the degree of alignment, cluster analysis will be used to reveal the patterns and configurations of the constructs in the SA-NCPF. The stronger the coherence among these elements, the greater would be the effectiveness of the national cybersecurity policy framework. If the degree of coherence is weak (elements are misaligned or not balanced), then the pieces of cyber legislation will be ineffective (Ajumobi & Kyobe, 2017). The proposed conceptual model is shown in Figure 3 below.

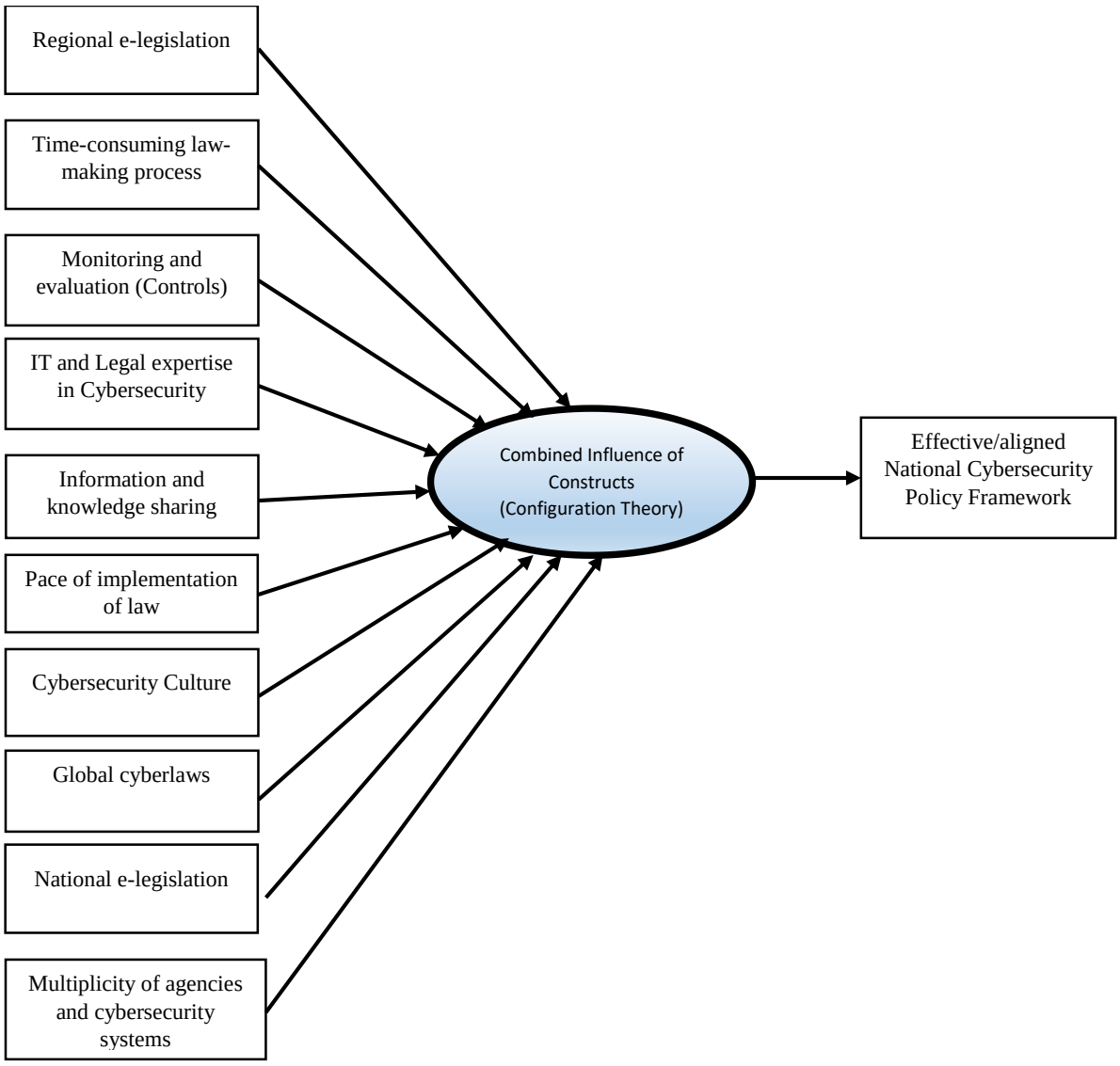

Figure 3: A configuration approach to alignment of National Cybersecurity Policy Framework (**Chigada, 2016)**

4.3 Propositions

The following research propositions were formulated based on the proposed conceptual model.
P1: The stronger the coherence among the seven constructs the more aligned is the national cybersecurity policy framework;

P2: The more coherent the national cybersecurity policy framework is perceived, the greater would be the degree of alignment of the SA-NCPF to national, regional and global cyberlaws.

P3: The more multiple agencies and information systems with overlapping mandates exist, the more complex it becomes to develop and implement aligned national e-legislation.

P4: Lack of IT and legal skills/expertise slows the law-making process and hinders the pace of implementation of legislation.

P5: The existence of multiple agencies and information systems depletes the already scarce IT and legal skills

P6: Sharing of information and knowledge between state agencies attributed to fear of exposing state secrets impacts development of a cybersecurity culture and information protection strategy.

P7: An apparent lack of a practical plan or strategy hinders the country from cultivating a cybersecurity culture which results in failure to implement critical policies adopted by the African Union Convention on Cybersecuirty and Data Protection.

P8: An agenda that forges public-priavte patnerships, education and traning should be encouraged at national level to create a cybersecurity culture.

5. Research Methodology

A positivist research paradigm informed by an objectivism ontological consideration, will be adopted in this study. The epistemological assumption is to separate the researchers from research participants. Data will be collected from randomly selected research participants working as Information Systems Managers, IT Managers, legal scholars, Cybersecurity legal experts, Policy makers, law makers (Members of Parliament) Software engineers, Information Communication (ICT) infrastructure, global cyberlaw experts and academics/researchers. Quantitative data will be collected from geographically dispersed research participants through the administration of questionnaires. Though, the majority of research participants will be from South Africa, data will also be collected from outside the borders of South Africa. The Configuration perspective will be adopted for data analysis and the interpretation of findings in order to understand and gain insights of the interplay between various constructs of the SA-NCPF.

6. Conclusion

In conclusion, this paper evaluated factors contributing to misalignment of legislation through the law-making process model shown in Figure 1. A critical analysis of literature revealed that cybercrimes are rising at alarming levels forcing many governments to devise intervention strategies such e-legislation. Various scholarship that was consulted, helped us to discuss the stages in the law making process, the inconsistencies/misalignment, gaps identified in literature and the theories explaining them resulting in the development of an integrative theoretical framework. Literature revealed that variables in the integrative theoretical framework interplay and influence each other over a sustained period of time resulting in the development of complex relationships which are difficult to understand from a human perspective. In addition, we synthesised literature to produce a conceptual model (Figure 3) which incorporates, the law-

making process, various theories that explain inconsistencies, gaps identified in literature and the integrative theroretical framework. The continuous interplay between constructs is complex to understand, therefore, we adopted a configuration theory to help us to identify these factors, tease out their combined influences and determine the degree to which they are coherent/aligned. We should be able to tell how and when we can achieve alignment.

References

Atoum, I., Otoom, A. & Ali, A.A. (2014). A holistic cybersecurity implementation framework, *Journal of Information Management & Computer Security*, 22 (3): 251-264.

Baker, W.H. (2010) Thoughts on Mapping and Measuring Cybercrime. Oxford Internet Institute Forum Mapping and Measuring Cybercrime,[Online] Available http://www.sfu.ca/~icrc/content/oxford.forum.cybercrime.pdf[10June 2016].

Campbell, D.T. & Fiske, D.W. (1959). Convergent and discriminant validation by the multi-trait multi-method matrix. *Psychological Bulletin*, 56: 81-105.

Canhoto, A. (2010) What' before 'How', Oxford Internet Institute Forum, [Online], Available: http://www.sfu.ca/~icrc/content/oxford.forum.cybercrime.pdf [24 May 2016].

Chigada, J.M. & Ngulube, P. (2015). *The role of knowledge management in enhancing organisational performance in selected banks of South Africa*. Published PhD Thesis. University of South Africa: Pretoria.

Chigada, J. (2016) Proposed Model for Alignment. PhD Thesis, University of Cape Town.

Classen, L., Cupido, C., Etsebeth, V., Klopper, H., Van der Walt, L.M., Ncube, C., Nel, S., Papadopoulos, S., Snail, S., Taylor, D. & Watney, M. (2012). Cyberlaw @ SAIII: The Law of the Internet in South Africa, 3rd Edition, Van Schaik Publishers, Pretoria.

.Colangelo, A.J. (2016). A Systems Theory of Fragmentation and Harmonisation, New York University *Journal of International Law and Politics (JILP)*, Forthcoming; SMU Dedman School of Law Legal Studies Research Paper No. 261. Available at SSRN: http://ssrn.com/abstract=2754402 [22 June, 2016].

Comizio, G.V., Dayanin, D. & Bain, L. (2015) Cybersecurity as a Global Concern in Need of Global Solutions: An Overview of Financial Regulatory Developments in 2015, *Journal of Investment Compliance,* 17 (1). Available on http://dx.doi.org/10.1108/JOIC-01-2016-0003 [6 May 2016].

Council of Europe Convention on Cybercrime: (2014). *Cybercrime Model Laws*, Strasbourg, France, 23 December 2014, [12 March 2016].

De, R. (2016). Cybersecurity Conference, Delaware University, State of Delaware, Washington DC, USA.

Department of Homeland Security (DHS), 2016). Cybersecurity Insurance. Washington DC, USA.

DeSmet, A., Veldeman, C., Poels, K., Bastiaensens, S., Van Cleemput, K., Vandebosch, H. & De Bourdeaudhuij, I (2014). Determinants of Self-reported Bystander Behavior in Cyberbullying Incidents amongst Adolescents. *Cyberpsychology, Behavior and Social Networking, 17*, 207-215.

Guba, E.G. & Lincoln, Y.S. (1989) Fourth Generation Evaluation. London: Sage Publications, CA.

Hannah, K. (2015). Cybercrime-Should we be hacking back? World Economic Forum, USA.

International Telecommunications Union (2012). Understanding Cybercrime: Phenomena, Challenges and Legal Responses, September 2012 Also available on www.itu.int/ITU-D/cyb/cybersecurity/legislation.html [Accessed 30 April 2016].

Kuhn, T.S. (1970). *The structure of scientific revolutions*. Chicago: University of Chicago.
Kyobe, M.E. (2010). Towards a framework to guide compliance with information systems Security policies and Regulations in a university, Institute of Electrical and Electronics Engineers; 1-7.
Kyobe, M.E. (2015). Towards a Framework for analysing impediments to cyberlaw Compliance in Africa, *Paper Proceedings of Second International Conference on Interdisciplinary Legal Studies 2015:* 55-60.
Leedy, P.D. and Omrod, J.E. 2010. *Practical research: planning and design*. 6th Edition, Upper Saddle River, N.J.: Pearson.
Maes, R., Rijsenbrij, D.,Truijens, O. & Goedvolk, H. (2000) Redefining business-IT alignment through a unified framework, Landelijk Architecture Congress, 2000 Amsterdam.
Marco, G. (2009). Understanding Cybercrime: A guide for Developing Countries, *International Telecommunications Union*. Geneva
Miller, D. (1991). Configurations of strategy and structure. *Strategic Management Journal*, 7, 233-250.
Miller, D. (1987). The Genesis of Configuration, *The Academy of Management Review*, 12 (4) 686-701.
Ncube, C.B. (2012). *Introduction to Electronic Transactions Law*, Department of Commercial Law, University of Cape Town. Cape Town.
Oltramari, A., Cranor, L.F., Walls, R.J. & McDaniel, P. (2015). Building an Ontology of Cybersecurity, Carnegie Mellon University, Pittsburgh, USA.
Orji, U.J. (2012). Cybersecurity Law and Regulation, Wolf Legal Publishers, the Netherlands.
Pokwana, U. & Kyobe, M.E. (2016) Investigating the Misalignment in the Existing E-Legislation of South Africa, Masters' Thesis, University of Cape Town, Cape Town.
Romm, N. & Ngulube, P. (2014). Mixed methods research. In Mathipa, E.R. and Gumbo, M.T. (eds). *Addressing research challenges: making headway for emerging researchers* (in press).
SABRIC (2015) Escalating Cybercrime: Banking clients' personal details accessed. (Online] http://www.sabric.co.za [2 June 2016].
Saunders, M., Lewis, P. and Thornhill, A. (2012). *Research methods for business students*, 4th Edition. Harlow: Prentice Hall.
Snail, S. (2009). Cybercrime in South Africa-Hacking, cracking and other unlawful online activities, *Journal of Information, Law and Technology*, http://go.warwick.ac.uk/jilt/2009_1/snail [22 June 2016].
South Africa Government Gazette, 4. (2015). The National Cybersecurity Policy Framework, 39475 of 2002. Pretoria.
Stangor, C. (2011). *Research Methods for the Behavioural Sciences* 4th Edition, Belmont:
Wadsworth, Cengage Learning. The Witwatersrand University Joburg Centre for Software Engineering (2016). The skills crisis. Johannesburg. South Africa.
United Nations Conference on Trade and Development [UNCTAD] (2009). Harmonising Cyberlaws and Regulations: The Experience of the East African Community. United Nations.
Van der Merwe, D. (2008). Criminal Law– Your partner in preventing information loss, Presented at the Lex Informatica, 23 May 2008 at the Innovation Hub.
Van Wyk, MM. (2012) Measuring Student's Attitudes to Economics Education: A Factorial analysis approach, *Journal Social Science,* 31 (1):1-42.

Venkatraman, N. (1989). The Concept of Fit in Strategy Research: Toward Verbal and Statistical Correspondence, *The Academy of Management Review* 14(3), 423-444.
Warren, B.C. (2012). Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore; 2-4.