UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

CYBERSECURITY POLICY AND LEGISLATION IN SOUTH AFRICA

By

Nandipha Ntsaluba
(Student No. 31416091)

Submitted in partial fulfilment of the requirements
for the degree of

Legis Legum Magister (LLM) in Intellectual Property

at the University of Pretoria

Prepared under the supervision of

PRINCIPAL SUPERVISOR:

PROFESSOR S. CORNELIUS
University of Pretoria
Department of Private Law
Faculty of Law

CO SUPERVISOR:

SIZWE SNAIL KAMTUZE
University of Fort Hare
Faculty of Law

October 2017

"And the Lord answered me, and said, write the vision, and make it plain upon tables, that he may run that readeth it. For the vision is yet for an appointed time, but at the end it shall speak, and not lie: though it tarry, wait for it; because it will surely come, it will not tarry." Habakkuk 2: 2- 3 (KJV)

DECLARATION OF ORIGINALITY

UNIVERSITY OF PRETORIA

Full names of student: Nandipha Ntsaluba……...……

Student number: …13416091……..……

Topic of work: …**CYBERSECURITY POLICY AND LEGISLATION IN SOUTH AFRICA**

……..

Declaration

1. I understand what plagiarism is and am aware of the University's policy in this regard.
2. I declare that this mini-dissertation is my own original work. Where other people's works have been used (either from a printed source, internet or any other source), this has been properly acknowledged and referenced in accordance with departmental requirements.
3. I have not used work previously produced by another student or any other person to hand in as my own.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

SIGNATURE ……  ……

ABSTRACT

The analysis focuses on the CyberSecurity posture of South Africa within the international legal instruments that profile CyberSecurity and CyberCrime as a strategic issue and a national security imperative. This dissertation provides the definitions dominating African and global literature whilst recognising the absence of agreement on these definitions.

The ever-increasing CyberAttacks present a threat to human, economic and national security and is attracting attention from the traditional Air, Marine, and Land space. The CyberSecurity and CyberCrime debates are progressive and maturing ones that originate from the International Convention, the Council of Europe Convention on CyberCrime (COECC), which focus on criminalisation of CyberCrimes and mechanisms to guide enforcement.

From a South African perspective, CyberSecurity and CyberCrime is aptly demonstrated by the Electronic Communication and Transaction Act 25 of 2002. Since then, global awareness of CyberCrime as a national security threat has led South Africa to develop a comprehensive draft Bill on CyberSecurity and CyberCrime as a response to the SADC model law on Computer Crime and CyberCrime. Geopolitical consideration also has affected positioning decisions South Africa has assumed within the CyberSecurity architecture.

The African Union (AU) Agenda 2063 profiles the importance of prioritising security of the submarine optic fibre network as the critical physical infrastructure underpinning the virtual cloud of CyberSpace.

The critical question to address is whether the CyberCrime and CyberSecurity Bill {2017}, which has undergone several revisions since 2015, comprehensively deal with the realities that manifest within the five domains (i.e. land, maritime, air, Outerspace, CyberSpace). The question worth asking is how secure are citizens in the advent of the cloud and crowd computing? How does the myriad of legislation on CyberSecurity guarantee one's security – physically, economically and socially?

The study recognises a plethora of legislative frameworks that promote safer CyberSpace and lately, the Cybercrime and CyberSecurity Bill that aims to present a one-stop shop platform for

identification, monitoring, reporting and criminalisation of violations of security within the CyberSpace. This qualitative study firstly, seeks to present the recommendations on improving the CyberSecurity posture of South Africa, which finds itself within a variety of legislative frameworks. Secondly, from a geopolitical and geostrategic perspective, a comparative analysis of South African legislative framework with those of Germany and Russia is conducted with the aim of deepening CyberSecurity protection and awareness amongst citizens.

Germany has demonstrated international commitment to protect society against CyberCrime by signing (2001) and ratifying (2009) the Budapest Convention as well as domesticating it to ensure enforcement. Further commitment has been displayed by the signing and ratification of the Additional Protocols to the Convention on CyberCrime that focuses on criminalisation of racist and xenophobic-natured acts committed through computer systems.

Russia views 'internet sovereignty' as of national interest and at the heart of national security. Russia, however, objects to ratification of the Budapest Convention as an infringement of its sovereignty. Russia's objection to the European Convention on CyberCrime provides an inherent mandate that allows the police to open an investigation or suspected online crime originating in another country without first informing local authorities, infringing on traditional ideas of sovereignty. This, Russia believes, would invite demands for cooperation in identifying, for example, the perpetrators of the CyberAttacks on Estonia in 2007 or Georgia in 2008, along with requests from foreign law enforcement agencies in shutting down the extensive CyberCriminal activity that originates on Russia territory. Russia believes that international collaboration across law enforcement agencies should act a better deterrent to CyberCrime without threatening territorial integrity than the COECC.

Russia has emphasised the need for a new international regime that more closely corresponds to its views on CyberSecurity. Unlike America, Russia favours an international treaty along the lines of those negotiated for chemical weapons and has pushed for that approach at a series of meetings and in public statements by a high-ranking official.

Unlike German governmental speakers, Russian officials do not fear the economic but rather the political consequences of CyberAttacks, which might even lead to a potential regime change. CyberSecurity discourses and dispositive in Germany and Russia reflects similarities as well as

differences with securitisation evidently present in both cases. This is further reflected in similar government interventions as determined by risk dependencies. Nevertheless, the fundamental perceptions of the CyberSpace and the risks of internet technology differ significantly, especially regarding the focus either on the stability of the economy (Germany) or the stability of the political system (Russia).

The CyberCrimes and CyberSecurity Bill of 2017 is analysed through the lens of the legislative frameworks of Russia and Germany. In this qualitative study, similarities between South Africa's draft legislation and the approach adopted by Germany and Russia are revealed. South Africa's engagement in promoting CyberSecurity within and across states makes protection of critical infrastructure more urgent. The study further presents CyberSecurity as integral to the enterprise risk-management architecture of private and public entities.

The analysis of stakeholder engagements on the draft CyberSecurity and CyberCrime Bill of 2017 of the study exposed the need to define protocols for the proposed governance structures, boundary management as well as synergy between the role players mandated by various legislative frameworks charged with the security of personal Information. Close collaboration with the organs of state charged with the establishment and the effective functioning of governance structures articulated in sections 53 and 54 of the Cybercrime and Cyber Security Bill, identification and delineation of critical infrastructure to ensure clear responsibility, unambiguous protocols and boundary management.

In recognition of the transnational nature of CyberCrime, the study recommends that all nation states need to agree that CyberCrime, CyberAttacks and terrorist attacks may end the economic and social advantages that the CyberSpace holds for generations to come and hence, the urgency of multilateral transnational cooperation and legislative frameworks. A transition from a narrative that depicts CyberSpace as one that cannot be regulated, to a space flooding with possibilities ever imagined must emerge.

Keywords

Critical infrastructure, CyberSecurity, CyberCrime, CyberSpace, CyberTerrorism, and CyberThreats, Information Security, CyberSystems, CyberCommand.

ACKNOWLEDGEMENTS

Many hands have shaped the pages of this original work. They range from the academic baseline that triggered the attention to CyberLaw as a discipline. I wish to record my thanks to Professor Steve Cornelius, the Coordinator for Intellectual Property Programme who allowed me to enrol for CyberLaw.

I have actively participated in the Government Information space, at GITOC level as well as a member of the **South African National Information Officers Forum(NIOF) and Coordinating C**ommittee which, through the secretariat functions provided by the South African Human Rights Commission, is charged with ensuring human capital development across all tiers of Government to realise institutionalisation, monitoring compliance as well as reporting on Promotion of Access to Information (PAIA) as part of the Government Management Performance Assessment Tool (MPAT) Programme mandated to regularly assess the quality of generic management practices in departments.

The CyberLaw programme not only consolidated and contextualised my intellectual property knowledge and debate; it situated the discourse within the CyberSpace, which is rife with intellectual property infringement across all forms. Engaging with the CyberLaw, through the leadership of Ms Sylvia Papadolous, ushered me into Sizwe Snail kaMtuze who co-edited the prescribed book. I wish to profile the role he played in redirecting me from the Intellectual Property research topic I had already started to the fascinating area of CyberSpace itself.

I wish to also thank the South African National Defence (SANDF) Community for the resource support and the interest shown during the development of the Chapters of this dissertation. My family has been a blessing as lifelong learner themselves who supported my efforts.

Finally, I give all glory and honour to the Almighty for revealing such supervisors to me who have become my destiny connectors. I thank God also for my spiritual interoperable oracle, Major Prophet Shepherd Bushiri for the Talitha Kum affirmation of such destiny through the priestly anointing and kingship declaration that:

‘‘God is not a man, that He should lie, Nor a son of man, that He should repent.
Has He said, and will He not do? Or has He spoken, and will He not make it good?’
Numbers 23:19 New King James Version (NKJV)

LIST OF ABBREVIATIONS AND ACRONYMS

AU	African Union
AUCSCPDP	African Union Convention on CyberSecurity and Personal Data Protection
AUCLCS	Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa
CoECC	Council of Europe Convention on CyberCrime
COMESA	Common Market for Eastern and Southern Africa
EAC	East African Community
ECOWAS	Economic Community of West African States
FD	Framework Directive
GCA	Global CyberSecurity Agenda
GSA	Global security agenda
ICT	Information Communications Technology
ITU	International Telecommunications Union
SADC	Southern African Development Community
UNCITRAL	United Nations Commission on International Trade Law
WSIS	World Summit on the Information Society

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

1.1. Background

CyberCrimes and CyberAttacks are by nature transnational as well as borderless in that they are not bound to a physical location, country, region or ethnicity.[1] Muyowa *et al* have asserted that although Information and Communication Technology (ICT) devices connected to the internet provide an improvement on how individuals, the public, and private sectors operate in the global space.[2] These pose a major threat in the form of CyberCrimes and CyberAttacks. Underlying all these developments is the need for citizens and organisations to feel safe and secure when using ICT in the borderless CyberSpace.

William Lynn, America's Deputy Secretary of Defence, in a 2010 article wrote that although CyberSpace is a 'man-made domain' it has become 'just as critical to military operations as land, sea, air, and space'.[3] Globally, almost 3 (three) billion people who are now connected to the internet, in CyberSpace. This figure is growing rapidly and by 2020 it is estimated that it will reach 5(five) billion people, using 50 billion devices. Functionally, internet usage for Africa as at March 2017 was 9.3% while the rest of the world usage was 90.3%.

Gorr and Schünemann amplify the reality that internet users are ignorant of the hosting location of the website, which they can easily access from home. This ignorance extends to recognition and knowledge of the transnational feature of the e-mail traffic, which provides the outlook of how many borders the data package transcends before reaching the mailbox of the recipient. The

1 Muyowa M, Mtsweni J & Mkhonto N 'Developing a Cyber-threat intelligence sharing platform for South African organisations' (2017) Paper presented at Information Communication Technology and Society (ICTAS) Conference on IEEE.

2 Muyowa *et al* (note 1 above).

3 Thomas R *CyberWar will not take Place* (2013) Oxford University Press: USA xiii.

multiplicity of borders transcended by emails, usher in an attributive posture of the internet as a technical infrastructure with a transnational or global dimension.[4]

As at March 2017, of the total population in Africa of 1.25 billion (which accounts for 16.6% of the global population), only 0.345 billion (27.7%) were internet users (with 0.146 billion owning Facebook pages). As at 30 June 2017, 0.388 billion were estimated internet users accounting for internet penetration in Africa of 31.2%, representing 10.0% of the total world internet users, whilst the rest of the world recorded an internet penetration of 55.8%, which is higher than the recorded penetration rates world average of 51.7%.[5] The vulnerability of Africa to CyberAttacks is glaring when presented within the context of the rest of the world. Globally, of the population of 6.27 billion, 3.39 billion (54%) are internet users, which accounts for a global participation of 90.7%, with 1.53 billion being Facebook owners.[6]

Grobler, van Vuuren and Leenen claim that in 2007/2008 South Africa's overall online activity was estimated to be 67% of overall online activity in Africa, whilst its population accounted for only 5% of the entire continent. By extrapolation, the increase in internet activity over the decade places the importance of proper CyberSecurity awareness and formalised training in this domain. Research done in the South African provinces of Gauteng, Mpumalanga and Limpopo displayed good internet behaviour on the part of South African citizens.[7] The above was based on quantitative survey wherein completed questionnaires retrieved from different geographical areas and grouped under urban areas, semi-rural areas and rural areas revealed progress on

---

4 Gorr D & Schünemann WJ 'Creating a secure CyberSpace: Securitisation in internet governance discourses and dispositives in Germany and Russia' (2013) 20:12 *International Review of Information Ethics* 37 - 51.

5 Internet World Stats 'Top 20 countries with the highest number of internet users' available at: http://www.internetworldstats.com/stats1.htm (accessed: 23 October 2017).

6 The 2017 population estimates are based mainly on figures from the United Nations Population Division and local sources. The internet usage numbers come mainly from data published by WWW, ITU, the Nielsen Company, Facebook, and other trustworthy sources. Data from this table may be cited giving the due credit and establishing an active link back to Internet World Stats.

7 Grobler M, Van Vuuren JJ & Lenen L 'Implementation of a CyberSecurity policy in South Africa: Reflection on progress and the way forward, IFIP International Conference on Human Choice and Computers' (2012) *Springer* 219.

CyberSecurity awareness. The levels of CyberSecurity awareness were calculated as 69% for urban areas, 53% for semi-rural areas and 40% for rural areas. A cumulative extrapolation of total awareness in South Africa based on the overall awareness of the sample group stood at an estimated 51%.[8]

Abdulrauf and Fombad attest to the exponential increase in internet penetration as indicated above, which further profiles the development of a credible Information Society as a non-negotiable.[9] Such a societal development would be underpinned by the availability of and access to the Internet.

The unintended consequence of a reliable internet infrastructure ushered in by 'being wired to the rest of the world has resulted in some positioning within the perimeter of CyberCrime, rendering the continent's information systems more vulnerable than ever before'.[10] Orji describes the posture that characterises the convergence of telecommunications and computer technologies as a 'techno crescendo of the information age'.[11]

Interconnectedness and interoperability have created a widespread integration of Information technologies in almost every area of citizens' lives through various applications aimed at improving service delivery through connected cities with one-stop shop e-service delivery platforms. The emergence of E-government, E-commerce, E-education, E-health, and E-environment have created viable channels for accounting, monitoring and evaluation delivery of basic services, especially in rural areas. This has led to the emergence of the Information age.[12]

In Africa, the development is turning every citizen into a player in CyberSpace where rules, jurisdiction as well as precedence are not yet clearly defined. The exponentially increasing Cyber footprint and presence of human species across the globe in the CyberSpace further exposes

8 Grobler, Van Vuuren & Lenen (note 7 above) 219.

9 Abdulrauf LA & Fombad CM 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8:1 *Journal of Media Law* 70.

10 Abdulrauf & Fombad (note 9 above) 71.

11 Orji UJ *CyberSecurity Law & Regulation* (2012) Wolf Legal 2.

12 Orji 2012 (note 11 above) 6.

high risks that require mitigation. By 30 June 2017, Nigeria was registered as the only African country that featured in the top twenty (20) countries with the highest number of internet users with a growth of 45.7% from 2000-2017.[13]

In his dissection of the multilateral arrangements that have been instituted to embrace the CyberSecurity agenda in Africa, Orji asserts that, within the past decade, Africa has witnessed a phenomenal growth in internet penetration and the use of ICT's. This posture has profiled the attributes of CyberSecurity, which are confidentiality, integrity, availability and accountability.[14] However, the spread of ICTs and internet penetration has also raised concerns about CyberSecurity at regional and sub-regional governance forums. This has led African intergovernmental organisations to develop legal frameworks for CyberSecurity.[15]

The exponentially increasing presence of human species across the globe in the CyberSpace further exposes the inherent jurisdictional challenge that demands a multilateral response. The jurisdictional problem of CyberCrime manifests itself in 3 (three) dimensions across states. The first dimension is lack of criminal statutes due to uneven maturity to enact statutes criminalising computer misuse offences.[16]

The second dimension is ushered-in by lack of procedural powers as states often lack the resources and procedural tools necessary to conduct computer crime investigation. The June 2017 WannaCry CyberAttacks that was linked to North Korea by defence agencies in the United States and the United Kingdom and the subsequent Petya malware outbreak with reported links to sources in Russia present evidence of the new strain of high profile global scale, debilitating attacks that appear to be government sponsored. These present the increasing entanglement of financially motivated CyberCrimes that wreaked havoc against worldwide businesses,

---

13 Internet World Stats (note 5 above).

14 Orji 2012 (note 11 above) 30-33.

15 Weber AM 'The Council of Europe's Convention on CyberCrime' (2003) 18:1 *Berkeley Technology Law Journal* 425-46.

16 Weber (note 15 above) 425-46.

governments and non-profit institutions command and control orchestrated creating chaos whose focus was on realisation of strategic geopolitical goals.[17]

Thirdly, prosecution is frustrated by a lack of enforceable co-operation due to the lack of mutual assistance provisions with foreign states wherein both the host and victim states have adequate criminal statutes and investigative powers. As international co-operation on CyberCrime has traditionally been the exception rather than the rule, these requirements are frequently an insurmountable barrier to the successful prosecution of Cyber criminals.[18] The latest South African citizens personal Information breach of 18 October 2017, which was reported by an Australian web security expert revealed a data breach of private records of about 31.6 million South Africans, further underscores enforceable mutual assistance provisions to underpin the multilateral response to Cyber Criminality.[19]

Organisations and individuals' personal and commercial Information are located on databases which some are hosted in the cloud and thus vulnerable to CyberAttacks. Vessels at sea, air capability and spacecrafts in Airspace depend on electronic communication as they traverse the globe. Orji asserts that the increasing interconnectivity of countries and national critical infrastructures in today's global network society have ushered the world into what has been aptly described as 'an age of interdependence' where each nation's security is also dependent on the actions of the other nations of the world'.[20] This state of affairs clearly underscores the need for the collective responsibility of states for global CyberSecurity.[21]

Cole *et al* attest to the traction on a global scale that has profiled CyberSecurity issues. On the one hand, at international level, more nations are becoming aware of how CyberSecurity can

---

17 2017 Midyear CyberSecurity Risk Review: Forecast and Remediation Executive Summary available at: www.accenture.com/za-en/insight-cyber-threat-scape-report-2017 (accessed: 23 October 2017).

18 Weber (note 15 above) 425-46.

19 Gous N 'Private Information of about 31.6m South Africans breached and still online' Herald Live available at: http://www.heraldlive.co.za/news/2017/10/18/private-Information-31-6m-south-africans-breached-still-online (accessed: 23 October 2017).

20 Orji UJ 'Deterring CyberTerrorism in the global Information Society: A case for the collective responsibility of states' (2014) 6:1 *Defence against Terrorism Review* 31.

21 Orji 2014 (note 20 above) 41.

affect their critical Information and communication infrastructure. Other countries maximise collaborative efforts to improve their relations with other developed countries, thus creating transnational posture to national, economic and human security through CyberSecurity. On the other hand, equivalent initiatives for response teams for CyberCrime and end-user education on CyberSecurity are patchy in Africa. There is a greater focus on CyberCrime legislative reforms and less triangulation to economic, social and national security. An assertion that Africa has more pressing socio-economic pressures which exposes Africa to more CyberSecurity vulnerabilities as the continent claims the highest percentage of cell phone subscribers in the world.[22]

The Draft international Conventions on CyberSecurity, as well as the COECC profile the synergies of CyberSecurity and Cyber Criminality.[23] This synergy emanates from the increase in the use of digital technology for critical infrastructure, military operations, and intelligence gathering or management, which demands the creation of comprehensive national CyberSecurity plans.[24]

CyberSpace has become a new battleground, which affects all aspects of life, hence the urgent need for CyberSecurity. Cassim depicts CyberSpace through the prism of global intelligence as 'a battle space of WarFare and criminality where nation states, terrorists, activists and organised criminals leverage the platforms ushered in by CyberSpace to conduct their nefarious activities'.[25] In response to these realities, South Africa has developed a comprehensive bill that anticipates all security concerns; the CyberSecurity Bill that provides for criminalisation of offences taking place within the CyberSpace.[26] Further, in strengthening the basis laid by the Electronic Communications and Transaction Act 25 of 2002 (referred herein as the ECT Act) regarding the responsibilities of service providers, it places responsibilities on internet service providers to protect the data subject that own the Information.

---

22 Cole K *et al* 'CyberSecurity in Africa: An assessment' (2008) *Atlanta, Georgia Sam Nunn School of International Affairs, Georgia Institute of Technology* 27

23 Cole *et al* (note 22 above) 1.

24 Cole *et al* (note 22 above) 1.

25 Cassim F 'Formulating specialised Legislation to address the growing spectre of CyberCrime: A comparative study' (2009) *PER* 18.

26 Snail kaMtuze S 'Cyber Crime in the context of the ECT Act' (2008) 16:2 *Juta's Business Law* 63-9.

The National Integrated Information and Communication Technologies White Paper was approved on 28 September 2016. The White Paper outlines the overarching policy framework for the transformation of South Africa into an inclusive and innovative digital and knowledge society. It further reinforces through extension the strategies that define South Africa Connect, the National Broadband Policy, the National CyberSecurity Policy Framework 2012 and the National Information Society and Development Plan.

The National CyberSecurity Policy Framework 2012 places CyberSecurity at the centre of national security and the safekeeping and protection of national interests. In 2012, Cabinet adopted the National CyberSecurity Policy Framework that established the CyberSecurity Response Committee (CRC) charged with addressing centralised coordination to address online infringement and CyberCrimes.[27] The strategic environment is characterised by a multi-layered organisation of players with associated responsibilities within the CyberSecurity environment with the establishment of security CSIRT and sector CSERT grounded through an ontology that profiles consistent drive on Cyber security education and awareness.[28] Gcaza argues that the successful implementation of the National CyberSecurity Policy Framework is dependent on deepening the cultivation of CyberSecurity culture among all people.[29] She further argues that to enable prominence of cultivating a CyberSecurity culture, explicit domain definition and delineation remain central.[30] Delineating and defining the national CyberSecurity culture domain would greatly contribute to realising the elements that should be in place for such a culture to be cultivated. It is contended that a clearly defined national CyberSecurity culture environment with boundary management, accurately contributes to modelling a well-defined and delineated approach to such a CyberSecurity culture.[31]

When defining CyberSpace, the former President of the United States of America, Barak Obama, presented it as a virtual space that touches on nearly every part of daily life, involving, as he

---

27 *SA Government Gazette (2011) Draft National CyberSecurity Policy Framework for South Africa*.

28 Grobler *et al* (note 7 above).

29 Gcaza N *el al* 'A general morphological analysis: Delineating a CyberSecurity culture' (2017) 25:3 *Info and Computer Security* 271

30 Gcaza *et al* (note 29 above) 264.

31 Gcaza *et al* (note 29 above) 265.

stated, 'the broadband networks beneath us and the wireless signals around us, the local networks in schools, hospitals and businesses and the massive grids that power nations'.[32] It is imperative that classified military and intelligence networks keep nations safe, within the context and realities of an Information age with the World Wide Web that makes people more interconnected now than at any other time in human history. CyberSpace must be secured to ensure economic growth and to protect the way of life.[33] This assertion complements South Africa's National Development Plan Outcomes, which envisages that all people in South Africa are, and feel safe whilst ensuring rapid expansion, modernisation, access and affordability of Information and communications infrastructure and electronic communication services, including broadband and digital broadcasting.[34] This crosscutting end state has implications for Air, Land, Maritime, Airspace as well as CyberSpace domains.

Orji proposes treaty based collaborative interventions premised on the need for every state to establish appropriate deterrent legal measures that would ensure that activities in CyberSpace that are conducted within its jurisdiction do not cause trans-boundary harm in other states.[35] He further underscores the institutionalisation of state accountability where its failure to establish regulatory measures to deter or prosecute CyberCrimes or CyberTerrorism within its territory.[36] This state of affairs has created a porousness in other states, which manifests in the perpetration of such acts and results in trans-boundary effects in other states.[37]

Orji asserts that the Information Society, as characterised by the integration of computer and digital communications technologies into all aspects of life, has redefined traditional notions of security.[38] The wired-up communities, countries and the global economy are adversely affected by malicious conduct against computer systems and networks in ways previously unimagined.

---

32 The New York Times 'Obama's remarks on Cyber Security' (May 2009) *The New York Times* available at: http://www.nytimes.com/2009/05/29/us/politics/29obama.text.html (accessed: 5 May 2017).

33 President Barack Obama: Remarks on CyberSecurity 29 May 2009.

34 Medium – Term Strategic Framework (MTSF) 2014-2019 9-14.

35 Orji 2014 (note 20 above) 38.

36 Orji 2014 (note 20 above) 35.

37 Orji 2014 (note 20 above) 31.

38 Orji 2014 (note 20 above) 31.

This reality factors in one of the most critical strategic risks of the Information Society, which is CyberTerrorism.[39]

At the sub-regional level, the Economic Community of West African States (ECOWAS) has adopted a Directive on CyberCrime, while the Common Market for Eastern and Southern Africa (COMESA) and the Southern African Development Community (SADC) has adopted model laws. At the regional level, the African Union (AU) has adopted a Convention on CyberSecurity and Personal Data Protection (AUCSCPDP).[40] Orji presents the challenge as operational limitations that bedevil the implementation of the AUCSCPDP. This relates to the inadequacy of the framework for mutual assistance and international co-operation among African states, which may limit and fragment international co-operation and mutual assistance along sub regional lines or bilateral arrangements. To address the challenge cited, a proposal is sponsored for the development of international co-operation and mutual assistance mechanisms within the framework of the AU and makes a case for the establishment of a regional Computer Emergency Response Team to enhance cooperation as well as coordination of responses to CyberSecurity incidents.[41]

The existence of few major significant CyberSecurity initiatives in Africa, especially in the SADC, and East and West Africa is a matter of concern given that ICTs are hailed as a major solution to many of Africa's pressing problems, and CyberSecurity is a critical issue that needs to be better addressed in Africa. Investing in CyberSecurity will not only protect a country's infrastructure and citizens from harm but will also strengthen a nation's identity as a secure nation in the global telecommunications sphere.[42]

---

39 Orji 2012 (note 21 above) 1-10.

40 Abdulrauf & Fombad (note 9 above) 73.

41 Orji UJ 'Multilateral legal responses to Cyber Security in Africa: Any hope for effective international co-operation?' (2015) *African Centre for Cyber Law and CyberCrime Prevention* 105.

42 Cole *et al* (note 22 above).

The reality is that CyberCrime operates in the virtual space, presents a challenge regarding normal jurisprudence and its rules, hence the need for agile legislation.[43] Judge Stein Schjølberg affirms the establishment of the Geneva Convention or the Declaration on CyberSpace, which has as objectives:

a. The development of a set of norms, rules, and standards to guide standards for international CyberSecurity measures;
b. International coordination and cooperation through INTERPOL in investigation of transnational serious CyberCrime;
c. Standards for global partnerships with the private sector for the investigation and prosecution of serious CyberCrime;
d. To harmonise CyberCrime laws; as well as
e. To establish an International Criminal Court or Tribunal for CyberSpace.[44]

Further, he argues further that discussions on CyberSecurity in international policy and academic circles should focus primarily on how to protect the Information that exists in CyberSpace.[45] He further substantiates this positioning of the global submarine network as the 'backbone' of the Internet that enables the ubiquitous use of e-mail, social media, phone and banking services; goods and services which contributes up to 95% of international communication.

This qualitative study compares South African CyberCrime and CyberSecurity Legislation with those of Russia and Germany. Both states feature in the 2017 top countries with the highest number of internet users.46 The two states can be used as legislative benchmarks, which manifests in the CyberSecurity posture of South Africa. South Africa and Russia are both members of BRICS have not ratified the International Convention, the Council of Europe Convention on CyberCrime (COECC). Both countries are canvassing for a global Protocol in

---

43 Schjølberg S & Ghernaouti-Hélie S 'A global treaty on CyberSecurity and CyberCrime' (2011) *CyberCrime Law* 97.

44 Schjølberg & Ghernaouti-Hélie (note 43 above) 97.

45 Davenport T 'Submarine Cables, CyberSecurity and International Law: An InterSectional Analysis' (2015) 24 *Catholic University Journal of Law & Technology* 58.

46 Internet World Stats (note 5 above).

Cybercrime and Cybersecurity. Germany has ratified the Convention with its Cybercrime and Cybersecurity Policy and Legislation, displaying similarities with contents of the current CyberCrime and CyberSecurity Bill. Germany is also a member of North Atlantic Treaty Organisation (NATO) which was one of the first international organisations to redefine its CyberDefence policy that focuses on safeguarding critical information infrastructure, hence the inclusion of NATO as one of the international organisations that have positively influenced the global cybersecurity discourse as well as canvassed for exponential increase in people as well as cybersecurity capabilities. NATO has profiled CyberSpace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea.

South Africa's membership has introduced it to Russia as member of BRICS as well as an active global player that has contended with the United States in making a case for global treaty on cybersecurity through its National Security Strategy 2020. The Security Strategy profiles Russia's commitment in promoting continental as well as block partnerships in promotion of cybersecurity. Russia's 2020 Security Strategy presents a critical view of the European security architecture as well as little progress in NATO-Russia relations which a symptomatic of Russia's inability to influence the Alliance's decisions, as a partner in the NATO-Russia Council. The Russian leadership has profiled invigoration of international organizations that can guarantee security issues and promotes the evolution of regional coalitions like the OSCE, CSTO, SCO and the BRIC (Brazil, Russia, India and China) group. This security posture presents opportunities for South Africa to benefit as member of BRICS.

Russia perceives other powerful actors - the EU,China and India - as necessary partners against global threats. It also promotes cooperation with the United States in terms of an equal strategic partnership in fields of common interests, making references to arms control, non-proliferation, counterterrorism and conflict settlement. The NSS marks the altered perception of the Russian leadership that tries to combine elements of the past and the future and set on a realistic basis Russia's relation to the rest of the world.[47]

Recommendations on this analysis will assist in providing the answers to the CyberSecurity outlook of citizens as well as provide an analysis of the CyberSecurity legal framework from a

[47] *Dimitrakopoulou, Sophia, and Andrew Liaropoulos. "Russia's National Security Strategy to 2020: A Great Power in the Making?" Caucasian Review of International Affairs 4.1 (2010): 39-41.*

South African perspective, giving due regard to the regional instruments that have been developed in this respect. The question worth asking is, how secure are citizens in the advent of the cloud and crowd computing? How does the myriad of legislation on CyberSecurity guarantee one's security-physically, economically and socially?

The reality that CyberCrime operates in a virtual space presents a challenge regarding the normal jurisprudence and its rules, hence the need for agile legislation that provides an effective deterrent system and cross-border cooperation against CyberTerrorist conduct.

This dissertation recognises the CyberCrime and CyberSecurity Bill of 2017, a product of several revisions which presents a one-stop shop platform for identification, monitoring, reporting and criminalisation of violations of security within the CyberSpace. The developmental trajectory of this aforementioned legislative framework reflects semblance of similarities with the provisions of Budapest Convention as depicted in the content thereof.

From a European perspective, 2 (two) international agreements are particularly relevant both for their European focus and their legal effect: the 2001 Council of Europe Convention on CyberCrime (CoECC), and the 2005 European Union Framework Decision on Attacks Against Information Systems (referred to as the Framework Directive (FD).[48] Substantive Criminal Law provisions exist in the first section of the second Chapter of the Convention. The Chapter covers specific categories, including crimes against the confidentiality, integrity and availability of data and systems (Articles 2-6); crimes related to computers (Articles 7-8); crimes related to the content of data (Article 9) as well as crimes against intellectual property and related rights (Article 10).[49]

The European legal framework provides a three-path solution: the reduction of frictions among national legislations; the introduction of new investigative powers; and the facilitation of

---

48 Schjølberg S *Wanted: A United Nations CyberSpace Treaty: Global Cyber Deterrence: Views from China, the US, Russia, India, and Norway* (2010) 28.

49 Council of Europe Convention on CyberCrime.

international cooperation.[50] South Africa, although not a signatory to the EU Agreements, has domesticated the contents of these agreements in various legislative frameworks. It is however, argued by various analysts that the implementation of these international instruments depends less on enforcement mechanisms. Considerations like international security and public opinion seem to drive the enforcement agenda.

1.2. Concepts defined: CyberSpace, CyberSecurity, CyberTerrorism, CyberWarfare and CyberCrime

1.2.1. CyberSpace

Judge Stein Schjølberg defines CyberSpace, as the fifth common domain – after Land, Sea, Air and OuterSpace that commands great co-ordination, co-operation and legal measures among all nations.[51] As such, a CyberSpace treaty or a set of treaties at the level of the United Nations, including CyberSecurity and CyberCrime, should be the global framework for peace and justice in CyberSpace. CyberSpace remains central to progressive development of international law to enable the investigation and prosecution of the most serious CyberCrimes and CyberAttacks of global concern, which should be adjudicated by an international court or tribunal for CyberSpace.[52]

CyberSpace and its underlying infrastructure are therefore, vulnerable to a wide range of risks stemming from both physical and CyberThreats and other hazards created by sophisticated CyberActors and nation-states that exploit vulnerabilities to steal information and money. A range of traditional crimes that threaten human and economic security dimensions is perpetrated through CyberSpace. Their capabilities also disrupt, destroy or threaten the delivery of essential services and of growing concern is the CyberThreat to critical infrastructure, which is increasingly subject to sophisticated CyberIntrusions that pose new risks.[53]

---

50 Papathanassiou A *et al* 'Legal and social aspects of CyberCrime in Greece' (2013) *International Conference on E-Democracy Springer* 5-6.

51 Schjølberg (note 47 above) 28.

52 Schjølberg & Ghernaouti-Hélie (note 43 above).

53 Cole *et al* (note 22 above) 9.

The emerging risks and potential consequences of such Cyber events have profiled the need to strengthen the security and resilience of CyberSpace as an essential attribute of all homeland security. Securing CyberSpace presents challenges emanating from the ability of malicious actors who operate from anywhere in the world, the linkages between CyberSpace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex Cyber networks.[54] These threats are serious and they constantly evolve, hence the need to address them effectively.[55] The end state being that of ensuring that the internet remains an engine for economic growth and a platform for the free exchange of ideas.

The uniqueness in conceptualising CyberSpace as a challenge to the achievement of consensus on the exact definition of CyberSpace has been and remains elusive. Van Epps defines CyberSpace as 'a complex and ever-changing man-made hybrid environment that is partly physical and partly virtual and which is characterised by the information technology networks — as well as the hardware, software, connective lines, and data that facilitate our digital interconnectedness'.[56]

However, Van Epps argues that most definitions are consistent with the US military's description of CyberSpace as 'a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers'.[57] Van Solms *et al* define CyberSecurity as the protection of CyberSpace itself, the electronic information, the ICTs that support CyberSpace, and the users of CyberSpace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in CyberSpace.[58] The United States Department of Defence

54 Cole *et al* (note 22 above) 11.

55 Kabanov Y 'Information (Cyber-) Security Discourses and Policies in the European Union and Russia: A comparative analysis (2013) *Foresight* 7.

56 Van Epps G 'Common ground: US and NATO engagement with Russia in the cyber domain' (2013) 12:4 *Connections: The Quarterly Journal* 18-19.

57 Van Epps (note 55 above) 19.

58 Von Solms R *et al* R 'From Information Security to CyberSecurity' (2013) 38 *Computers & Security* 97-102.

(DoD) defines CyberSpace as a 'domain characterised by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via network systems and associated physical infrastructures'.[59]

1.2.2. CyberSecurity

Van Epps argues that CyberSecurity has emerged as 'a critical national security issue, spawning a growth industry that researches solutions to the technical, legal, and policy challenges'.[60] This strategic issue emerged because of the exponential growing dependence of modern society on digital technology and the inherent risks that characterises the vulnerability of digital systems to Cyber threats.[61]

CyberSecurity is premise on the following priorities:

i. Protection of the country's critical infrastructure, which includes the global submarine optic fibre networks;
ii. Improved identification and reporting on incidents and developing capabilities to anticipate future incidents; and
iii. Promotion of international collaboration for open, interoperable, secure and reliable CyberSpace for citizens to transact with full assurance that their data is safe and secure.[62]

Delaney defines CyberSecurity as encompassing integrated and interconnected efforts to secure digital information, the equipment processing that information.[63] These are means of hosting as well as transmitting that Information among various devices and platforms. Central to CyberSecurity is Information Security that emanates from assurance of the preservation of

---

59 Thibodeaux A 'Hacking back: Surviving in the digital age' (2015) *Preview Diss. Utica College* 3-5.

60 Van Epps (note 56 above).

61 Van Epps (note 56 above) 19.

62 Kabanov (note 55 above).

63 Van Epps (note 56 above) 19e.

confidentiality, availability, and integrity of information as this relates to authenticity, accountability, non-repudiation, reliability and resilience.[64]

For Van Solms *et al*, CyberSecurity has to do with the protection of CyberSpace itself, the electronic information, the ICTs that support CyberSpace, and the users of CyberSpace in their personal, societal and national capacity, including any of their interests, either tangible or intangible that are vulnerable to attacks originating in CyberSpace.[65]

CyberSecurity, which aims to ensure that the internet remains an engine for economic growth and a platform for the free exchange of ideas, is premise on the following priorities:

i. protection of the country's critical infrastructure, which includes the global submarine optic fibre networks ;
ii. improved identification and reporting on incidents and developing capabilities to anticipate future incidents; and
iii. Promotion of international collaboration for open, interoperable, secure and reliable CyberSpace for citizens to transact with full assurance that their data is safe and secure.[66]

1.2.3. CyberTerrorism

According to Lewis, CyberTerrorism involves 'the use of computer network tools to shutdown critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population'.[67] He further argues that, from a strategic military perspective, attacks that do not degrade national capabilities are not significant. This is because such CyberAttacks do not cause damage that rise above the threshold of the routine

---

64 Delaney DG 'CyberSecurity and the administrative national security state: Framing the issues for federal legislation' (2013) 40 *J. Legis.* 251.

65 Von Solms R *et al* 'From Information Security to CyberSecurity' (2013) 38 *Computers & Security* 97-102.

66 Kabanov (note 55 above).

67 Lewis JA *Assessing the Risks of CyberTerrorism, CyberWar and other CyberThreats* (2002) 1.

disruptions every economy experiences, therefore it does not pose an immediate or significant risk to national security.[68]

Cassim affirms CyberTerrorism as one of the recognised CyberCrimes relating to the premeditated use of disruptive activities, or threat thereof in CyberSpace, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in the furtherance of such objectives. Such attacks assume a variety of approaches, which for example, range from breaking into a company's computer network to create some havoc, sabotaging a country's gas lines, or causing havoc on the international finance system.[69]

Terrorist attacks against information infrastructures, computer systems, computer programmes and data are meant to intimidate or persuade a government or its people to further a political or social objective. These attacks present a high risk of probable injury, loss of life and destruction of property and thus present a threat to the CyberSecurity posture of States and their citizenry.[70] It remains essential to differentiate between hacktivism and terrorism, as the latter primarily revolves around use of digital means for organisational purposes and the use of digital communications to commit acts of terror.[71]

1.2.4. States' response to CyberTerrorism

In Africa, various legislative frameworks have been introduced albeit at various maturity levels, that aimed at domesticating the African treaties on CyberSecurity and data protection.

South Africa's offensive response in addressing CyberTerrorism and terrorist financing is evidenced by the Prevention of Organised Crimes Act (POCA),[72] the Financial Intelligence Centre

---

68 Lewis (note 66 above) 3.

69 Cassim F 'Addressing the spectre of CyberTerrorism: A comparative perspective' (2012a) 15:2 *Potchefstroom Electronic Law Journal* 380-415.

70 Cassim (note 69 above) 384.

71 Cassim (note 69 above) 385.

72 Act 38 of 1999.

Act (FICA) as amended,[73] the Electronic Communications and Transactions Act (ECTA)[74] the Regulation of Interception of Communications and Provision of Communications-Related Information Act (RICA)[75] and the Protection of Constitutional Democracy against Terrorism and Related Activities Act (PCDTRA)[76] and the CyberCrime and CyberSecurity Bill, which creates governance structures for a secure transacting space. The Bill establishes responsibilities for incident reporting as well as timely resolution of breach incidents. Flowing from the Bill are the responsibilities for the establishment of CyberSecurity hubs with the requisite strategies, policies and regulatory frameworks. Central to these is the South African National Defence Force CyberSecurity Strategy and the norms and standards to inform the operational effectiveness, internal, external and locative efficiency of the CyberCommand centre.

Boundary management and effective operationalisation of legislative protocols to guide collaborative and collective interventions across the various organs of states herein underscored in ensuring that all people are and feel safe in South Africa across all the five domains.

1.2.5. CyberWarfare

CyberWarfare according to Raymond Parks, is define as ‘an epitome of asymmetric WarFare’, that is, a combination of a computer network attack with computer network defences, as well as possibly special information operations.[77] CyberWarfare is a sub-set of information WarFare that involves the application of the kinetic principle of economy of force, the kinetic principle of unity of command is applicable to CyberWarfare in certain circumstances, the kinetic principle of security, the kinetic principle of manoeuvre as well as the kinetic principle of simplicity. There are many CyberWorlds, but the one most relevant to CyberWarfare is the internet and related networks that share media with the internet.[78]

---

73 Act 38 of 2001.

74 Act 25 of 2002.

75 Act 70 of 2002.

76 Act 33 of 2004.

77 Parks RC & Duggan DP 'Principles of CyberWarFare' (2011) 9:5 *IEEE Security & Privacy* 30-5.

78 Parks & Duggan (note 77 above) 30-5.

Hoisington defines CyberWarfare as ranging from relatively innocuous web vandalism to severe attacks on critical national infrastructure.[79] While the temporary de-activation of government webpages may represent little more than a nuisance, the threat of misinformation spread to military commanders in the field, or a concerted attack on a state's electric, water, communications, transportation, or fuel networks represents a serious risk to both soldiers and civilians.[80]

CyberWarfare is distinct from Cyber espionage in the sense that whilst CyberWarfare aims to destroy the enemy's capabilities, CyberEspionage aims at gaining access to computer systems that contain essential commercial and military information without detection, and locate with the aim of draining essential intelligence information.

1.2.6. CyberCrime

CyberCrime is quintessentially transnational and involves jurisdictional assertions of multiple states hence the need for development of multilateral agreements on jurisdiction and enforcement to avoid conflicting claims.[81] CyberCrime entails internet-related traditional crime, which includes all forms of crimes in which offenders rely on the use of the internet to either facilitate or commit a traditional form of crime as well as those crimes in which offenders use the internet to commit the offence, referred to as 'computer assisted crimes'. Computer-assisted crimes might constitute an entirely new form of crime, as they are significantly different from traditional crimes.

In an article entitled 'Novelty of CyberCrime: An assessment in light of routine activity', Majid distinguishes between 'computer-assisted crimes' (those crimes that pre-date the internet but take on a new life in CyberSpace, for example, fraud, theft, money laundering, sexual harassment, hate speech, pornography) and 'computer-focused crimes' (those crimes that have emerged in

---

79 Hoisington M 'CyberWarFare and the use of force giving rise to the right of self-defence' (2009) 32 *BC Int'l & Comp. L. Rev* 439.

80 Janczewski L (ed) *Cyber WarFare and CyberTerrorism* (2007) IGI Global.

81 Sofaer AD *et al A Proposal for an International Convention on CyberCrime and Terrorism* (2000) Stanford University, Centre for International Security and Cooperation 13.

tandem with the establishment of the internet and could not exist apart from it, for example, hacking, viral attacks, website defacement).[82]

He situates CyberCrime into four established legal categories; the first being CyberTrespass that entails activities that involve illegal boundary crossing into other people's property and/or causing damage, for example, hacking, defacement, viruses. The second category is Cyber-deception and theft which encapsulates stealing (money, property), credit card fraud, and intellectual property violations (also known as 'piracy'). The third category, CyberPornography, criminalises activities that breach laws on obscenity and decency. Lastly, CyberViolence or doing psychological harm to, or inciting physical harm against others, thereby breaching laws pertaining to the protection of the person, such as hate speech and stalking for example.[83]

Most jurisdictions have legislation concerning thefts and provide legal measures for the recovery of lost assets, as well as intellectual property laws to protect against the unauthorised exploitation of intellectual property. Most jurisdictions also have variants of the obscenity laws and laws that prohibit incitement, although their legislative strength can vary where Internet content is protected by laws of free speech. In common with the other two crime groups, legislation does nevertheless vary across jurisdictions in terms of judicial seriousness.[84]

Orji argues that whilst recognising the increasing internet penetration in Africa, the negative impact of CyberCrime in the African economy is worth profiling also. Nigeria, which has the largest Internet user population in Africa, is estimated to lose over US$13 billion annually due to CyberCrime. South Africa is reported to lose over R5.7 billion annually due to CyberCrime while Norton also reports that 70% of South Africans have fallen victim to CyberCrime compared with a global average of 50%.[85] It is also foreseeable that the impact of CyberCrime on African

---

82 Majid Y 'The novelty of "CyberCrime": An Assessment in light of routine activity theory' (2005) 2:4 *European Journal of Criminology* 407-27.

83 Majid (note 81 above) 407-27.

84 Cassim F 'Addressing the growing spectre of CyberCrime in Africa: Evaluating measures adopted by South Africa and other regional role players' (2011) 44:1 *Comparative and International Law Journal of Southern Africa* 123-38.

85 Orji UJ 'Regionalising CyberSecurity governance in Africa: An assessment of responses' (2016) *Securing CyberSpace* 203.

economies will continue to advance with increasing availability and dependence on ICTs and the availability of broadband capacity.

1.3. Chapter Outline and Conclusion

This Chapter provides the background to the topic, the approach to the comparative analysis, the definition of concepts used as provided for by various authors in the CyberSecurity space. Most authors claim that no singular definition exists for CyberSecurity or for CyberCrime; hence the focus has been on attributions that prevail in the CyberSpace. It is quite evident that CyberSpace has ushered in the latest battleground within the international law space, hence the need to dissect the global, continental and regional space to better situate the South African CyberSecurity posture.

This dissertation is structured as follows:

Chapter 1 is the introductory Chapter, which sets out and provides the outline of the different Chapters.

Chapter 2 deals with international legal instruments that deal with CyberCrime, CyberSecurity and Cyber-terrorism on the international landscape.

Chapter 3 deals with the South African legal context with reference to legislation, case law as well as Common Law.

Chapter 4 deals with German Comparative Law on CyberCrimes and CyberSecurity.

Chapter 5 also adds the Russian legal dynamic by giving an exposition of Russian CyberCrime and CyberSecurity legislation.

Chapter 6 provides a comparative analysis of the Governance, Risk and Compliance dimensions across the selected jurisdictions.

Chapter 7 is the concluding Chapter containing various suggestions on the way forward regarding South African CyberCrime and CyberSecurity with reference to International law as well as Russian and German comparative approach.

This Chapter introduces an overview of the global and continental CyberSecurity landscape as gleaned from the internet penetration and internet usage trajectory. South African internet penetration is triangulated using continental and regional prism, thus unveiling the inherent vulnerabilities that the CyberSpace have been ushered in by the big data that characterise the cloud and crowd computing of the wired information age. The interplay of the concepts that characterise the CyberSpace and the absence of consensus on definitions within the CyberSpace has been elucidated through a presentation of various views.

The need to establish CyberSpace as a *sui generis* mechanism of transnational character requires further amplification as it repositions the narrative within its own distinct space that interacts cross the Land, Maritime, Air and OuterSpace, thus assuming a cross cutting attribute. The role of the international legal instrument – the Budapest Convention – in raising the profile of CyberCrime beyond just Common Law has been aptly presented together with regional responses, which give substance to the *Sui genesis* attribute of CyberSpace. South Africa has introduced a myriad of legislation to deal with CyberCrime across various sectors in line with international legal instruments. Invoking Section 233 of the Constitution[86] relating to the domestication of international law has been aptly presented by the ECT Act, as the principal legislation that created a variety of crimes beyond Common Law.

Driven by the National Development 2030 outcome document in ensuring that all people feel and are safe, the question addressed relates to how secure citizens are in the advent of the cloud and crowd computing as well as the extent to which legislation on CyberSecurity guarantees personal security – physically, economically and socially. These questions are addressed in the various Chapters that focus on international legal instruments, domestic legislation as well as comparative analysis with German legislation and a BRICS partner, Russia. This endeavour aims at responding to the critical question of whether the CyberCrime and CyberSecurity Bill (2017), comprehensively deals with the realities that manifest within the four domains, that is, Land,

86 Constitution of the Republic of South Africa 1996.

Maritime, Air and the OuterSpace. In the Chapter that follows, I present the international legal CyberSecurity landscape and define South Africa's response, which reflects geopolitical considerations.

CHAPTER 2: INTERNATIONAL LEGAL INSTRUMENTS

2.1. Introduction

The quest for peace, justice and security in CyberSpace through the creation of a better and safer CyberSpace that contributes to national, economic and human security dimensions of CyberSecurity have also foreground the global initiatives that ensued for a coherent and global approach to CyberSecurity and CyberCrime issues.[1] This Chapter uncovers the international legal instruments that guide the CyberSecurity space at international, continental and regional levels, as well as customary law governing CyberCrime, CyberSecurity, CyberTerrorism, and CyberWarfare frameworks. Further, the Chapter examines the extent to which African regional and sub-regional multilateral organisations are responding to CyberSecurity concerns, which are rooted in human rights, as a mechanism to rejuvenate the emergence of a safe and secure global Information Society.

As previously stated, CyberSpace is the fifth dimension – distinct from Air, Water, Land and OuterSpace, which is characterised by inherent strategy and risks emanating from inappropriate disclosure, misappropriation and destruction of data and information. Such incidents, when viewed at a macroscopic level, constitute threats to global and domestic competitiveness as well as to public safety, national security and territorial integrity.[2] Since CyberSpace is the fifth common space, it requires co-ordination, co-operation and legal measures among all nations, in the same way as these other domains. This will ensure robust and resilient legal infrastructure to service a durable and all-inclusive global Information Society.[3]

---

1 Cole K *et al* 'CyberSecurity in Africa: An Assessment' (2008) *Sam Nunn School of International Affairs, Georgia Institute of Technology* 4-9.

2 Ghernaouti-Hélie S 'Need for a United Nations CyberSpace treaty' (2012) *WISIS Forum* 2.

3 Cole *et al* (note 1 above) 3.

2.2. The Stanford Proposal

The need for effecting international co-operation in dealing with CyberCrime and CyberTerrorism were the subject of a conference sponsored by the Hoover Institution: the Consortium for Research on Information Security and Policy (CRISP) and the Centre for International Security and Cooperation (CISAC) at Stanford University (known as the 'Stanford Conference'). The theme of the conference was International Cooperation to Combat CyberCrime and Terrorism. The conference constructed a legal framework to address CyberCrime at a global level entitled *The Draft International Convention on CyberCrime and Terrorism*,[4] which seeks to protect transnational information infrastructure. Meeting at Standard in December 1999, members of government, industry, the NGO sector, and academia from many countries around the world, emerged with a clear consensus that underscored international co-operation rooted in a multilateral treaty, focusing on the criminal abuse of CyberSystems to help build the necessary cooperative framework.[5]

The Stanford conference reaffirmed CyberCrime as a transnational phenomenon, and articulated the need for a transnational response through multilateral legal instruments. The need for a multilateral convention was premise on the reality that CyberCriminals exploit weaknesses in the law and enforcement practices of states. As a result, States are exposed to dangers that are beyond their capacity unilaterally or bilaterally to respond. Orji confirms that the draft recognises the increasingly growing reliance and dependence of persons and governments globally on the reliable, secure information infrastructure.[6] It is a matter of common cause that the speed and technical complexity of Cyber activities requires pre-arranged, agreed procedures for co-operation in investigating and responding to threats and attacks.[7]

---

4 Sofaer AD *et al* 'A proposal for an International Convention on CyberCrime and Terrorism (2000) *Stanford University Centre for International Security and Cooperation* 25-37.

5 Sofaer *et al* (note 4 above) 13.

6 Orji UJ *CyberSecurity Law & Regulation* (2012) Wolf Legal.

7 Sofaer AD & Goodman SE 'CyberCrime and security: The transnational dimension' (2001) *The Transnational Dimension of CyberCrime and Terrorism* 1-34.

The Stanford conference concurred that a multilateral convention ensured that all state parties adopt laws that:

1. Make dangerous Cyber activities criminal;
2. Enforce those laws, or extradite criminals for prosecution by other States;
3. Co-operate in investigating criminal activities and provide usable evidence for prosecutions; and that the States
4. Participate in formulating an agreement to adopt and implement standards and practices that enhance safety and security.

The draft International Convention on CyberCrime and Terrorism is designed to encourage universal recognition of basic offences in CyberSpace and universal agreement to cooperate in investigating, extraditing, and prosecuting perpetrators with a focus on individuals to the exclusion of state conduct undertaken for public non-commercial purposes, including activities undertaken by military forces of the state[8] Eleven offences covered in the draft relate to interfering with the function of a CyberSystem, CyberTrespass, tampering with authentication systems, interfering with data, trafficking in illegal CyberTools, using CyberSystems to further offences specified in other treaties and targeting critical infrastructures. [9]

To ensure global monitoring of compliance as well as protection of transnational infrastructures, the draft Convention makes provision for an International Agency for Information Infrastructure (AIIP). The transnational agency's mandate is to construct a platform and provide the forum for international discussion, ongoing response to technological developments, and technical assistance to developing countries. Operationally and structurally, the International Agency is model after the International Civil Aviation Organisation (ICAO) and the International Telecommunications Union (ITU).[10]

The Stanford draft proposal makes clear that member States would have no duty to act in any manner that might infringe upon the privacy or other human rights of any individual or entity as

8 Orji 2012 (note 6 above) 183.

9 Article 3 of the Stanford Draft Convention.

10 Article 9(3) of the Stanford Draft Convention.

defined by the law of that state. To ensure compliance with this commitment to protecting sovereignty, member States agree to refuse to cooperate with investigations and prosecutions they might consider unfair or inconsistent with national policies.[11] Further, the draft Convention proposed establishing within any international CyberSecurity entity created by agreement, a Committee of Experts tasked with following and reporting on the protection of privacy and human rights, to serve as a forum for ongoing exposure and debate.

2.3 Global Protocol on CyberSecurity and CyberCrime: The Draft Code for Peace and Security in the CyberSpace

In 2009, a Draft Code on Peace and Security in the CyberSpace was initiated. At the centre of this initiative to realise peace and security in the CyberSpace, was a publication by Ghernaouti-Hélie and Schjølberg, who argue for the recognition of the CyberSpace through a Global Protocol that accords similar respect as the Kyoto Protocol – an international agreement linked to the United Nations Framework Convention on Climate Change.[12] The Global Protocol on CyberSecurity and CyberCrime[13] should be seen as a truly global approach which, when finalised, would create a safer transacting space by reducing risks and threats in the CyberSpace. The authors propose the establishment of crimes against peace and security in the CyberSpace as crimes under international law, notwithstanding that they may be punishable under domestic law.[14]

The Global Protocol on CyberSecurity and CyberCrime, the authors argue, would contribute to a better understanding of all aspects of CyberSecurity through the creation of 'an age of interdependence where each nation's security is also dependent on the actions of the other nations of the world'.[15] Furthermore, the Global Protocol would:

---

11 Sofaer A, Clark D & Diffie W 'CyberSecurity and international agreements' (2009) *National Research Council, Proceedings of a Workshop on Deterring Cyber-attacks* 195.

12 United Nations Framework Convention on Climate Change *Kyoto Protocol* (1997) 19.

13 Schjølberg S & Ghernaouti-Hélie S 'A global protocol on CyberSecurity and CyberCrime' (2009) *CyberCrimelaw.Net*.

14 Orji 2012 (note 6 above) 133.

15 Ghernaouti-Hélie (note 2 above) 1.

a. Facilitate the development and deployment of measures to help increase resilience to the impacts of CyberThreats and the effectiveness of international cooperation;
b. Reposition and define an appropriate CyberSecurity culture to develop efficient measures for raising awareness among the population;
c. Aggressively assist developed and less developed countries to extend an inclusive Information Society by reducing the security digital divide; and
d. Develop capacities to enforce and enhance peace and security in CyberSpace and in real life.
e. Provide legal mechanisms for combating CyberCrime in relation to phishing, botnets, spam, identity theft, crime in virtual worlds, terrorist use of internet, and massive and coordinated cyber-attacks against information infrastructures.[16]

The Draft Code for Peace and Security in the CyberSpace profiles 3 (three) strategic thrusts: The first being the principles underpinning a Global Protocol on CyberSecurity and CyberCrime, which focused on substantive criminal law that underscores the implementation of Articles 2–9 of the Council of Europe Convention on CyberCrime (CoECC).

Secondly, it further requires countries to establish substantive criminal law provisions against phishing, spam, identity theft, and preparatory acts prior to, as well as attacks already conducted to critical information infrastructure.

In addition, the Code's procedural provisions establish procedures necessary for conducting investigations and prosecution as provided for in Articles 14-22 of the CoECC. The draft Code also underscores the need for international co-operation and co-ordination in investigation and prosecution, thus embracing articles 23-25 of the CoECC. Proposals to inform a preliminary CyberCrime model law embraces the provisions of the CoECC, but further creates provisions for procedural law and the explanatory commentaries on the general provisions.[17]

---

16 Ghernaouti-Hélie (note 2 above) 1.

17 Schjølberg S & Ghernaouti-Hélie S *A Global Treaty On CyberSecurity And CyberCrime*: *CyberCrime Law* (2011) 97.

2.3. The Council of Europe Convention on CyberCrime (CoECC)

The Council of Europe Convention on CyberCrime (CoECC) was adopted on 8 November 2001 and opened for signatures at a Conference in Budapest. It remains an historic milestone in the legal control of CyberCrime and has been ratified by 48 states and entered into force on 1 July 2004.[18] Whilst Russia has neither signed nor ratified the CoECC, South Africa signed, but has not ratified the treaty. However, the Convention's substantive provisions have been captured in South Africa's legislative frameworks, notably Section 86-87 of the ECTAct,[19] the Copyright Act[20] and the Films & Publications Act.[21] This Convention, which is commonly referred-to as the Budapest Convention, breaks new ground by decisively dealing with computer-related crimes and economic crimes. The Convention also aims to achieve three outcomes at a global level. These are:

1. Reducing friction through harmonisation and approximation of CyberCrime legislation by providing law enforcement with the tools and new investigative measures;
2. Facilitating co-operation through minimum rules in a more complex framework; and
3. Striving for effective implementation.[22]

The Convention criminalises conduct against the integrity, availability and confidentiality of computer systems as well the misuse of computer systems.[23] Orji attests to the technological neutrality and futuristic posture posited by the Convention, providing a platform for international collaboration across states, apart from the distinctive foresight feature of the Convention portrayed in the administrative provisions.[24] Upon signing or ratifying the Convention, States agree to ensure that their municipal laws criminalise the conduct prohibited by the substantive

---

18 Schjølberg S & Ghernaouti-Hélie S 'A global protocol on CyberSecurity and CyberCrime' (2009) *CyberCrimelaw.net*.

19 Electronic Communications and Transactions Act 25 of 2002.

20 Copyright Act 98 of 1978.

21 Films and Publications Act 65 of 1996.

22 Schjølberg & Ghernaouti-Hélie (note 18 above).

23 Snail kaMtuze S 'CyberCrime in South Africa: Hacking, cracking and other unlawful online activities' (2009) 1 *Journal of Information, Law and Technology* 10.

24 Orji 2012 (note 6 above) 119.

provisions of the Convention as well as establish systems and procedures to ensure investigation and prosecution of prohibited conduct.[25]

The Convention deals with the substantive law provisions that provide for the criminalisation of computer related offences, content related offences and copyright related offences. Furthermore the treaty provides for procedural matters to the balance between protection of human rights and providing computer data necessary for prosecutions. Lastly it provides for international cooperation to facilitate the investigation and prosecution of criminal offences, including extradition for trial in member country.[26]

South Africa has complied with the substantive provisions of the Treaty through the Section 87 to 89 of the ECT Act[27] that criminalises the computer related crimes, whilst the Films Publication Act[28] criminalise the content related crimes and the copy right related crimes are provided for in the Copyright Act.[29] The CyberCrime and CyberSecurity legislative framework will enable South Africa to comply with the procedural as well the international cooperation provisions. However, the geopolitical and trade relations strategic positioning within BRICS will render the ratification of the aforementioned Convention impossible.

2.4. The European Union (EU) Directive

In further strengthening the security of information systems within the EU, the European Commission in 2005 sponsored a proposal[30] for a European Union Directive focusing on data retention through enforcing a duty on internet service providers to retain data traffic necessary for

25 Orji 2012 (note 6 above) 119.

26 Papadopoulos, S & Snail, SL *Cyberlaw @ SA III: The law of the Internet in South Africa* (2012) Van Schaik: Pretoria (2012) 102.

27 Act 25 of 2002

28 Act 65 of 1996

29 Act 78 of 1978

30 Proposal for a Council Framework Decision on Attacks against Information Systems.

the identification of criminal actors in CyberSpace. The proposal was adopted by the EU.[31] The EU Directive provides for the criminalisation of instigating, aiding and abetting and attempting to commit one of the three offences described above. The sentences entail a minimum penalty of at least between one and three years of imprisonment for illegal system interference and illegal data interference. The Directive also provides for aggravating circumstances, at least between two and five years of imprisonment for offences committed within the framework of a criminal organisation. The Directive further underscores the duty of Internet Service Providers (ISPs) to retain traffic data necessary for identifying criminal actors in the CyberSpace.[32]

The efficacy of the legal instrument is compromised by the current realities that the majority of countries globally with the highest number of internet users have not signed or ratified the Convention and the pace of ratification is relatively slow in Africa, compared to other international legal instruments. Cassim asserts that at a global level, implementation is even lower.[33] Notwithstanding its uncertain global reach, the CoECC shows a remarkable indirect impact in influencing domestic legislation and as such, is recognise as a worldwide benchmark for CyberCrime legislation.[34]

2.5. The International Telecommunications Union (ITU)

The International Telecommunications Union (ITU) is a specialised agency of the United Nations (UN) responsible for playing a focal role in the development of the global Information and Communication Technology footprint. It serves as a global focal point for governments and the organised private sector in the development and standardisation of a telecommunications network and services and the promotion of initiatives directed at protecting the Information Society.

---

31 Orji 2012 (note 6 above) 120.

32 Orji 2012 (note 6 above) 121.

33 Cassim F 'Formulating specialised legislation to address the growing spectre of CyberCrime: A comparative study' (2009) 12:4 *PER: Potchefstroom Electronic Law Journal* 36-79.

34 Cassim (note 33 above) 43.

The UN General Assembly Resolution[35] provides a legal basis for the ITU to take the lead role in co-ordinating the robust, multi-stakeholder participation to create a framework for international co-operation to promote CyberSecurity for the enhancement of confidence and security in the Information Society.[36]

A Global Security Agenda (GSA) was launch by the ITU whose mandate is to provide a global framework to inform dialogue and international co-operation through co-ordination of international responses to CyberSecurity as well as enhance confidence and security. In delivering on this mandate, and as part of advancing a CyberSecurity posture, the GSA has argued for the development of a CyberCrime legislation that is globally applicable and consistent with existing national and regional legislative measures.[37]

The (ITU) defines CyberSecurity as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the Cyber environment and the 'organisation and user's assets'. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the Cyber environment.[38]

CyberSecurity strives to ensure the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the CyberEnvironment. The general security objectives comprise of Availability, Integrity (which may include authenticity and non-repudiation) as well as Confidentiality.[39]

---

35 United Nations A/RES/56/183 (2002) available at: *https*://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002.pdf (accessed: 23 October 2017) 2.

36 United Nations (note 35 above).

37 Orji 2012 (note 6 above) 107.

38 Davenport T 'Submarine Cables, CyberSecurity and International Law: An InterSectional Analysis (201) 12:43 *Catholic University Journal of Law & Technology* 201-242.

39 Orji UJ 'Multi-lateral legal responses to cyber security in Africa: Any hope for effective international cooperation?' (2015) *Cyber Conflict: Architectures in CyberSpace (CyCon)* 7th International Conference on IEEE 107.

2.6. BRICS Framework on Ecommerce

E-commerce was listed formally among the priorities of the BRICS Trade and Investment Cooperation Frame, which was endorsed by the BRICS Trade Ministers in 2013.

Driven by the outcome of systematically and effectively advancing the BRICS E-commerce cooperation and directly contribute to the goal of building a closer economic partnership, the BRICS members developed the Framework for BRICS E-commerce Cooperation (the Framework) to promote current and future initiatives in this sphere. It is envisaged that this Framework could establish a process through which the BRICS countries could further cooperate in trade and investment areas based on a spirit of trust and partnership.[40]

Framework promotes cooperation in cross-border e-commerce so as to align with global cross-border E-commerce and accelerate the development of BRICS E-commerce industry and market as well as address hindrances to utilisation of e commerce as a means to promote cross border trade. Such cooperation would be achieved through promotion of studies on Policies that drive cross border Ecommerce, strengthening partnership between public and private sectors to promote capacity building; development of favourable Ecommerce cross border Infrastructure environment.[41]

BRICS Framework on E-commerce has profiled CyberCrime and CyberSecurity as a priority. With Regards to Information Security and CyberSecurity the Framework proposes the following strategic interventions

(i) Development of mutually acceptable definitions of CyberSecurity and critical information infrastructure and CyberCrime

40 Draft Framework for BRICS E-commerce Cooperation (Proposed by Russia and China).

41 Draft Framework for BRICS E-commerce Cooperation (note 40 above) 3-4.

(ii) Develop harmonised Policy for CyberSecurity that responds to fundamental rights, freedom of expression, personal data and privacy, promote multi stakeholder approach to governance, shared responsibility for CyberSecurity

(iii) Develop strategic initiatives that profile achieving cyber resilience, reduce cyber threats, Promoting Public Private Partnerships for ensuring CyberSecurity.[42]

2.7. The African Union (AU) Convention on CyberSecurity and Data Protection

Before the adoption of the African Union (AU) Convention, some efforts on data protection had been achieve. These efforts commenced in 2011 with the Draft African Union Convention on the Establishment of a Credible Legal Framework for CyberSecurity in Africa (AUCLCS)[43] a draft which was subsequently reviewed in 2013. Snail kaMtuze in his dissertation[44] argues that the AUCLCS which gives substance to a Resolution of the last session of the Assembly of Heads of State of Governments of the African Union, with specific purpose on harmonising African Cyber Legislations on E-commerce personal data protection, CyberSecurity promotion and CyberCrime control, profiles CyberSecurity and CyberCrimes provisions on as opposed to enablement and regulation of E-commerce in Africa.

The second draft was the African Union Convention on Confidence and Security in CyberSpace. The absence of consultation during the drafting of these legal instruments was at the core of the criticism levelled against them by the private sector, civil society organisations and privacy advocates.[45]

---

42 Draft Framework for BRICS E-commerce Cooperation (note 40 above) 5.

43 African Union Commission, Draft African Union Convention on the Establishment of a Credible Legal Framework for CyberSecurity in Africa (2011) *African Union Commission*.

44 Snail kaMtuze S *A Comparative Review of Legislative Reform of Electronic Contract Formation in South Africa* (2015) 83.

45 Abdulrauf LA & Fombad CM 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8:1 *Journal of Media Law* 70-76.

Nigeria tops the chart in Africa as the country with the highest number of internet users.[46] Africa also hosts four of the ten countries with the highest CyberCrime levels in the world.[47] To augment the inadequacy of Cyber legislations in Africa, the AU Convention on Security in CyberSpace and Personal Data Protection (AUCSCPDP)[48] was sign on 27 July 2014 in Malabo, Equatorial Guinea. The Convention seeks to harmonise and strengthen African Cyber Legislations on electronic commercial organisations, personal data protection, CyberSecurity promotion and CyberCrime control. It also sets broad guidelines for incrimination and repression of CyberCrime. The African Union has fifty-four-member States.[49]

Unlike the Council of Europe Convention on CyberCrime (CoECC),[50] the AUCSCPDP[51] relates directly to the challenges that prevail in the African context by:

1. Prohibiting identity flexibility and associative anonymity in e-commerce;
2. Outlawing spam (unsolicited electronic commission);
3. Addressing the use of encryption in CyberCrime; and
4. Prohibiting key forms of online discrimination.

While all these challenges currently constitute Africa's biggest vulnerability in CyberSpace, the AUCSCPDP further provides for independent expert vulnerability testing of internet services; an

46 Internet World Stats (note 5 above).

47 Abdulrauf & Fombad (note 45 above) 70.

48 African Union Convention on Cyber Security and Personal Data Protection. Date of adoption 27 June 2014. Date of last signature: 04 July 2017 available at: https://au.int/en/.../african-union-convention-cyber-security-and-personal-data- protection (accessed: 23 October 2017).

49 Orji UJ 'Regionalising CyberSecurity governance in Africa: An assessment of responses' (2016) *Securing CyberSpace* 203.

50 Budapest Convention on CyberCrime (ETS 185) available at: https://www.coe.int Conventions (accessed: 23 October 2017).

51 African Union Convention on Cyber Security and Personal Data Protection EX.CL/846(XXV) available at: https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf (accessed: 23 October 2017).

initiative that introduces an essential process through which Africa's ICT development will proactively incorporate online security measures.[52]

According to Cassim, the threefold provisions permitting non-consensual interference with private, personal and sensitive data; the interference with online traffic or content data; and the issuance of search and seizure warrants that permit inappropriate and broad ongoing investigation. The fact that judges will have to be mandated will inadvertently undermine the values that the AUCSCPDP is seeking to protect, such as the rights to privacy and freedom of expression.[53]

2.8. African Intergovernmental Organisation

Regional Economic Communities (RECs) are the sub-regional groupings that champion sub-regional initiatives and were originally not establish to 'foster human rights, but to facilitate a process of economic convergence through closer economic and financial cooperation and harmonisation policies and programmes'.[54] With regard to data protection prior to the AU Convention, four RECs had taken concerted actions by adopting legal instruments to address the matter.[55] Several African intergovernmental organisations were established to develop frameworks for CyberSecurity. With time however, human rights became a critical aspect of their mandates.

In response to the AU initiative, the Economic Community of West African States (ECOWAS) adopted a Directive on CyberCrime.[56] The Directive provides for offences specifically related to ICT, which include fraudulent access, remaining in computer systems, incorporating traditional offences into ICT offences as well as provision of sanctions for CyberCrime offences. An

52 Orji (note 6 above) 105-118.

53 Cassim (note 33 above).

54 Abdulrauf & Fombad (note 45 above) 73.

55 Abdulrauf & Fombad (note 45 above) 73.

56 ECOWAS Directive on CyberCrime and related texts on Cyber Legislation available at: https://ccdcoe.org/sites/default/files/.../ECOWAS-110819-FightingCyberCrime.pdf(accessed: 23 October 2017).

implementation evaluation in Africa revealed that the execution of this directive within ECOWAS has recorded some progress, given its binding nature on the states and measured against the fundamental CyberSecurity objectives that underpin human, economic and national security.[57] Further, ECOWAS adopted a Supplementary Act,[58] which is annexed to the treaty and enforce through the ECOWAS Court of Justice. The Supplementary Act[59] on Personal Data Protection seeks to provide for protection of personal data within the Community as well as establish mechanisms relating to personal data protection, processing, transmission, storage and use.[60]

The Common Market for Eastern Africa and Southern Africa (COMESA) in 2011 established a Model CyberCrime Bill[61] to provide for a uniform framework to serve as guide for the development of CyberCrime laws across member States. Because the Bill does not establish any binding obligation among member states to criminalise CyberCrime, its implementation evaluation revealed patchy and uneven levels, thus presenting a risk to harmonisation across multilateral arrangements. However, the Model Law does not have a binding effect.[62]

The East African Community (EAC) has developed a Legal Framework for CyberLaws (I and II),[63] with a mandate is to harmonise law reforms across partners as well as reflect international best

---

57 Cole *et al* (note 1 above) 4-7.

58 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS ('ECOWAS Supplementary Act') adopted 16 February 2010.

59 ECOWAS Directive and related texts presented at CoE Regional Conference on Cyber legislation 2017 available at: https://rm.coe.int/-3148-3-2-3-nigeria-ecowas-o-3-auc-moctar.../1680748652 (accessed: 23 October 2017).

60 Makulilo AB 'Data protection regimes in Africa: Too far from the European 'adequacy' standard?' (2013) 3:1/1 *International Data Privacy Law* 42–50.

61 Official Gazette of the Common Market for Eastern and Southern Africa (COMESA) Vol. 16 No. 2 (15 October 2011).

62 Cole *et al* (note 1 above).

63 Draft EAC Legal framework for CyberLaws (2008) available at: <www.eac.int/index.php?option=com_docman&taskdoc_view&gid=632&Itemid=148>; Framework for Cyberlaws, Phase II (UNCTAD, 2011) <http://r0. unctad.org/ecommerce/docs/EAC_Framework_PhaseII (accessed: 23 October 2017)..

practise. Unlike the ECOWAS Supplementary Act, these are not enforceable through the Court of law.[64]

African countries have been criticised for dealing inadequately with CyberCrime. This criticism is cause by the inadequacy of the personnel and infrastructure within the law enforcement agencies. The private sector is also lagging behind in curbing CyberCrime for the same reasons.[65] In addition, the preoccupation of African countries with pressing social issues such as poverty, the AIDS crisis, the fuel crisis, political instability, ethnic instability and traditional crimes such as murder, rape and theft, have also contributed to the lag in the fight against CyberCrime.[66] Another point is that combating internet crime and corruption demands mutual legal and technical assistance that is rooted in partnerships.

Besides South Africa, the initiatives by African countries in addressing CyberCrime, although at various maturity levels, are worthy of mention. Kenya has enacted Cyber legislation to combat CyberCrimes.[67] Botswana has presented a Bill on CyberCrime and Computer-Related Crimes to their National Assembly, which will go for a third reading before it is sign into law.[68] The Economic Community of West African States (ECOWAS) is considering the implementation of ICT policy and legislation, access and interconnection regulation, the granting of universal access and the provision of guidelines for gradual transition to open markets. Lack of IT knowledge by the public coupled with the absence of suitable legal frameworks to deal with CyberCrime at national and regional levels has affected the response of African Countries to CyberCrime.[69]

64 Abdulrauf & Fombad (note 45 above) 71.

65 Cole *et al* (note 1 above) 25.

66 Cole *et al* (note 1 above) 26-27.

67 Orji 2016 (note 49 above) 207.

68 Bill on CyberCrime and Computer-Related Crimes.

69 Cole *et al* (note 1 above) 27.

2.9. The SADC Model Laws

The Southern African Development Community (SADC) with its Data Protection Model Law[70] also presented a response to a sub-regional initiative prior to the AU Convention. The objective of this Model Laws, among others, is to 'create a uniform system in a given area in order to create a safe environment for citizens'.[71] In March 2012, the SADC also adopted a Model Law on Computer Crime and CyberCrime[72] to serve as a guide for the development of CyberSecurity laws in SADC member states. The Model Law does not impose any binding obligations on members to establish CyberSecurity laws neither does it establish provisions and protocols to guide the development of international cooperation regimes in member states nor establish any international cooperation obligations on member states. In order to creatively deal with this legislative lacuna, Orji argues that member states that have used the Model Law as framework for developing their CyberSecurity laws may rely on the SADC Protocol on Mutual Legal Assistance in Criminal Matters[73] and the Protocol on Extradition[74] to obtain international CyberSecurity cooperation from other member states.[75] Thus, the Model Laws seek to ensure harmonisation of data protection in member states as well as prosecution of CyberCrime. One of the factors that made this necessary was the porousness and permeability of traditional borders between countries. The Model Laws gives prescriptive guidance to member states in enacting their data protection and CyberCrime legislation.[76] Orji further presents the SADC situational analysis of CyberSecurity legislation, which in 'January 2016, registered six(6) SADC members states namely, Angola, Democratic

---

70 Data Protection: Southern African Development Community (SADC) Model law available at: https://www.itu.int/en/ITUD/Projects/ITU-ECACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_pro tection.pdf (accessed: 23 October 2017).

71 Data Protection: Southern African Development Community (SADC) Model law <www.itu.int/en/ITU-D/Projects/ITUECACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf (accessed on 23 October 2017).

72 SADC Model Law on Computer Crime and CyberCrime Version 2.0 adopted on 02 March 2012.

73 SADC Protocol on Mutual Legal Assistance in Criminal Matters (Luanda 3 October 2002).

74 SADC Protocol on Extradition (Luanda, 3 October 2002).

75 Orji (note 59 above) 207.

76 Snail kaMtuze S L & Matanzima S 'CyberSecurity in Africa: Cyberlaw' (2014) 14:9 *Without Prejudice* 88-9.

Republic of Congo, Lesotho, Malawi, Mozambique and Swaziland which did not have CyberCrime laws'.[77] Like EAC Framework, the SADC Model Law, has a non-binding character. Given the human rights attribute that characterise the regional legal instruments, the non-binding character waters down any potential influence it may have in effective human rights protection.[78]

2.10. The Draft International Convention on CyberCrime and CyberTerrorism

The quintessentially transnational character of CyberCrime factors cross-jurisdictional collaborations and agreements to guide enforcement of transnational responses. Such collaboration shall encourage universal recognition of basic offenses in CyberSpace and universal agreement to cooperate in investigating, extraditing, and prosecuting perpetrators. As such multilateral Convention International Convention on CyberCrime and CyberTerrorism[79] remains an essential global instrument to give substance to the cross jurisdictional collaborations. Orji points out that the 1999 Stanford Conference sponsored the draft International Convention to enhance the protection against CyberCrime and terrorism.[80] The draft Convention proposed the establishment of an International Agency for Information Infrastructure Protection (AIIP). Further, the Draft Convention enjoins member states to criminalise the conduct prohibited by the draft Convention. Its scope of application does not extend to any state's conduct undertaken for public non-commercial purposes, which includes activities conducted by the military in the protection of territorial integrity.

The Draft Convention provides for the definition of CyberCrime, CyberTerrorism, CyberSystems, critical infrastructure and transnational information infrastructure. In addition, the draft Convention also provides for:

1. The creation of offences against CyberSystems and critical infrastructures;
2. The enactment of domestic laws by state parties;

---

77 Orji (note 6 above) 207-210.

78 Abdulrauf & Fombad (note 45 above) 75.

79 Sofaer AD *et al* 'A proposal for an international convention on cyber-crime and terrorism' (2000*) Stanford University, Centre for International Security and Cooperation* 25-39.

80 Orji (note 6 above).

3. The establishment of jurisdiction in respect of offences created by the Convention,
4. The promotion of mutual legal assistance and co-operation in law enforcement; as well as
5. The establishment of an Agency for Information Infrastructure Protection AIIP.[81]

The nature and culture of the Cyber world demand that multilateral responses, both voluntary and legally mandated to CyberCrime and CyberTerrorism are fore-grounded by maximised private-sector participation and control, as well as to ensure that privacy and other human rights are not adversely affected.

The Draft International Convention to Enhance Protection from CyberCrime and Terrorism profiles Mutual national legal assistance is key for successful prosecution as well as provides for Extradition of individual found committing CyberTerrorism. It is critical to underscore that character of the International Convention that its application excludes political means. Inherent in the Convention is the introduction of a new concept of Cyber deterrence as an attribute of CyberWarfare which is rooted on three pillars CyberResilience, CyberAttribution as well as development of CyberOffensive and CyberDefensive capabilities.[82]

2.11 The NATO Convention

The North Atlantic Treaty Organisation (NATO) was one of the first international organisations to redefine its CyberDefence policy that focuses on safeguarding critical information infrastructure. Through its 2008 response to Cyberattacks against Estonia, the NATO CyberDefence Policy led to the establishment of a NATO Co-operative CyberDefence Centre of Excellence in Talim. The Talim frameworks provides the rules of engagement during CyberWarfare and assist member states to achieve collective self-defence in CyberSpace by defying the countering threats of CyberWarfare and CyberTerrorism.[83]

---

81 Orji (note 6 above) 194.

82 Cohen A 'CyberTerrorism: Are we legally ready' (2010) 9 *J Int'l Bus & L* 1.

83 Orji (note 6 above) 131.

The 2017 edition of the Talim Framework covers a full spectrum of international law as applicable to CyberOperations, ranging from peacetime legal regimes to the law of armed conflict. The analysis of a wide array of international law principles and regimes that regulate events in CyberSpace includes principles of general international law, such as the sovereignty and the various bases for the exercise of jurisdiction. The law on state responsibility, which includes the legal standards for attribution, is examined at length. Additionally, numerous specialised regimes of international law, including human rights law, air and space law, the law of the sea, and diplomatic and consular law are examined within the context of CyberOperations.[84]

To keep pace with the rapidly changing threat landscape and maintain a robust CyberDefence, NATO adopted an enhanced policy and action plan, which was endorse by Allies at the Wales Summit in September 2014. The policy profiles CyberDefence as part of the Alliance's core task of collective defence, confirms that international law applies in CyberSpace and intensifies NATO's co-operation with industry, the top priority being i the protection of the communications systems owned and operated by the Alliance.[85] Leaders of NATO adopted a CyberDefence Pledge at the NATO Summit in Warsaw in July 2016, which profiles funding CyberDefence as a top priority and underlined their commitment to enhance and strengthen the CyberDefences of national infrastructures and networks as a matter of priority.[86]

At Warsaw, NATO's mandate was re-affirmed, which recognises CyberSpace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. As most crises and conflicts today have a Cyberdimension, treating CyberSpace as a domain will enable NATO to better protect and conduct its missions and operations.

---

84 NATO Cooperative Cyber Defence Centre of Excellence 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' (2013) *Cambridge University Press* available at: https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual (accessed: 3 August 2017).

85 NATO (note 84 above).

86 NATO Review 'Spending for success on cyber defence' available at: http://www.nato.int/docu/review/2017/Also-in-2017/nato-priority-spending-success-cyber-defence/EN/index.htm (accessed: 3 August 2017).

Eneken Tikk presents 4 (four) dimensions that underpin CyberSecurity organisational architecture as Internet Governance, CyberCrime, CyberTerrorism and CyberWarfare as triangulated through the responsibility matrix and CyberSecurity focus across various multilateral institutions.[87] Tikk asserts that international organisations possess different quantitative and qualitative abilities to improve global CyberSecurity.[88] Strategic positioning within international CyberSecurity landscape requires contextualisation of responses sponsored against CyberConflicts and national security relevant incidents as well as CyberWarfare through the prism of the CyberThreats that are being addressed.

The analysis of the four dimensions of CyberSecurity reveal that while Internet Governance and fighting CyberCrime are the focus of several major international organisations, CyberWarfare falls under the authority of only the UN and NATO. While collective self-defence in case of a 'Cyber armed attack' would be resolved through NATO, from a legislation and policy viewpoints.[89]

2.12 Conclusion

The enforceability of laws against CyberOffences enacted at the national level becomes complicated by the source, object, or path of an attack that has its physical *nexus* in more than one country. The main procedural difficulty that emerges, exclusive of the absence of territorial *nexi* in CyberCrimes committed via CyberSpace, is that of the plurality of national connections, and the accompanying jurisdictional claims.[90]

The porousness of the CyberSpace underpins the need for responsive and timely multilateral legal responses to CyberSecurity. CyberCriminals traverse electronic CyberSpace borders with great ease and with few repercussions because jurisdiction remains a major hurdle in enforcing legislation. Each country, as dictated by its economic, human and national security posture,

---

87 Tikk E 'Global CyberSecurity: Thinking about the Niche for NATO' (2010) 30:2 *SAIS Review of International Affairs* 105-119.

88 Tikk (note 87 above) 108.

89 Tikk (note 87 above) 107.

90 Putnam TL & Elliott DD *International Responses To Cyber Crime: Transnational Dimension of Cyber Crime and Terrorism* (2001) 61.

enforces a different standard of tolerance for CyberCrime, which requires a flexible global regulatory system to maintain each nation's sovereignty. In striving for multi-jurisdictional harmonisation, however, the problem of legislative 'spill-over' from territorial regulation of the Internet is inevitable. The problems of uncertain jurisdiction and overlapping regulations render it desirable to adopt uniform and jurisdictional standards by international treaty. Such an international treaty would protect transnational organisations and companies from liability that emanate from disparate domestic legislative arrangements.

Within the continent of Africa, the developmental trajectory reflects that notwithstanding the delayed adoption at AU level of the AUCSCPDP in June 2014, some African states have already established national legal and policy frameworks for CyberSecurity, while many others are developing such framework. These pro-active policies include the ECOWAS Directive on Fighting CyberCrime adopted in August 2011, the COMESA Model CyberCrime Law adopted in October 2011, and also within the SADC, the adoption of a Model Laws on Computer Crime and CyberCrime.

The drive for a multilateral system of governance at international level has been demonstrated by the translation of the spirit and provisions of the Budapest Convention in the Global Protocol on Peace and Security in the CyberSpace as well as the draft International Convention to enhance Protection from CyberCrime and Terrorism. The strengthening of the criminal substantive provisions demonstrates the commitment to the collective response to curb CyberCrime, shield participants of the global Information Society from all forms of infrastructure and cultural vulnerabilities and create a safe and peaceful CyberSpace.[91]

[91] Sofaer AD & Goodman SE '*CyberCrime and Security: The Transnational Dimension of CyberCrime and Terrorism* (2001) 19-21.

CHAPTER 3: MAKING A CASE FOR THE SOUTH AFRICAN CONTEXT

3.1. Introduction

This Chapter presents the evolution of the legislative framework that aims at combating or criminalising CyberCrimes and to promote security in the CyberSpace. Most of the so-called traditional crimes such as murder, rape, theft, malicious injury to property and housebreaking originate from the South African Common Law, namely Roman-Dutch Law. These traditional crimes deal only with tangibles whereas IT crime or CyberCrime deals with intangibles; a situation that has fuelled the perception that Common Law cannot effectively deal with IT crime.[1]

Grobler *et al*[2] argues that one of the problems associated with the technological revolution is that the CyberSpace is full of complex and dynamic technological innovations that are not well suited to any lagging administrative and legal system. A further complication is the lack of comprehensive and enforceable treaties facilitating international co-operation with regard to CyberCriminality as well as CyberSecurity and CyberDefence. The result is that many developing countries in particular, are neither not properly aware, nor well prepared, or adequately protected by both knowledge and legislation in the event of a CyberAttacks on a national level.[3] Even when such threats are forecasted, the prolonged consultative process to inform legislative processes, render *ex-post facto* solutions and counter-measures.

---

1 Snail kaMtuze S 'CyberCrime in South Africa: Hacking, cracking, and other unlawful online activities' (2009) 1 *Journal of Information, Law and Technology* 1.

2 Grobler M, van Vuuren JJ & Zaaiman J *Preparing South Africa for CyberCrime and CyberDefence* (2013) 32.

3 Grobler *et al* (note 2 above).

3.2. Common Law

As has been alluded to earlier, the crimes that occupy the CyberSpace are quite new and Common Law does not provide room for adjudication of these crimes. Snail kaMtuze asserts that prior to the promulgation of the Electronic Communications and Transactions Act hereafter (ECT),[4] Common Law and statutory law could apply to crimes of defamation, indecency, CyberSmearing, CyberFraud, contempt of court and theft, with limitations as applied to online crimes.[5]

Before the commencement of the ECT Act[6] Common Law and statutory law applied to online forms of offences such as indecency (child pornography), fraud (CyberFraud) and *crimen inuria* (CyberSmearing). However, the Common Law was ineffective in addressing crimes such as theft, extortion, spamming and phishing.[7] Invoking Common Law, however, has its limitations and narrows significantly when dealing with online crimes involving assault, theft, extortion, spamming, phishing, treason, murder, breaking and entering into premises with the intent to steal and malicious damage to property.[8]

Snail kaMtuze asserts that crimes such as the possession and distribution of child pornography could be prosecuted in terms of Section 27(1) and Section 28 of the Films and Publications Act[9] whilst illegally making, producing and distributing were covered in the Copyright Act.[10]

3.3. Provisions of the Electronic Communications and Transactions Act 25 of 2002

In 2002 the ECT Act was enacted and, amongst other things, repealed the Computer Evidence Act(CEA). The ECT Act is largely based on the United Nations Commission on International

---

4 Act 25 of 2002

5 Snail kaMtuze (note 1 above) 1.

6 Act 25 of 2002.

7 Snail kaMtuze (note 1 above) 1.

8 Snail kaMtuze S & Madziwa S 'Hacking, cracking and other unlawful online activities: Communications law' (2008) 8:2 *Without Prejudice* 30-31.

9 Act 65 of 1996.

10 Act 98 of 1978.

Trade Law (UNICTR[11]AL'), Model Law on Electronic Commerce with Guide to Enactment 1996 ('Model Law').

The ECT Act is an omnibus Act that deals with many different provisions regarding transactions and communications that are concluded electronically.[89] The Act accommodates developments in technology by creating a new type of evidence that is related to information represented in any electronic form. The Act has done away with concepts such as computer printouts,and provides for the legal recognition of 'data' and 'data messages' as electronic evidence. The ECT Act excludes the validity of certain types of electronic transactions, such as a bill of exchange, will or codicil, long-term lease or alienation of immovable property agreement. The Act also does not limit the operation of any law that regulates, authorises or prohibits the use of data messages.[12] The ECTAct establishes Cyber inspectors

The ECT Act provides for the following:

1. The facilitation and regulation of electronic communications and transactions;
2. The development of a national E-strategy for the Republic of SA;
3. The promotion of universal access to electronic communications and transactions and the use of electronic transactions by SMMEs;
4. The provision for human resource development in electronic transactions;
5. The prevention of abuse of information systems; and
6. Creation of CyberCrimes as well as appointment as well as role definition of Cyber Inspectors;
7. Limitation of Liability of Service Providers;
8. The encouragement of the use of E-government services, and to provide for matters connected therewith.[13]

[11] UNCITRAL is a subsidiary of the United Nations General Assembly

[12] Gert Petrus van Tonder the admissibility and evidential weight of electronic evidence in South African legal proceedings: a Comparative Perspective,2013. 10

[13] Electronic Communications and Transactions Act 25 of 2002.

3.3.1. CyberCrimes

The ECT Act presents the first attempt to deal with computer and CyberCrime and takes its cue from the European Commission Convention on CyberCrime, referred to as the Budapest Convention. The countermeasures against CyberCrime are presented in Sections 85 to 89. Section 86(1) deals with unauthorised access to data criminalises unauthorised access to, interception of and interference with data and further adds two provisions that relate to prohibited actions. These relate to interference of as well as interference with unlawful access and modification of data including surveillance and monitoring of communication.[14]

Section 86(2) dealing with unauthorised interception of data prohibits unlawful modification of data by criminalising interference with data that would cause such data to be modified, destroyed, or rendered ineffective and thus address the creation and distribution of computer viruses. Section 86(3) provides for misuse of digital services and creates several offences for the utilisation of digital devices for unlawful purposes, and Section 86(4) dealing with utilisation of digital devices to overcome data security measures.[15]

Section 86(5) covers the Denial of Service (DOS), a provision that criminalises acts performed whose effect and functions slow or stop the lawful user from access the IT services. This Section criminalises unauthorised access, interception or interference of data with the intent to interfere with the systems, whereas Section 87 creates the statutory-related common crimes of extortion, fraud and forgery. The Act also criminalises unauthorised access to interception of or interference with data; computer-related extortion, fraud and forgery; and attempt, as well as aiding and abetting provided for in Section 88. Section 89 provides for criminal sanctions for crimes prohibited by Sections 37(3), 40(2), 58(2), 80(5), 82(2) or 86(1), (2) & (3) to a fine or imprisonment for a period not exceeding 12 months. A fine or imprisonment for a period not exceeding five years is levied for all offences in Section 86(4) or (5) or Section 87.

---

14 Van der Merwe DP (ed) *Information and Communications Technology Law* (2016)487.

15 Papadopoulos S & Snail kaMtuze S *Cyberlaw @ SA III: The Law of the Internet in South Africa* (2012) 343-344.

3.3.2. Extra territorial jurisdiction

With regard to jurisdiction, South African Courts are vested with jurisdiction in terms of Section 90, to try offences under the ECT Act[16] when:

(a) The offence was committed in the Republic;
(b) Any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;
(c) The offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or
(d) The offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

3.3.3. Protection of critical data and databases

Section 53 of the ECT Act provides for the declaration, classification, protection and management of information that is vital for protection of national security as well as the economic and social well-being of the citizens of South Africa. These critical data and databases relate to the critical information infrastructure. The ECTA defines critical data as data that is declared by the Minister in terms of Section 53. Orji argues that the scope of protection of these critical data and critical databases does not cover malicious conduct against these critical data and databases.[17]

3.3.4 Cyber Inspectors

To ensure monitoring of compliance with the provisions of the ECT Act, section 80- 84 provides for the appointment of Cyber Inspectors, the mandate , powers to inspect, search and seize as well as preservation of confidentiality.

---

16 Snail kaMtuze (note 1 above) 1.

17 Orji UJ *CyberSecurity Law and Regulation* (2012) Wolf Legal.418.

3.3.5. The ECT Act and its effect

The ECT Act focuses on definition as well as the protection of 'data', defined in Section 1 of the Act. Section 15 further provides for conditions for admissibility of data messages, which underscore reliability of manner of storage, generation and communication, reliability of admission, manner of maintenance of message, manner in which the originator is identified and other relevant factors. The Act thus creates a rebuttable presumption that data messages and/or printouts are admissible in evidence.

The Act deals comprehensively with CyberCrime as well as the introduction of an anti-cracking (anti-thwarting) and hacking law, which prohibits the selling, designing or producing of anti-security circumventing technology; e-mail bombing and spamming crimes of extortion, fraud and forgery as well as cites in instances where the ECT has not made any specific provisions for criminal sanctions, wherein Common Law will prevail. Crimes relating to money laundering and other financially related crimes are address in terms of the Prevention of Organised Crime Second Amendment Act[18] (POCAA) and Financial Intelligence Centre Act (FICA).[19]

The Act also provides for the recognition of Cyber Inspectors who are authorised to enter premises or access information regarding CyberCrime. This provision has not been enforced as yet, thus signalling regulatory implementation deficiencies'. Inadequacy of criminal sanctions in the ECT Act is further supplemented by the Regulation of Interception of Communications and Provision of Communications-Related Information[20] (the RICA), which prescribes harsher measures.

ECT Act, Promotion of Access to information Act 2 of 2000, as well as RICA , prohibit the unlawful interception or monitoring of data messages.

---

18 Act 38 of 1999.

19 O'Reilly K 'South African law coming to grips with CyberCrime: News' (2013) *De Rebus* 15.

20 Act 70 of 2002.

3.4. Promotion of Protection of Personal Information Act (POPIA)

In giving substance to the Constitutional right to privacy as provided for in Section 14 of the Bill of Rights as well as in embracing the data Protection International and regional provisions South Africa developed the legislation on Protection of Personal Information Act 2014 (POPIA) whose enforcement capability is provided for through the establishment of the Information Regulator

(**PoPIA**) was developed as a response to obligations placed by the continental, EU and regional international agreements regarding data protection and privacy. These being African Union Convention on the Establishment of a Credible Legal Framework for **Cyber Security** in Africa signed in June 2014 , the EU Data Protection Directive 95/46/EC as well as SADC Model law.

The EU Data Protection Directive 95/46/EC has exercised influence on Africa through its Art 25 and 26. The latter demands assurance of protection of personal information by restricting transfer of personal data from EU to third countries unless the data protection system there provides for an adequate protection. In Africa there are 15 countries out of 54 which have implemented omnibus data protection legislation.[21]

At Continental level the need for harmonisation commenced through the African Union Convention on Cybersecurity and Personal Data Protection 2014 (hereinafter the AU CyberSecurity Convention). Central to the AU CyberSecurity Convention are three main issues: electronic transactions, personal data protection and cybercrimes with Chapter II (Articles 8–23) of the Convention encapsulating protection of personal data. The Convention provides for the rights of the individual whose personal data is the subject of processing: the right to information, right of access, right to object, and right to rectification and erasure (Arts 16,17,18 and 19 respectively). At the same time it contains four provisions on obligations of the data controller. These include confidentiality, security, storage and sustainability (Arts 20,21,22, and 23 respectively). International transfer of personal data to non-Member States of the African Union is restricted unless such a state provides an adequate level of protection for privacy, freedoms

[21] Makulilo, Alex B. "Myth and reality of harmonisation of data privacy policies in Africa." *Computer Law & Security Review* 31.1 (2015): 78-89.

and the fundamental rights of individuals in relation to the processing or possible processing of such data [Art 14(6)(a)][22].

At sub-regional level, the SADC privacy initiative is provided for in the SADC Data Protection Model-Law 2012 (i.e. the Model-Law) that profiles the protection of an individual's right to privacy as well as harmonisation of data privacy policies and laws. Central to the Model Law are provisions articulated in IV, V, VI and VII of the Model-Law which contain basic principles and condition for processing personal data which are fair and lawful processing [Art 12(1)]; explicit purpose [13(1)]; legitimacy (Art 14); sensitivity (Art 15); data quality (Art 11); security (Art 24); openness (Art 29) and accountability (Art 30). The Model law accords the specific rights to data subjects right of access; right of rectification, deletion, temporary limitation of access; right of objection; and representation of the data subject who is under age. These provisions form the basis of POPIA whose lawful processing is measured against eight standard. These being accountability, processing limitations, purpose specification, further processing limitations, information quality, openness, security safeguards and data subject participation. Further POPIA stablishes the information Regulator[23] that is subject to the Constitution and is accountable to the National Assembly, charged with the mandate of developing systems and processes to monitor compliance with the provisions of the Act.

The Information Regulator has under section 112(2) of the Protection of Personal Information Act 4 of 2013, developed regulations that provide for the correction, deletion of personal information, marketing requests , complaints management, duties of Information Officers as well as role of the Regulator as a conciliator in investigations.

3.5. **The Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002 (RICA)**

In embracing the constitutional right to privacy as provided for in section 14 of the Bill of Rights, Regulation of Interception of Communication and Provision of Communication Related Information Act ,referred to hereafter as RICA was promulgated. The schedule to RICA lists the different kinds of crimes the Act aims to combat which include, amongst others, high treason,

[22] African Union Convention on Cybersecurity and Personal Data Protection 2014
[23] Section 39 of POPIA

sedition, fraud and money laundering. RICA sets out circumstances under which law enforcement personnel may apply to a designated Judge of a High Court for an interception and monitoring direction and entry warrants, and the manner in which such directions and entry warrants are to be executed. When RICA came into effect, it repealed the Monitoring Prohibition Act, 1992.
RICA provides an extension and improvement of the legislative provisions of the Monitoring and Prohibition Act (MPA)24 that provided for the same but was not universally applied across the public and private sectors. Section 2 of RICA contains a provision that states that "no person may intentionally intercept or attempt to intercept or cause the authorisation and procuring or attempt to intercept communication direct or indirect within the Republic. Section 5 of RICA further provides that any person may authorise or give anyone else written permission to monitor or intercept any data communication unless it is for the purposes of unlawful conduct.

RICA provides, in sections 3–11, exceptions to the above prohibitions where in certain instances communications may be monitored or intercepted. These exceptions entail

- a directive has been granted that permits the above prohibited activities;
- the party protected by RICA gives requisite consent;
- the entity engaging in the above activity was also a party to those communications;
- intercepting, monitoring or disseminating information of an employee while carrying on a business;
- interception to prevent serious bodily harm;
- interception to determine a location during an emergency; or
- when entitled to do so in terms of other legislation.[25]

RICA establishes a balance between both rights to privacy and security by providing judicial oversight and limiting interception of communication. The Act also permits the interception of indirect communication in connection with the carrying on of business; monitoring of signal for

24 Act 127 of 1992.

25 Act 70 of 2002

purposes of installation or maintenance of equipment, facilities or devices; and monitoring of signal and radio frequency spectrum for purposes of managing radio frequency spectrum.[26]

RICA states that no person—who is not a party to the communication, does not have prior written consent or is not acting in the course of business—may intentionally intercept, attempt to intercept, authorise or procure any other person to intercept or attempt to intercept at any place in the Republic any communication in the course of its occurrence or transmission (Sections 2, 4, 5). However, any authorised person who executes an interception direction or assists with the execution thereof may intercept any communication (Section 3). Further, a postal service provider to whom an interception direction is addressed may intercept any indirect communication, to which that interception direction relates (Section 3). Under RICA Chapter 3, an applicant may apply—orally or in writing—to a designated judge for the issuing of an interception direction (Sections 16, 17 and 23).[27]

Pistorius argues that indirect communication entailing interception of snail mail, electronic communication, Internet, short message service (SMS), downloading of personal and private emails, transfer of visual images to mention but a few.[28]

Whilst the RICA criminalises the interception of communication, it provides processes to be followed in legalising such interception. The RICA aims at creating a safer E-savvy South Africa by enabling law enforcement agencies to identify users of cell phone numbers, thus enabling the tracking down of criminal activities using cell phones. Non-compliance with the provisions of the Act results in the disconnection of cellular numbers from their cellular networks.

Baseline data was created from 1 August 2009 through a pre-emptory requirement for all customers with cell phone numbers on cellular networks in South Africa to register their details with their respective networks. Such an enforcement mechanism, as invoked by Section 39 of the RICA, imposes specific data fields that telecommunication service providers must require from all

[26] T Cohen, ISPA ADVISORY 10: The Regulation of Interception of Communications and Provisions of Communication-related Information Act, No. 70 of 2002, February 2003. 207

[27] Act 70 of 2002

[28] Pistorius T 'Monitoring, interception and Big Boss in the workplace: is the devil in the details?' (2009) 12:1 *PER: Potchefstroomse Elektroniese Regsblad* 7.

data subjects prior to approval of contracts. A similar requirement is invoked by the provisions of Section 40 of the RICA to sellers of cellular phones and SIM cards. Section 40 of the RICA provides for information that must be obtained and securely kept by electronic communication service providers of mobile cellular electronic services to citizens, non-citizens and juristic persons in compliance with security standards as provided for in the gazette.

Section 5 of RICA allows communications to be intercepted if a party to those communications gave prior written consent to do so. The question arises whether privileged communications between an attorney and client could also be intercepted in terms of the provisions of s 5? Section 5 of RICA has yet to be tested by our courts, but it is asserted that where a general consent to have communications intercepted inadvertently intercepts communications that are privileged, the right to privacy and fair trial would be infringed. In each instance, one would have to look at the surrounding circumstances and the parameters of the written consent to determine if such infringement was justifiable.[29]

The RICA also prescribes harsher measures and supplements the provisions of the ECT Act. The efficacy of the provisions of the RICA have widely been displayed during police convictions as intercepted cell phone evidence. Convictions have depended on cell phone evidence either in terms of the communication between individuals involved in crime or determining the location of individuals involved in crime.[30] The non-existence of adequate data triangulation systems has been shown to impact negatively on the implementation of the Act. This has resulted in unscrupulous traders reselling sold RICA-registered SIM cards without asking buyers for their personal information and documentation in contravention of the law.

RICA[31], the ECTA[32] and PAIA generally prohibit the unlawful interception or monitoring of any data message.[33]

---

[29] Russel Luck RICA: walking a fine line between crime prevention and protection of rights." De Rebus, Jan/Feb 2014:30 [2014] DEREBUS 6

[30] Cassim F 'Addressing the spectre of cyber terrorism: A comparative perspective' (2012) 15:2 *PER: Potchefstroomse Elektroniese Regsblad* 01-37.

[31] Section2 of RICA

[32] Section 6 of ECTA

[33] Cohen 2001:2-4

3.6. **The Protection of Constitutional Democracy against Terrorism and Related Activities**

The Protection of Constitutional Democracy against Terrorism and Related Activities (PCDTRA)[34] provides measures to prevent and combat terrorist and related activities by giving effect to international instruments addressing such activities through measures to prevent and combat the financing of terrorist related activities as well as through investigative measures in respect of terrorist and related activities.

Cassim defines 'terrorist activity' as *inter alia*, any act which 'causes serious interference with the disruption or delivery of an essential service, facility or system, whether public or private'.[35] The coverage of 'an essential service, facility or system' encapsulates electronic system, including an information system, a telecommunication system, a banking or financial service or system, an essential government service system, an essential public utility or transport system, an essential infrastructure facility or any essential emergency services such as the police, medical or civil defence service.[36] Thus, essential service by its very nature is characteristic of critical infrastructures, which encompass banks, communications systems, government departments and computer networks. The harm caused within such infrastructure presents a threat to territorial integrity, thus causing insecurity within the country, a perception that negatively affects the profile of the mandated organs of state as well as/or international bodies.[37]

3.7. **National CyberSecurity Policy Framework and Policy**

South Africa has profiled CyberSecurity as a critical component contributing towards national security.[38] This is premised on the reality that geographical regions of the country are becoming integrated into the global village, and secondly, the emergence of smart city E-government initiatives that have necessitated additional government initiatives aimed at bridging the digital

---

34 Act 33 of 2004.

35 Cassim (note 32 above) 383-4.

36 Cassim (note 32 above) 01-37.

37 Cassim (note 32 above).

38 Grobler, van Vuuren & Zaaiman (note 2 above).

divide and addressing CyberSecurity. One of these initiatives is the development and implementation of a South African specific CyberSecurity Policy.

South Africa adopted a National CyberSecurity Policy Framework (NCPF)[39] to steer the country to respond to CyberThreats. The NCPF provides guidelines for organs of state within the Justice Crime Prevention and Security (JCPS) Cluster to craft CyberSecurity measures in their respective departments to ensure safety of the National Critical Information Infrastructure (NCII). The JCPS Cluster mandated the CyberSecurity Response Committee (CRC) to co-ordinate and led the effort of fulfilling the NCPF's mandate. More than 5 (five) years later, the objectives of the NCPF have not translated into action and South Africa is still vulnerable to devastating attacks due to the narrow and fragmented approach adopted in implementing the NCPF. In addition, South Africa's approach was fragmented and perceived to be voluntary rather than prescriptive and mandatory. Failure in the implementation of NCPF can be attributed to the fact that there is a lack of recognition of the following facts:

1. Threats to SA's national security are not limited to a few government departments (JCPS Cluster).
2. The most critical threats are to the South African military, intelligence agencies and critical infrastructure of which the vast majority is controlled and managed by local and provincial governments and the private sector.
3. CyberSecurity is not the preserve of ICT departments or ICT professionals, CyberSecurity involves all aspect of life.
4. To effectively address CyberSecurity, new laws and regulations are required, new institutions have to be established and new capabilities have to be developed and acquired.
5. Development and Institutionalisation of Cybersecurity Culture within the citizenry remains a non negotiable

The National Cyber-Security Policy Framework sets out a number of tasks directly aligned to the Department of Defence, which include, inter alia, addressing national security threats in cyber-

[39] National CyberSecurity Policy Framework for South Africa in the South African Government Gazette No 39475 of 4 December 2015.

space, combating cyber-warfare, cyber-crime and other cyber ills; developing, review and update existing substantive and procedural laws to ensure alignment; and building confidence and trust in the secure use of information and communication technologies. In order to protect its interests in the event of a cyber-war, a cyber defence capacity has to be built. The NCPF thus promotes that a Cyber Defence Strategy, that is informed by the National Security Strategy of South Africa, be developed, guided by the JCPS Cybersecurity Response Committee.[40]

3.7.1 Institutional Arrangements

In terms of institutional arrangements, the NCPF establishes the Cyber Response Committee(CRC) chaired by the State Security Agency. The CRC was established in 2013 and the members are the DGs of the JCPS Cluster Departments or their alternates as well the DTPS, SITA, DST, DIRCO & SARS. The CRC meets monthly and responsible for coordinating the implementation of the NCPF as well as the coordination and facilitation approval of various Cybersecurity strategies and regulations by the relevant Ministers. CRC is mandated to provide national guidance and policy advice on CyberSecurity matters. Monitoring of progress is conducted through reports to the JCPS cluster DGs on the implementation of the NCPF.

The NCPF envisages the National Cybercrime Centre (NCC) to provide technical support to Law Enforcement Agencies (LEAs) in the fight against various forms of Cybercrime. It is envisaged that the NCC will act as a 24/7 contact point regarding matters relating to cybercrime; develop and maintain cross-border law enforcement cooperation in respect of cybercrime;develop response protocols to guide coordinated responses to cybercrime incidents and interaction with the various stakeholders as well as provide regular updates on cybercrime matters to the Cybersecurity centre for analysis purposes.

The fight against Cybercrime requires an institutionalised public-private partnership. The NCPF establishes the Cybersecurity Hub that promotes cooperation between Public and Private sector stakeholders. The Cybersecurity Hub encourages and facilitates the development of appropriate additional sector CSIRTs; assists sector CERTS/CSIRTs to conduct efficient and effective computer emergency response and disseminates the information to other sector CSIRTs, vendors

[40] NCPF (note 39 above)24-29

and technology experts as well as Facilitates compliance with national response protocols in order to guide response by private sector to Cybersecurity incidents and interaction with the various stakeholders within the private sector.

In giving substance to the just on time response,as well as developing the skills base to enable the CyberSecurity culture, the Hub is developing procedures to coordinate responses and resolve incidents in 'real-time' at a national level as well as developing National Skills Framework for Cybersecurity that will form the basis for development of accredited programmes to be developed in collaboration with the relevant Sector Education and Training Authorities(SETAs) and The Quality Council for Trades and Occupations (QCTO) which is a Quality Council established in 2010 in terms of the Skills Development Act. Its role is to oversee the design, implementation, assessment and certification of occupational qualifications on the Occupational Qualifications Sub-Framework (OQSF).

To deepen cyber awareness the CyberSecurity Hub has profiled Implementation of a collaborative software solution that will provide 'war room' CyberSecurity Foresight and hacking back offensive capabilities that will inform development of occupational national Awareness Portal development as well specific awareness programs in conjunction with private partners and the Gov-CSIRT.

The NCPF mandates the Defence and Military Veterans Vote with the overall responsibility for coordination,accountability and development of policies and strategies to inform cyber defence measures as part of protection of territorial intergrity. The inescapable reality is that the establishment of all the Cyber-domains requires substantial funding and skilled personnel. The cyber Command within the DOD has not been fully established due to dearth of requisite funding appropriation and allocation, identification, recruitment, or training of personnel with the correct skills at all levels.

Grobler, van Vuuren and Zaaiman assert that within the South African context, CyberSecurity policy requirements should be premised on 5 (five) fundamental determinants: Political will, adapted organisational structure, accurately identified pro-active and re-active measures,

aggressive crime reduction initiatives that are fore-grounded by high impact education and awareness programmes.[41]

Grobler *et al* further propose that CyberSecurity Policy should give credence to CyberSecurity actors, the protector, the protected and the criminal.[42] The advent of the CyberCrime and CyberSecurity legislation aims to strengthen the gaps that resulted in the slow implementation of the NPF.

3.8. **Security legislation**

The National Strategic Intelligence Act[43] provides for the establishment of the National Intelligence Coordinating Committee as well as provide for specific functions as these relate to security of the Republic.[44] The critical functions of the Agency being to gather, correlate, evaluate and analyse domestic intelligence as well as conduct threat analysis of potential threats to security of the Republic.[45] The Act provides for the South African National Defence Force (SANDF) mandate of gathering, correlating , evaluating through the use of foreign military intelligence as well provide support to the strategic intelligence of NICOC. The SANDF collection excludes gathering of intelligence of a non-military nature in a covert manner.

3.9 The CyberCrime and CyberSecurity Bill

In South Africa, the criminalisation of CyberCrimes is provided for in various legislative frameworks. These are the ECT Act[46], the RICA Act,[47] and the Protection of Personal Information Act (POPIA).[48] Flowing from the National Cybersecurity Policy Framework, the Cybercrime and Cybersecurity Bill was developed, published for comments in 2015, whose content displayed

41 Grobler, van Vuuren & Zaaiman (note 2 above) 217-219.

42 Grobler *et al* (note 40 above).

43 Act 39 of 1994.

44 Section 2 of the National Strategic Intelligence Act 39 of 1994.

45 Section 2(b).

46 Section 85 & 86 of Act 25 of 2002

47 Section 5 of Act 70 of 2002.

48 Protection of Personal Information Act 4of 2013 Government Notice No 37067 of 26 Nov 2013.

similarities with the provisions of the Budapest Convention. The 2015 version of the Bill experienced revisions upon analysis of comments received which culminated in the 2017 version which is herein referred to as, the Bill.

The CyberCrime and CyberSecurity Bill[49] aims to extend the substantive CyberCrimes that were limited to the ECT Act, as well as to criminalise more activities relating to unlawful use of computer systems.[50]

Section 2 criminalises unlawful securing of access whilst section 3 criminalises unlawful acquiring of access. Section 4 deals with unlawful acts committed using computer software or hardware whilst section 5 criminalises unlawful interference with data and computer programmes. Section 6 deals with unlawful interference with data storage medium and computer system. Section 7 criminalises unlawful interference with computer device, computer networks, databases, critical database, electronic communication network and national critical information infrastructure. Section 9 provides for the unlawful acquisition, possession, receipt or use of passwords, access codes or similar data or devices whilst section 10 deals with computer related fraud. Sections 11to 21 introduces new proposed cybercrime offences that encompass cyber forgery and uttering, cyber appropriation, cyber extortion, cyber terrorism, cyber espionage and unlawful access to restricted data, prohibition of dissemination of racist and xenophobic material, prohibition of incitement of violence, prohibited financial transactions, copyright infringement, child phonography as well as harbouring or concealing person who commit crime.

In recognition of the emergence of CyberSpace as the battleground, whose regulation straddles across various jurisdictions, the Bill creates a Cyber command[51],. Snail kaMtuze argues that given the threat of CyberTerrorism, which is characterised by effects-based CyberTerrorism as well as intent-based terrorism. The mandate of the proposed CyberCommand should be to decisively deal with offences against CyberSystems and critical information infrastructure.[52] It

---

49 Memorandum on the Objects of the CyberCrimes and CyberSecurity Bill 2017 available at: www.ellipsis.co.za/wp.../Summary-of-CyberCrimes-and-CyberSecurity-Bill-2017.pdf (accessed: 10 September 2017).

50 Papadopoulos S & Snail kaMtuze S *Cyberlaw @ SA III: the law of the Internet in South Africa*.

51 Clause 55 of the Cybersecurity and Cybercrime Bill 2015

52 Republic of South Africa *CyberCrime and CyberSecurity Bill* [B 6-2017] published in Government Gazette No 40487 of 9 December 2016.

can be seen therefore, that enhancing CyberSecurity and protecting critical information infrastructures are essential to each nation's security and the economic well-being. Making the internet safer and protecting, the users of ICTs have become integral to the development of new services as well as governmental policy.[53]

The CyberCrimes and CyberSecurity Bill create offences and prescribe penalties. The Bill criminalises hacking, unlawful interception of data, ransom ware, Cyber forgery and uttering Cyber extortion. Jurisdiction[54] in respect of all offences, which can be committed in CyberSpace is expanded substantially in terms of the Bill, mainly to deal with CyberCrime which originates from outside our borders.

The CyberCrimes and CyberSecurity Bill gives the police service (and their members and investigators) extensive powers to investigate, search, access and seize just about anything (like a computer, database or network) wherever it might be located, provided they have a search warrant. Foreign states are expected to co-operate in investigating CyberCrimes. A 24/7 round-the-clock capability to detect and investigate CyberCrimes is assign to the Minister of Police.[55]

To improve CyberSecurity, the CyberCrimes and CyberSecurity Bill creates a CyberResponse Committee (CRC),[56] under the accounting and executive leadership of State Security whose function is to implement government policy relating to CyberSecurity. To ensure identification and protection of critical infrastructure, the Bill assigns to the Executive Authority of State Security the responsibility for the establishment and operational effectiveness of a capability resourced Computer Security Incident Response Team (CSIRT)[57] for government.[58]

---

53 Media Briefing: Statement by the Deputy Minister of Justice and Constitutional Development, the Hon JH Jeffery, MP on the new proposed CyberCrime and CyberSecurity Bill, 19 January 2017 available at: http://www.justice.gov.za/m_speeches/2017/20170119-CyberCrimeBillBriefing.html (accessed: 10 September 2017).

54 Clause 25 of the Bill

55 Clause 52 of the Bill

56 Clause 49 of the Bill

57 Clause 53 of the Bill

58 Grobler M *et al* 'Preparing South Africa for cyber-crime and cyber defence' (2013) 11:7 *Journal of Systemics, Cybernetics Informatics* 32-41.

In addition, the Executive Authority of the Defence and Military Veterans mandate is required to establish and maintain a CyberOffensive and CyberDefensive capacity[59] as part of the Defence Force's mandate.[60] Clause 55 of the 2015 Bill establishes prescribes that the Cabinet member responsible defence must , in consultation with the Cabinet Member responsible for national financial matters establish Cyber Command as part of Defence Intelligence capability of the SANDF contemplated in section 33 of the Defence Act 42 of 2002. The aforementioned Cabinet member is responsible for ensuring equipping, operation , maintenance as well as exercise final responsibility over the administration and functioning of the Cyber Command. Clause 55 further prescribe to the Chief of the South African National Defence Force to appoint a member or employee with the requisite skills ,competencies and experience with the appropriate security clearance issued in terms of section 37 of the Defence Act. The provision articulated in Clause 55 of the 2015 version of the Bill provided for the location of the capability, its appreciation as well as its resources appropriation were drastically revised in the 2017 version in Clause 54(3).

Clause 54(3) of the 2017 version, does not refer to the establishment of Cyber Command, its appreciation, its resourcing as well as maintenance of it full operational capability. This drastic revision has unfortunately removed the appropriation of funding, an omission that will adversely impact on the sustained agenda of the defence mandate. The CyberSpace domain is a sui generis and requires its distinctive appreciation and appropriation as it extends the application of the defence mandate of protection of territorial intergrity in accordance with the Constitution and the principles of international law regulating the use of force. The defence mandate is thus extended beyond Land, sea, air, and outerspace.

The Bill established a functionally maintained CyberSecurity Hub[61] delegated to the Executive Authority of the Telecommunications and Postal Services (DTPS). The mandate of the CyberSecurity Hub aims at promoting CyberSecurity in the private sector, providing a one-stop shop service for the public and private sector on CyberSecurity; provide prompt responses to

---

59 Clause 54(3) of the Bill

60 Department of Defence 'South African Defence Review 2015' available at: http://www.dod.mil.za/documents/defencereview/defence%20review%202015.pdf (accessed: 04 November 2017).

61 Clause 54(4) of the Bill

CyberSecurity incidents as well as helping to establish nodal points and Private Sector Computer Security Incident Response Teams (PSCSIRT)[62] in different sectors.

In forging collective responsibility in curbing the scourge of CyberCrime, which has become a global feature, the Bill provides for multilateral agreements and empowers the executive authority responsible for the justice mandate to make regulations on information sharing.[63] This includes sharing information on CyberSecurity incidents, detecting, preventing and investigating CyberCrimes. In recognition of the similar provisions that have been invoked in existing legislation, the Bill also proposes consequential amendments through repeal of such similar or identical provisions in the ECT Act, notably, Chapter 9 in particular Sections 85, 86, 87, 88 and 90 of the ECT Act.

3.10 Critical Infrastructure Legislation

The Critical Infrastructure Protection Bill, 2017 seeks to repeal the National Key Points, 1980 (Act No. 102 of 1980) and related laws of the former TBVC States and to provide for the protection of Critical Infrastructure in the Republic. The Bill further provides for the establishment of a Critical Infrastructure Council, sets out the procedure for the appointment of members of the Council. The Bill further provides for the functions of the Critical Infrastructure Council. The Bill [64]assignes the responsibility for application and administration to the control of the National Commissioner of the South African Police Service locates the provision of costs of installing security measures of a critical infrastructure to be borne by the owner of the critical infrastructure. It is worth considering that whilst clause 9 of the Critical Infrastructure Bill mandates the Commissioner to consult the CRC established in terms of clause 53 of the CyberCrime and Cyber Security Bill 2017, Clause 57 of the CyberCrime and CyberSecurity Bill 2017 underscores the role of the State Security Agency in consultation with CRC.

62 Clause 55 of the Bill

63 Republic of South Africa 'CyberCrime and CyberSecurity Bill' (note 39 above) clause 56.

64 **Critical Infrastructure Protection Bill**, **2017**: Annexed summary of the Bill is hereby published in accordance with rule 241(1)(c). 41114

3.11 Military strategy and related legislation

The Department of Defence (DOD) has overall responsibility for the coordination, accountability and implementation of cyber offensive and defence measures in South Africa as an integral part of its constitutional mandate which is articulated in section 200(2) of the Constitution of the Republic of South Africa stated as

"(2) *The primary object of the defence force is to defend and protect the Republic, its territorial integrity and its people in accordance with the Constitution and the principles of international law regulating the use of force."*[65]

The above constitutional mandate must find expression in the five domains which are land, sea, air, OuterSpace and CyberSpace.

The conventional approach to defence is the presence of a military strategy that situates itself within the three-layered approach on homeland, continent and global. Unfortunately, CyberSpace is a complex battlefield with unclear rules of engagement. The realisation of the shift of the battle space from conventional WarFare to information WarFare and CyberWarFare has occupied centre stage within the military. The development of rules of engagement as presented by the Talim Framework aptly signifies the shift as well as the centrality of information WarFare and CyberWarFare.

South Africa has established a National CyberSecurity Policy Framework (NCPF) purposed to create a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of Critical Information Infrastructure whilst strengthening shared human values and understanding of CyberSecurity in support of national security imperatives and the economy. The NCPF sets out a number of tasks directly aligned to the Department of Defence, which entail:

1. Addressing national security threats in CyberSpace;
2. Combating CyberWarFare, CyberCrime and other Cyberills;
3. Developing reviews and updates of the existing substantive and procedural laws to ensure alignment; as well as

65 Section 200 of the Constitution of the Republic of South Africa, 1996

4. Building confidence and trust in the secure use of Information and Communication Technologies.[66]

The South African Defence Review 2015[67] as approved by Cabinet attests to the reality that South Africa requires the protection of its CyberDomain, and a comprehensive information WarFare capability integrated into its intelligence-related Information Systems at the international, national and defence levels. An increased reliance on Information Communication Technology (ICT) networks has in effect, exposed the State's CyberSpace to ever-increasing vulnerability. The integrity of key national infrastructure, including financial and commercial institutions are at risk. The vulnerabilities manifest in:

1. CyberEspionage which entails the silent gathering of classified information without the permission of the holder of the information;
2. CyberCrime involving the use of malware, viruses, identity theft to commit crime;
3. CyberTerrorism which entails internet-based attacks by individuals for terrorist objectives;
4. CyberWarFare that entails offensive and defensive military information and CyberSecurity operations.[68]

The Technological domain of the Environmental Scanning that underpins the strategic planning Instruments for the 2017 fiscal year of the South African National Defence Force[69] reveal that the Department of Defence has during the 2016 Fiscal Year developed a comprehensive CyberWarFare strategy that responds to the national policy in respect of capabilities for offensive informationWarFare actions. In addition, the establishment of the DOD CyberSecurity Incident Response Team (CSIRT) is planned for 2017.[70]The purpose would be to prevent

66 Department of Defence (note 60 above).

67 Cilliers J 'The 2014 South African Defence Review: Rebuilding after years of abuse, neglect and decay (2014).

68 Department of Defence (note 60 above) 2-18.

69 SANDF Annual Performance Plan for 2017.

70 Department of Defence *Annual Performance Plan for 2017* (2017) 6.

informationWarFare through the establishment of a CyberCommand Centre with all its essential capabilities.[71]

Cyberspace has ushered in a domain whose international law rules are evolving as provided for by the Talim Manual versions. The dearth of the global Treaty negatively impacts the development of offensive and defensive cyber capabilities to provide comprehensively for identification, and management of cyberattacks at Land, air as well as at sea, a domain that houses the cabling of the internet that forms the backbone of global economic activity.

In embracing the National Development Plan, extension of Outcome 3 'All People in South Africa are and feel Safe ' [72] to encapsulate CyberSecurity has become an immediate and urgent reality of the Justice, Crime Prevention and Security (JCPS)Cluster and a non negotiable strategic thrust for the military strategy as a means to ensure secure infrastructure within the CyberSpace.[73]

3.12 Case law relating to CyberCrime

The promulgation of the ECT Act ushered in new factors for determination of admissibility of evidence in general and electronic evidence in particular. This was evidence by the evolution of case law relating to CyberLaw matters. The case of *S v Mashiyi*[74] considered the question of admissibility of computer-generated documents. The Court held that, documents which contain information that has been processed and generated by a computer, are not admissible as evidence in a criminal trial. On the other hand, the Court found that where documents have been scanned to produce an electronic image of the original, then such an image is regarded as an exact image and is therefore admissible. However, in terms of the 'prevailing law' the Court could not admit into evidence the disputed documents which contained information that has been processed and generated by a computer'.

---

71 Clause 55 of the CyberCrime and CyberSecurity Bill 2015

72 Medium Term Strategic Framework: A framework to guide Government's Programme in the Electoral Mandate Period (2009-2014) 30-32

73 MTSF (note 71 above) 17-18

74 *S v Mashiyi* 393 C-D2002 (2) SACR 387.

The Court in *Mashiyi* referred to *Narlis v South African Bank of Athens*,[75] which held that a computer printout could not be received as evidence in terms of Section 34 of the Civil Procedure and Evidence Act.[76] The reason for the rejection of a computer printout as admissible evidence in the above case was that a computer is not a person and therefore a computer printout is not a statement made by a person. The Court also referred to *S v Harper*[77] in which it found that computer-generated documents were admissible under the Section only if the computer merely stored or recorded the information.

In *Narlis v South African Bank of Athens*,[78] the Court held that a computer printout was inadmissible in terms of the Civil Procedure and Evidence Act. The Court also held that a computer is not a person. It was also clear that the law regarding value of electronic data in legal proceedings required urgent redress. This resulted in the premature birth of the Computer Evidence Act,[79] which provided for such admissibility subject to over cautious approach with regard to reliability and authenticity. Further, the legislation applied to civil matters rather than criminal matters. Section 142 of the said Act made provision for an authentication affidavit in order to authenticate a computer printout.[80]

In the case *Ndlovu v Minister of Correctional Services*,[81] the Court had to consider *inter alia* whether a computer printout, which was a copy, complied with the best evidence rule or could not be admitted as evidence unless properly proved. The Court found that firstly, the plaintiff's failure to object to the evidence during the trial precluded him from relying on the best evidence rule only during argument.[82] The plaintiff had also referred extensively to the printout during evidence without objecting, with the result that it amounted to a tacit waiver of the best evidence principle. Secondly, the Court found that because the printout was generated by computer, it was governed

---

75 *Narlis v South African Bank of Athens* 1976 (2) SA573 (A).

76 Act 25 of 1965.

77 1981 (1) SA 88 (D).

78 1976 (2) SA 573 (A).

79 Act 57 of 1983.

80 Watney M 'Admissibility of electronic evidence in criminal proceedings: An outline of the South African legal position' (2009) 1 *Journal of Information, Law and Technology* 2.

81 *Ndlovu v Minister of Correctional Services* and another 2006 All SA 165 (W) para 172.

82 *Ndlovu v Minister of Correctional Services* (note 56 above).

by the ECT Act. However, the Court found that the printout was admissible as evidence, not in terms of Section 15 of the ECT but in terms of the Court's statutory discretion to admit hearsay evidence in terms of the Law of Evidence Amendment Act.[83] The decision has presented concerns about the efficacy of invoking Section 15 to test the authenticity and hearsay rule.[84]

In *S v Ndiki*,[85] the state sought to introduce certain documentary evidence consisting of computer-generated printouts, designated as exhibits D1-D9, during the course of a criminal trial. The Court found that because certain individuals had signed exhibits D1 to D4, the computer had been use as a tool to create the relevant documentation. Therefore, these documents constituted hearsay. The duty to prove such accuracy and reliability lay with the state. Notwithstanding the cautious approach adopted by Courts, the ECT Act, has ushered a paradigm for admissibility and evidential weight of electronic evidence.[86] In *S v Van den Berg*, the alteration of information stored on the computer of a bank was held to be a misrepresentation for the purposes of establishing criminal liability for fraud.[87]

The impact of section 5 of RICA on attorney client privilege was analysed in the cases cited below. In Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others [2008] ZACC 13; 2009 (1) SA 1 (CC)88 the court, in paras 183 and 184, maintained that attorney-client privilege is to be taken very seriously but it is not an absolute right and can be outweighed by countervailing considerations.

Similarly in *S v Tandwa and Others* **2008 (1) SACR 613** (SCA),[89] the court outlined in paras 18 and 19 that attorney-client privilege can be waived expressly, tacitly or by conduct sufficient to impute that the privilege has been waived by the client.

---

83 Act 45 of 1988.

84 *Ndlovu v Minister of Correctional Services* (note 56 above) para 172.

85 *Ndiki* 2008 (2) SACR 252 (Ck).

86 Watney (note 77 above) 3.

87 *S v Van den Berg* 1991 (1) SACR 104 (T) 106.

88 *Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others [2008] ZACC 13; 2009 (1) SA 1 (CC)Para183-184*

89 *S v Tandwa and Others 2008 (1) SACR 613 (SCA),Para 18&19*

3.13 Conclusion

Grobler *et al* attest that on many levels, CyberWarfare brings the battle closer to home since more people are potentially affected.[90] In many instances, the enemy is omnipresent, since any piece of equipment that uses technology is a potential battlefield or a medium that could be used by enemy forces. The overview of South African CyberSecurity landscape has sketched a trajectory that marks CyberCrime from Common Law to various statutory provisions that had to fill the gaps created by the dynamics of the crimes committed in the fifth dimension, the CyberSpace, whose rules are non-existent and amphibious but whose effects affect all humankind.

The ECT Act ushered new rules for admissibility of electronic evidence as well as criminalisation of activities. Various legislative frameworks addressed various CyberCrimes but still a need for a one-stop shop legislative framework to deal with CyberCrime and CyberSecurity was essential. This is the space that the current CyberCrime and CyberSecurity Bill is meant to fill. Nonetheless, the Bill is a product of international and continental treaties.

The developments surrounding the Hate Speech Bill are also noted and recognised as these will have impact on South Africa's approach to CyberCrime, CyberStalking, CyberTerrorism and CyberSecurity.

Several enforcement provisions exist within the ECT Act, notably the appointment of Cyber Inspectors. Regrettably, this provision has not been implemented to date, suggesting the need to strengthen the compliance mechanisms and institutional arrangements. Notwithstanding the aforementioned implementation readiness challenges, South Africa remains committed to decisively ensure that citizen experience a secure but agile CyberSpace, with clear protocols governing multilateral organisations to promote boundary management through collective governance.

The CyberCrime and CyberSecurity legislative developments should improve on the gains made through the implementation of the ECT Act by strengthening the identified weaknesses that expose vulnerabilities of the state and its citizens to cyberattacks, cybercrimes, cyberterrorism

90 Grobler, van Vuuren & Zaaiman (note 2 above) 33.

and cyberespionage. The mandate analysis of the security sectors elements together with the structures designated for supporting the cybersecurity agenda, its accountable implementation with clear boundary management remains paramount and critical.

The distinctive roles of the Information Regulator capabilities charged with the enforcement of the implementation of the POPIA, Internal Audit and the Office of the Auditor General capabilities as well as digital forensic capabilities remain sacrosanct. It is an unfortunate reality that the establishment of all the Cyber-domains require substantial funding and skilled personnel. Development and Implementation of a National Cybersecurity Infrastructure Plan remains sacrosanct and must be informed by full appreciation of system readiness to enable the identification of critical information infrastructure. Such appreciation should reconcile the roles and responsibility of organs of State in relation to Critical information Infrastructure as articulated in Cybercrime and CyberSecurity Bill and the roles as spelled out in the Critical Infrastructure Bill.[91]

[91] Critical Infrastructure Bill 2017 Government Gazette No 41114 of 15 September 2017 accessed from https://www.parliament.gov.za/. on October 2017.

CHAPTER 4: GERMANY

4.1. Introduction

This Chapter provides a detailed foreign comparative law survey with focus on German CyberCrime and CyberSecurity legislation and case law. The jurisdiction selected relates to the origin of the South African Cyber Policy Framework, which has its antecedence in the German CyberSecurity Policy.

The "2016 Germany CyberReadiness Report" profiles Germany as one of the world's most technologically advanced telecommunications systems that has invested in intensive capital expenditures since its 1990 reunification to yield an internet penetration rate of over 86% (eighty six percent). The German government has been aggressively driving ICT development and internet connectivity since the advent of the internet and has strategically driven many internet related projects. Germany was the first country in the world to digitise its libraries after the introduction of the World Wide Web.[1]

Central to the aggressive internet connectivity has been the German Criminal Code[2] whose provisions encompass specific provisions that pertain to utilisation of the computer systems for committing offences in the CyberSpace. European Union (EU) Member States have statutes prohibiting 'mere accesses of systems without authorisation and some states attach further requirements in order to trigger criminal penalties. Germany has enacted Legislation against unauthorised access whose application is dependent on evidence of "secure systems" for which some effort has been made to inhibit open access.

---

1 Hathaway M *et al* 'Germany Cyber Readiness at the glance' (2016) *Potomac Institute for Policy Studies 2*.

2 Criminal Code in the version promulgated on 13 November 1998, Federal Law Gazette [Bundesgesetzblatt] I p. 3322, last amended by Article 1 of the Law of 24 September 2013, Federal Law Gazette I p. 3671 and with the text of Article 6(18) of the Law of 10 October 2013, Federal Law Gazette I p 3799.

On the International Governance Platform, the Internet Governance Forum of the United Nations (IGF) has been established to deal with the transnational quality of CyberSpace but also other policy fields such as, the inter-national governance of the internet through organisations and regimes. This is marked by the same weaknesses of institutional complexity, a lack of cohesion, Authority and Compliance. The field of Internet Governance in the International Community is characterised by clear ideological orientation that range from a group of autocratic states to liberal democracies. Autocracies seek to hold control of the internet because of fear of destabilisation of political systems given the free transnational flows of Information whilst liberal democracies publicly support, data and information flows and thus the leading vision of a "Web of the Freehand thus becoming critical of governmental control or censorship of internet content.[3]

4.2. Situational analysis

In 2011, Germany Government released the CyberSecurity Strategy for Germany,[4] wherein which profiled the recognition and acknowledgement of interconnections between ICTs and economic and social growth, and classified internet with its underlying ICTs as a critical infrastructure for German society.

The national CyberSecurity strategy profiles key strategic areas and objectives to better combat Germany's cyber threat environment and entails:

a. Protection of critical infrastructure and IT systems;
b. The strengthening of public administration's IT security through the adoption of a uniform 'federal network';
c. The creation of a National CyberResponse Centre for incident response and protection;

---

3 David G & Schünemann WF 'Creating a secure CyberSpace–Securitisation in internet governance discourses and dispositives in Germany and Russia' (2013) 20:12 *International Review of Information Ethics* 37-51.

4 Federal Ministry of the Interior 'CyberSecurity Strategy for Germany' (2011) available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf (accessed: 23 October 2017).

d. The establishment of a National CyberSecurity Council for improved cooperation between the public sector and private sector entities;
e. The promotion of effective international coordination for CyberSecurity; the development of reliable and trustworthy IT through innovation; and
f. The training of skilled personnel in federal authorities; and the effective use of public sector tools including statutory powers to combat CyberAttacks.[5]

The Strategy further establishes National CyberSecurity Council whose mandate is to provide a coordinated approach to CyberSecurity issues across all policies. The strategic posture advanced in the Digital Strategy further accelerates 'exploitation of the potential of innovation to realise further growth and employment whilst promoting national security'[6]

In 2014 Germany Government approved the Germany's 2014 Digital Strategy 'Digital Agenda 2014-2017'[7] that further echoes elements of the National CyberSecurity Strategy by recognising the importance of ICT for economic growth while acknowledging the need for increased security in CyberSpace. The Digital Strategy 2014 provides a foresight of strategic global positioning of Germany as a leader in the internet economy. The Strategy profiles opportunities for boosting competitiveness, economic growth, and social well-being of the country through enhancing high-speed networks and trust.[8]

In response to the footprint that depicts that only 20% (twenty percent) of Germany's rural areas have access to wireless broadband, and in recognition of importance of ICT for economic growth 'Digital Agenda 2014-2017'[9] that aims to widen access by accelerating the roll out of high-speed

5 Hathaway *et al* (note 1 above) 5.

6 Hathaway *et al* (note 1 above) 6.

7 The Federal Government, 'Digital Agenda 2014-2017' (2014) 21 available at: https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda-engl.pdf?__blob=publicationFile&v=6 (accessed: 23 October 2017).

8 Hathaway *et al* (note 1 above) 6.

9 Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme see also Farley W & Williams 'Briefing: The new German IT Security Act' February 2016.

broadband in remote areas as well as and provide all households downloads speeds of at least 50 megabits per second by 2018.[10]

In July 2015, Germany established a new IT Security Act[11] with the goal of preventing the loss of important IT systems such as those used by the BSI, telecommunications providers, and critical infrastructure operators. According to the Country Report,[12] operators of critical infrastructures are obliged to undergo IT security audits or certifications at least every two years, wherein industry-specific security standards are presented.

According to the Reuters,[13] German government registered 82,649 cases of computer fraud, espionage and other CyberCrimes in 2016, as compared to 2015 statistics of 45,793, which presents an increase of just over 80% from 2015. The German Interior Minister Thomas de Maiziere released the new statistics, as part of the government's annual crime report on 24 April 2017, which reflects a resolution rate of 38.7%. Further, regarding instances where the internet is used to commit crime; German police also registered 253,290 cases of CyberCrimes carried out with the help of the internet, which is an increase of 3.6% from 2015.[14]

The resilience report that was publish, focuses on key components of CyberResilience, which project the ability to prevent, detect, contain and recover from a CyberAttacks.[15] The 2017

---

10 The Federal Government (note 8 above) 9.

11 Farley W & Williams 'Briefing: The new German IT Security Act' February 2016 available at: http://www.wfw.com/wp-content/\uploads/2016/02/WFW-Briefing-Germany-IT-Security-Feb-2016-EN-15-Feb.pdf (accessed: 23 October 2017).

12 Hathaway *et al* (note 1 above) 9.

13 Reuters German CyberCrime rose 80 percent in 2016: report – available at https://www.reuters.com/article/us-germany-crime-cyber-idUSKBN17P0YB (accessed: 23 October 2017).

14 Business Information Industry Association 'German Cyber Crime rose 80% in 2016 according to the latest statistics issued by German Ministry of Interior' available at: http://www.biia.com/german-cyber-crime-rose-80-in-2016-according-to-the-latest-statistics-issued-by-german-ministry-of-interior (accessed: 30 August 2017).

15 The Second Annual Study on the CyberResilient Organisation: Germany Ponemon Institute, February 2017 1.

resilience report portrays a Germany with 57% (fifty–seven percent) and 56%(fifty-six percent) respondents displaying most confidence in detecting and containing a CyberAttacks respectively whilst registering less confidence since last year in their ability to prevent attacks and recover.[16]

The South African landscape has introduced similar intervention. In 2013, South Africa approved a National Broadband Policy: South Africa Connect, Creating Opportunities and Ensuring Inclusion,[17] developed in terms of Section 3(1) of the Electronic Communication Act 36 of 2005. The South Broadband Policy framework aims to widen access to broadband, by creating opportunities to ensure digital readiness, digital development, fore sighting a digital future and realising emerging digital opportunities. In 2014, the National Integrated ICT Policy development process was initiated that responds to the National Development Plan[18] vision of a fully connected Information Society by 2030.

4.3. Policy and Legislation

4.3.1. Overview

CyberAttacks are perceived by the German Government as attacks coming most frequently from terrorists, professional fraudsters, and criminal organisations because those IT attacks are more attractive than conventional attacks.[19] internet communication in Germany seems to be very free and the rather hesitant measures of regulation and control by the government have been responded to by open protests (see the domestic debate on 'Netzsperren' in the year 2009).[20]

As regards new tools, institutions and practices that have been established in the policy field, Germany recently adopted measures to secure CyberSpace by a 'National Cyber Response

16 Ponemon Institute © *Research Report* 2017 1.

17 National Broadband Policy 2013: South Africa Connect: Creating opportunities, Ensuring inclusion

18 National Development Plan Vision 2030.

19 Ponemon Institute© Research Report, 2017 1.

20 Gorr D & Schünemann WJ 'Creating a secure CyberSpace–Securitisation in internet governance discourses and dispositives in Germany and Russia' (2013) *International Review of Information Ethics* 51.

Centre' which was set up in April 2011 to 'optimise operational cooperation between all state authorities and improve the coordination of protection'.[21]

As do many other countries, Germany struggles to find the right balance between privacy and CyberSecurity as this entails a balancing act on many fronts. This state of affairs has been evidently recorded during the Parliamentary hearings in South Africa on the CyberCrime and CyberSecurity Bill of 2017 where the balance between right to privacy[22] and right to access to information[23] was raised by the Centre for Constitutional Rights (CCR) and the South African Information Regulator. The German government has suggested a mandatory (bulk) data retention law (*Vorratsdatenspeicherung*) that will require companies to store traffic data for certain time periods in case this information is needed for the prosecution of potential terrorist activity or other serious crime. These sensitive data sets must be stored in Germany. Many Germans believe that the bulk collection of their traffic data (calls, cell tower location data, and email connection data) infringes with their fundamental privacy rights.[24]

German National CyberSecurity Strategy explicitly states that it considers only Information and Communication Technology (ICT) connected to internet.[25] Germany was the first country to react to the Cyber threat in Europe. In a report from the Federal Office for Information Security in 2005, Udo Helmbrecht, its president, announced that CyberSecurity must be part of a national security response (Bundesamt für Sicherheit in der informationstechnik 2005).[26] Apart from the installation of new authorities, the federal government generally seeks to portray itself as a role model as regards CyberSecurity by the publication of guidelines and a general framework addressing CyberThreats. State agencies shall establish minimum standards, harmonise rules, introduce

---

21 EMarketer 'Two in five internet users in Germany hit by CyberCrime in 2013: Malware was the most widespread issue, affecting one-quarter of people online' (2013) 20:12 *Information Ethics* 37.

22 Sect 14 of the Constitution of South Africa.

23 Sect 32 of the Constitution of South Africa.

24 Dr Spies is the author of AICGS Issue Brief 46: German/U.S. Data Transfers: Crucial for Both Economies, Difficult to Regain Trust 16 July 2015.

25 Luiijf E, Bestselling K & De Graaf P 'Nineteen national CyberSecurity strategies' (2013) 9:1/2 *International Journal of Critical Infrastructures* 7.

26 Guitton C 'Cyber insecurity as a national threat: Overreaction from Germany, France and the UK?' (2013) 22:1 *European Security* 21-35.

legal commitments, strengthen law enforcement agencies and promote coordination at national and international level (EU, NATO, United Nations and OECD Coordination Proposition).

In 2012, South Africa approved the National CyberSecurity Policy Frameworks that seeks to:

a. Promote a CyberSecurity culture and facilitate compliance with minimum security standards;
b. Strengthen mechanisms in place to prevent and address CyberCrime, CyberWarfare, CyberTerrorism, and other related issues;
a. Establish public-private and societal partnerships within South Africa and internationally to strengthen awareness and enforcement;
b. Ensure the protection of national critical information infrastructure;
c. Promote and ensure a comprehensive legal framework governing CyberSpace; and
d. Ensure adequate national capacity to develop and protect South Africa's CyberSpace[27]

The Policy framework established the National CyberSecurity Council, CyberSecurity Hub, CyberCommand Centre, and National Computer Incident Response Teams. The CyberSecurity and CyberCrime Bill of 2017, provides for creating offences and imposing penalties which have a bearing on CyberCrime, establishes a 24/7 contact centre as well as establish structures to promote CyberSecurity, information sharing and capacity building.

4.3.2. Case Law: Germany

There is only limited impact of judicial decisions on the German legislation. Ever since the attack on the website of Lufthansa in 2001, German jurisprudence and literature began to redefine the concept of 'online' demonstration in relation to the German Constitution,[28] which protects demonstration that is peaceful and without arms.[29] Only very few judgments have led to

[27] SA Government Gazette (2011) Draft National CyberSecurity Policy Framework for South Africa.

[28] Weisser B CyberCrime – The Information Society and Related Crimes Section 2 – Special Part National Report on Germany 2.

[29] Die 'Lufthansa-Blockade' 2001 – eine (strafbare) Online-Demonstration AG Frankfurt A.M., Urt. v. 1.7.2005 – 991 Ds 6100 Js 226314/01 = MMR 2005, 863 (864).

amendments of the law on CyberCrime.[30] One of the judgements that led to legislative amendments was the judgement made by the online demonstrations that caused by the distribution of denial of service attack through the Lufthansa web servers.[31]

The first Criminal Chamber of the Frankfurt Appellate Court dropped all charges and ruled (No 1 sect 319/05) that the demonstration was in fact, non-violent and without coercion, but had been targeted at influencing public opinion.[32]

Prof Dr Bettina Weisser, the Chair of German and international law asserts that very few judgements have led to amendments to the law on CyberCrime.[33] In 2007, an amendment was effected on the German Criminal Code to include a new regulation that includes in the crime of Computer Sabotage, a provision that criminalises unauthorised entering as well as transmitting of data into computer systems. The regulation was prompted by a judicial decision of the higher Regional Court of Frankfourt a.M.[34]

The case entailed the conducting on line demonstration consisting of denial; of service attack against the website of the German Lufthansa. The said protest was instigated against the company's support of the German deportation practice that was manifest by flying foreign illegal residents out of the country. [35]The aim of the Lufthansa attack was to hamper access to the website by simultaneous access from a large number of internet users to the website.

The actors planned to demonstrate against the participation of Lufthansa in the so-called „deportation-business" The Court argued that the conduct of online demonstration cannot be a criminal offence under Germany Penal code as the temporary suppression of access of data was

30 Weisser (note 28 above) 2.

31 Court of Frankfurt a.M. (22.5.2006-1Ss3119/05).

32 AG Frankfurt a.M., Urt. v. 1.7.2005 – 991 Ds 6100 Js 226314/01 = MMR 2005, 863 (864).

33 Weisser (note 36 above) 3.

34 22.5.2006-1Ss3119/05

35 Higher Regional Court says online demonstration is not force in Germany(1.06.2006)http://www.heise.de/newsticker/meldung/73755

not punishable.[36] The subsequent amendment that is provided for in Section 303 [37]of the German Criminal Code stipulates that entering or transmitting data with the intention of causing damage to another is a criminal offence.

4.3.3. Legislation

Germany ratified the Council of Europe Convention on CyberCrime in 2009 and has amended the Criminal Code,[38] which now contains comprehensive provisions on computer crime and CyberCrime. Germany also has modern electronic commerce and electronic signature laws in place. Like most European countries, Germany has comprehensive privacy legislation, but it includes onerous registration requirements that may act as a cost barrier for the use of cloud computing. In addition, Germany has seventeen Data Protection Authorities, but the lack of boundary management leads to uncertainty in the application of the law. Germany has a strong commitment to international standards and interoperability, which has improved with recent policy revisions.[39] By way of comparison, South Africa has promulgated various pieces of legislation, notably, the ECT Act that provides for validity of electronic transactions, and digital signatures as well as Cyber Inspectors. However, the legislation has not fully been implemented as no Cyber Inspectors have been appointed.

Within the South African context, Sections 53 to 56[40] of the CyberCrime and CyberSecurity Bill that establishes CyberResponse Committees, prescribes various governance structures to develop standards to promote CyberSecurity and timely incident reporting, processing, Cyber foresight as well as transnational information sharing.

---

[36]Die „Lufthansa-Blockade“ 2001 – eine (strafbare) Online-Demonstration AG Frankfurt a.M., Urt. v. 1.7.2005 – 991 Ds 6100 Js 226314/01 = MMR 2005, 863 (864).

[37] German Criminal Code (Section 303b): Translation of the German Criminal Code provided by Prof. Dr. Michael Bohlander and accessed from https://www.gesetze-im internet.de/englisch_stgb/englisch_stgb.html on 14 Sept 2017

[38] ‘Strafgesetzbuch’

[39] Country Report (note15 above).

[40] CyberCrime and CyberSecurity Bill of 2017.

Germany has demonstrated international commitment to protect society against CyberCrime by signing (2001) and ratifying (2009) the COECC as well as domesticating it to ensure enforcement. Further commitment has been displayed by the signing and ratification of the Additional Protocols to the Convention on CyberCrime that focus on criminalisation of acts of a racist or xenophobic-natured committed through computer systems.[41] South Africa signed the COECC, but has not ratified. Provisions of Article 2-9 of the Convention are reflected in the South Africa Copyright Act, Films Publications Act, and the ECT Act. Watney argues that the alignment of South Africa with Brazil, Russia, India, China, and South Africa (BRICS) might prevent South Africa from ratifying the Convention.[42]

National Report on Germany,[43] published in 2013, affirms the nonexistence of a special code of CyberCrime but situates computer related crimes in various other codes and special laws with the German Criminal Code providing a legal base for the computer related offences. German Criminal Code[44] contain provisions (202-206) that offences created by violation of privacy through phishing, data espionage, acts of preparatory of data for espionage as well as acts of preparation for espionage. The same provisions are envisaged by the CyberCrime and CyberSecurity Bill of 2017.

CyberCrimes as depicted in the German Criminal Code relate to certain criminal behaviour that is propagated through the use of computer systems. The German Criminal Code covers criminal damage caused by data tempering computer sabotage,[45] encouraging the commission of serious crimes threatening territorial integrity, distribution, acquisition and possession of pornographic materials, performances through broadcast,[46] data interception,[47] stalking, fraud, sabotage

41 See (note 5 above) 7.

42 Watney MM 'The way forward in addressing CyberCrime regulation on a global level' (2012) 1:1/2 *J Internet Technol Secur Trans* 62.

43 Weisser B 'CyberCrime: The Information Society and related crimes' (2013) *National Report on Germany* 2.

44 Criminal Code (note 2 above) Sect.

45 Section 303 of the German Criminal Code: Translation of the German Criminal Code provided by Prof. Dr. Michael Bohlanderas.

46 'Urheberrechtsgesetz' Criminal Code (note 2 above) Sect 184.

47 Criminal Code (note 2 above) Sect 202b.

,organising and participating in unlawful gaming as well as violation of private secrets and breach of official secrets and confidentiality.[48] If we compare the position with South Africa, the same provisions are covered adequately in Chapter 2 of the CyberCrime and CyberSecurity Bill of 2017.

In addition to the offences articulated in the German Criminal Code is the German Copyright Act[49] that criminalises unauthorised exploitation of copyright, infringement of neighbouring rights and unlawful commercial focused exploitation. The Telecommunication Act also provides for criminal offences as well as acts against unfair competition that criminalises disclosure of trade and industrial secrets. Federal Data Protection Act provides for lawfulness of data collection, processing and use in quest of protection of personal information. Within the South African Context, the Copyright Act, Electronic Communication and Transactions Act as well as Protection of Personal Information Act (POPIA) equally contain similar provisions. Further, these provisions are captured in the CyberCrime and CyberSecurity Bill.

In July 2015, Germany promulgated a new IT Security Act[50] whose object is that of preventing the loss of important IT systems such as those used by the BSI, telecommunications providers, and critical infrastructure operators.[51] Other acts aim is to provide minimum CyberSecurity standards as well as minimum-security requirements to realise improvements of the availability, authenticity, confidentiality, and integrity of IT security throughout Germany. Increased internet security for citizens and better protection of critical infrastructure are of national importance. Germany has promulgated other laws that directly prohibit CyberCrimes such as computer fraud, data tampering, computer sabotage, data espionage, phishing, as well as other related CyberCrimes through the prosecution of the traditional crime statutes[52]

Germany has further, passed the IT Security Law (BSI) that aims to force the 'operators of critical infrastructure' to provide better IT security and report risks, a goal, which is shared by almost

48 Criminal Code (note 2 above) Chap 15.

49 German Copyright Act (KUG).

50 Federal Data Protection Act (BDSG).

51 Federal Government 'Digital Agenda 2014-2017' 5.

52 Hathaway *et al* (note 1 above) 9.

everyone in Germany, given the recent global CyberAttacks.[53] The country report recognises the Act on Framework Conditions for Electronic Commerce 2001 that implements the EU E-Commerce Directive into German law. The Directive is based largely on the UNCITRAL Model Law on E-Commerce.

Many computer offences are envisaged without any systematic approach in ensuring their application. Computer related crimes are also stipulated in various other codes and special laws. The German Criminal Code stipulates Computer-related crimes. Additional legislative frameworks that provide for criminal sanctions for offences committed in the CyberSpace. These are the Data Protection Act,[54] the German Copyright Act,[55] and the Protection of Young Person's Act[56] as well as Telecommunications Act.[57]

4.3.3.1 Legislative amendments prompted by the Case Die 'Lufthansa-Blockade' 2001

The regulation was prompted by a judicial decision of the higher Regional Court of Frankfurt[58]. The case entailed the conducting online demonstration consisting of denial of service attack against the website of the German Lufthansa. The said protest was instigated against the company's support of the German deportation practice that was manifest by flying foreign illegal residents out of the country.[59] The aim of the Lufthansa attack was to hamper access to the website by simultaneous access from a large number of internet users to the website.

The actors planned to demonstrate against the participation of Lufthansa in the so-called 'deportation-business'. The Court held that the conduct of online demonstration could not be a

53 Dr Spies is the author of AICGS Issue Brief 46: German/U.S. Data Transfers: Crucial for Both Economies, Difficult to Regain Trust 1.

54 Federal Data Protection Act (note 46 above).

55 German Copyright Act (KUG) (note 45 above).

56 Protection of Young Person's Act (JuAshG).

57 Telecommunications Act (TKG).

58 a.M. (22.5.2006-1Ss3119/05.

59 Higher Regional Court says online demonstration is not force in German (1.06.2006) available at: http://www.heise.de/newsticker/meldung/73755 (accessed: 14 September 2017).

criminal offence under the Germany Criminal Code as the temporary suppression of access of data was not punishable.[60] The subsequent amendment provided for in Section 303[61] of the German Criminal Code stipulates that entering or transmitting data with the intention of causing damage to another is a criminal offence.

4.3.3.2 Scarlet Extended SA v Société Belge des Auteurs, Compositeurs et Editeurs SCRL (SABAM)

Germany has strict censorship laws in place relating to specific online content with specific focus on principally holocaust denial and related content. These laws are regularly enforced by State Courts. Plans to introduce mandatory internet filtering, principally against online child pornography, were abandoned in April 2011. This coincided with a preliminary decision by the Advocate General of the European Court of Justice, which states that no ISP may be forced to filter the internet as this would breach European privacy and human rights laws in the case of the German Constitution that promotes the Universal Declaration of Human Rights.[62]

The above was determined in the case of *Scarlet Extended SA v Société Belge des Auteurs***,** *Compositeurs et Editeurs SCRL (SABAM) 426*,[63] entailing the installation of a system for filtering electronic communications in order to prevent file sharing which infringes copyright. The main issue before the Court of Justice was to determine whether under the EU Directives 2000/31,[64] 2001/29, 2004/48, 95/46, 2002/58, and in light of the applicable fundamental human rights, it is proper to issue an injunction against an ISP to introduce a system for filtering all electronic

---

60 Die 'Lufthansa-Blockade' 2001 – eine (strafbare) Online-Demonstration AG Frankfurt a.M., Urt. v. 1.7.2005 – 991 Ds 6100 Js 226314/01 = MMR 2005, 863 (864).

61 German Criminal Code (sect 303b): Translation of the German Criminal Code provided by Prof. Dr. Michael Bohlander available at: https://www.gesetze-im internet.de/englisch_stgb/englisch_stgb.html (accessed: 14 September 2017).

62 The Second Annual Study on the Cyber Resilient Organisation: Germany Ponemon Institute, February 2017 1.

63 ECLI: EU: C: 2011:771: Case C70/10.

64 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of Information Society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

communications for an unlimited period and at its expense in order to block unlawful use or transfer of copyrighted works.

The Court first noted that under Article 8(3) of Directive 2001/29[65] and Article 11 of Directive 2004/48, 'holders of intellectual property rights may apply for an injunction against intermediaries, such as ISPs, whose services are being used by a third party to infringe their rights'.[66] Relying on its case-law, the Court further explained that those directives permit national courts to issue orders against 'intermediaries to take measures aimed not only at bringing to an end infringements already committed against intellectual-property rights using their Information-society services, but also at preventing further infringements'[67] The Court, however, emphasised that such orders should not violate Article 15(1) of Directive 2000/31 against adopting measures that 'would require an ISP to carry out general monitoring of the information that it transmits on its network'.[68] Additionally, the Court held that an injunctive order against an ISP should not be incompatible with Article 3 of Directive 2004/48,[69] which prohibits unfair, disproportional or excessively costly measures imposed on internet intermediaries.

Based on the foregoing standards, the Court found that the obligation imposed on Scarlet to install a filtering system in order to identify and block unlawful use of file sharing would in effect demand the company to carry out a costly general monitoring function for an unspecified period, which is contrary to Directive 2000/31. Furthermore, the Court noted that the fundamental right to property, which includes the protection of intellectual property rights 'must be balanced against the protection of other fundamental rights'[70] Here, the order to install a filtering system only concerned the interests of copyrights holders in musical works. Yet the measure would not only limit Scarlet's right to conduct business, it could also infringe the fundamental rights of the internet users, namely

65 001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the Information Society.

66 Para 30.

67 Para 31.

68 Para 35.

69 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

70 Para 44.

the rights to the protection of personal data and freedom of expression respectively guaranteed under Articles 8 and 11 of the EU Charter of Fundamental Rights.

In view of the above-mentioned reasons, the Court concluded that the injunction against Scarlet company was incompatible with the EU Directives 2000/31, 2001/29, 2004/48, 95/46[71] and 2002/58,[72] construed in the light of the fundamental rights to protection of personal data and freedom of expression.[73]

Germany has established a mature institutional ability to address different elements of CyberCrime. These institutions include National CyberResponse Centre, BSI and the Federal Criminal Police Agency (BKA) that jointly lead the national CyberCrime efforts. Further interstate collaborations have realised a Germany that participates in various intra-state and inter-agency partnerships to foster information sharing. One of these being US-Germany Cyber Bilateral Meeting serves as a recognised partnership to facilitate sharing of CyberSecurity assets across borders.[74] Within the South African context, Section 53 and 54 of the South Africa CyberCrime and CyberSecurity Bill establishes structures to deal with CyberSecurity. The CyberResponse Committee shares of information relating to CyberSecurity incidents to ensure detection, prevention, investigation and mitigation of CyberCrime. Section 55 – 58 provides for a declaration of nodal points and the Private Sector Security Computer Incident Response Teams as well as the Identification Protection and Auditing of critical information infrastructure.

To deepen the Cyber astuteness and ensure sustainability of the interventions focused on Germany IT security research capability, Germany has prioritised empowerment through continuous professional development of state officials. The intervention also focused at addressing the significant shortage of CyberSecurity professionals, especially in government

---

71 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

72 S 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

73 Scarlet Extended SA v Société Belge des Auteurs, Compositeurs et Editeurs SCRL (SABAM) ECLI: EU: C: 2011:771: Case C70/10.

74 Hathaway *et al* (note 1 above) 10.

service. In recognition of need to create a secure global CyberSpace, Germany routinely addresses development cooperation issues and participates in projects dedicated to Cyber Capacity building, CyberSecurity capacity building, and Cyber Confidence building in developing countries.[75] The greatest achievement has been the establishment of an International Cyber Policy Coordinating Capability and the establishment of a functional Cyber and Information Space Command Capability in 2016.[76]

The CyberResilience Report presents a positive correlation between CyberResilience and Security Posture. The research also revealed that a CyberSecurity Incident Response Plan (CSIRP) applied consistently across the entire enterprise with senior management support makes a significant difference in the ability to achieve high level CyberResilience.[77] The report further claims that CyberResilience is affected by the length of time it takes to respond to a security incident, hence the need to profile incident response platform and to share threat intelligence as key initiatives for improving CyberResilience.[78]

In embracing the basic tenant of internet technology as a possibility to boost the economy, apart from the aforementioned publication of guidelines addressing Cyber threats, the authorities have adopted initiatives to build the future for sustainability. The building for the future strategy entails intensification of research on IT security, promotion of further training for personnel and dedication of more resources to tackle CyberThreats. Also, the Federal Ministry of Economics and Technology has set up a task force on 'IT security in industry' in order to support small and medium sized businesses in protecting their infrastructures. Overall, State agencies are expected to promote awareness among private users (businesses and citizens) by providing better information and education relating to IT security (Awareness Promotion Proposition (APP).[79]

---

75 Hathaway *et al* (note 1 above).

76 Potomac Institute for Policy Studies 'Cyber readiness index: Country profiles' available at: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index (accessed: 31 August 2017).

77 The Second Annual Study on the CyberResilient Organisation: Germany Independently conducted by Ponemon Institute Sponsored by Resilient, an IBM Company Publication Date: February 20171-2.

78 Second Annual Study on the CyberResilient Organisation (note 73 above).

79 Second Annual Study on the Cyber Resilient Organization (note 73 above) 1-2.

4.4. Conclusion

Analysis of the German Criminal Code portrays features that embellish the COECC as it relates to Article 8 as well as the criminalisation of various offences that relate to unauthorised use, denial of service as well as the utilisation of the platform to commit crimes. These provisions resonate with the provisions of Section 86 of the South African legislation on ECT Act as well as the provisions of the CyberSecurity and CyberCrime Bill. The legislation further makes provisions that criminalise specific offences within the German Criminal Code, which triangulates across other legislative frameworks and resonate the Chapters 2[80] and 3[81] provisions of the South African CyberCrime and CyberSecurity Bill of 2017. South Africa has also domesticated the provisions of Article 8 within the Copyright Act [82], which has since been amended to include neighbouring rights, the Films Publication Act[83] that criminalises possession, acquisition and distribution of pornographic material as well as the ECTAct and the POPIA, just to name a few.

The existence of a comprehensive CyberCrime, privacy legislation with modern electronic commerce and Electronic Signatures in place as well as up-to-date intellectual property provides Germany with reasonable protection for cloud computing services. The liability Web hosting businesses and access providers for copyright breaches that occur on their systems however, remains uncertain. The German *status has similarities to* the South African CyberCrime legislative developments. South Africa, like German, through the ECT Act, currently does not place liability on the service provides for online harassment and stalking but requires the orders on take down, to be effectively implemented. The Bill further strengthens the shortcomings of the ECT Act, prescribes obligations for electronic communication service providers and financial institutions.[84]

---

80 CyberCrimes: sect 2 – 15 of the CyberCrime and CyberSecurity Bill of 2017.

81 Malicious Communications: Sections 16 to 22 of the CyberCrime and CyberSecurity Bill of 2017.

82 Act 98 of 1978.

83 Act 65 of 1996.

84 Clause 52 of CyberCrime and CyberSecurity Bill of 2017.

CHAPTER 5: RUSSIA

5.1. Introduction

Russia is a member State of the Council of Europe but in protection of its sovereignty, has not signed the Council of Europe Convention on CyberCrime. Like South Africa, Russia is an active player with Brazil, Russia, India, China and South Africa (BRICS). Russia is the most influential actor in terms of hard security and seems to be the only power that has both the means to react to a crisis and a sense of responsibility to engage. The responsibility to react to or to intervene in events in what it considers as its neighbourhood, is limited though and would only be translated into action if key Russian interests (or territory) were to be directly affected. In this sense, Russia can be qualified as the 'reluctant soldier'.[1]

Russian doctrines and strategy papers emphasise that Information Security is not explicit on words like 'CyberSpace', 'CyberAttacks' or 'CyberWarfare'. The disposition of Russian leaders towards CyberSecurity is premised on the attribution and profiling of information 'valuable asset', which needs to be protected 'in times of peace and war'. As such, Cyberattacks are gleaned as elements of Information Warfare. National security of the Russian Federation depends on the level of Information Security. Thus, it is believe that with technical progress this dependence is bound to increase. Russia constitutes a very large population of internet users in Europe with its critical infrastructure and military systems heavily relying on digital technologies and communication networks.

The Exponential growth in CyberCrime has been attributed to the increasing dependency on information technologies as well as the disbanding of the Federal Agency for Government Communication and Information, which resulted in employees being recruited by hacker groups. These hacker groups claim responsibility for several malicious and unlawful Cyber Activities, Denial of Service attacks, hosting of fraudulent websites for criminal organisations as well as the provision of malware and distribution of child pornography, phishing, scams spamming and online

[1] Peyrouse S, Jos B & Marlène L 'Security and development approaches to Central Asia: The EU compared to China and Russia' (2012) *Eurasian Centre* 5.

gambling.[2] These provisions are enshrined in the ECT Act, the Films and Publications Act as well as the CyberCrime and CyberSecurity Bill within the South African context.

CyberSpace: CyberSpace is perceived by the Russian Government as something that the State has no control over yet. However, if a State wants to retain its sovereignty, it is argued, it should also be able to regulate and monitor the information sphere. In this sense, oversight over any phenomenon – information technology in this case, is seen as the most natural thing and has to be protected at all costs.[3]

5.2. Policy and legislation

5.2.1. Overview

Russia views internet sovereignty as national interest and at the heart of national security. The ability of the government to monitor and, if necessary, control the information domain is an essential element of the Russian position on CyberSecurity, which remains a key component of Russia's international efforts on Cyber Issues to date. This position remains an important point of disagreement with the U.S. and other mature democracies.[4] The Russian government is still controlling online communication to a much higher degree and protests for a free internet are often repressed by State forces. Van Epps further argues that Russian internet restriction bill, which initially was created as a blacklist of internet sites with contents that is seen as harmful to children, is considered to be used for censorship of online contents of a broader kind. Russia positions itself as the leading nation of an international coalition of new governmental powers of internet regulation, especially within the organisational frame of the Shanghai Cooperation.[5]

---

2 Orji UJ *CyberSecurity Law & Regulation* (2012) Wolf Legal 347.

3 Van Epps G 'Common ground: US and NATO engagement with Russia in the Cyber domain' (2013) 12:4 *Connections: The Quarterly Journal*.

4 Van Epps (note 3 above).

5 Van Epps (note 3 above).

5.2.2. International Information Security 2020 Policy Position[6]

In September 2000, the Russian government adopted the Russian Information Security Doctrine as the country's National Policy to inform CyberSecurity, which embraces the protection of Russia's national interests in the information sphere whose posture is rooted in balancing of the individual, the State and societal interests.[7] The Russian Information Security Doctrine focuses on data protection, personal privacy, access to and hacking of State Information. The Russian Federation State Policy is premise on a foresight International Information Security 2020, a contribution to national security, rooted in an international system that facilitates equitable partnerships in the global information space to counter the threats that characterise the International Information Security landscape whilst embracing the national interests of the Russian Federation.

The major threat identified by the Russian Federation is the use of information technologies as a weapon for military and political purposes, which violates International Law principles, causing hostilities or aggression that are aimed at discrediting the sovereignty and territorial integrity of States and thus also threatening International peace, security and stability.

For terrorist purposes, this threat broadly encompasses recruitment for terrorist activities as well as causing destruction on critical information infrastructure and interfering in the affairs of sovereign States. It also encompasses violation of public order, incitement of interethnic, inter-racial and inter-confessional strife as well as advocacy of racist and xenophobic ideas that ignite hatred, discrimination and violence as well as crimes, which include the unauthorised access to computer information, creation, use and dissemination of malicious computer software.[8] Within

---

6 Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020 available at: https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf (accessed: 24 August 2016).

7 Orji 2012 (note 2 above) 356.

8 Basic Principles for State Policy (note 6 above).

the South African context similar provisions are contained in Chapter 2[9] and 3[10] of the South African CyberCrime and CyberSecurity Bill 2017.

Based on the above threat analysis, the Russian Federation has identified five strategic priorities to be addresses by the international Information Security 2020.[11] Firstly, the establishment of an International Information Security System at bilateral, multilateral, regional and global levels that creates conditions for international promotion of the Russian initiative to develop and adopt the Convention on International Information Security by the United Nations member States, promote bilateral and multilateral consultations of experts. These consultations are expected to coordinate the positions and plans with member States across all multilateral organisations. This includes the Shanghai cooperation organisation, participating States of the Commonwealth, members States of the Asian Pacific Economic Cooperation, BRICS states, G8 and G20 member States as well as harness scientific, research and the expert potential of the United Nations and other international organisations to advance Russia's initiatives in establishing an International Information Security System. Chapter 6[12] of the CyberCrime and CyberSecurity Bill provides mutual assistance for the prosecution of transnational crimes.

The second strategic priority focuses on realising reduced risks in the use of Information and Communication Technologies to carry out hostile activities that discredit sovereignty, violate territorial integrity and threaten international peace and security through development of regional and global information systems based on universally recognised principles and standards of international law. At the centre is the creation of bilateral and multilateral collaborations of confidence building measures to counter threats in the use of Information and Communication Technologies to carry out hostile activities and acts of aggression.

The third priority is the establishment of mechanisms of international cooperation to counter the threats of using Information and Communication Technologies for terrorist purposes. This priority is premise on strengthening cooperation among participating member states to mobilise

9 Section 2 to 15 CyberCrime and CyberSecurity Bill of 2017.

10 Sections 16 to 22 of the Bill of 2017.

11 Basic Principles for State Policy (note 6 above) 5-6.

12 Sections 44 to 49 of the Bill.

contributions to the prevention, detection, suppression, disclosure and investigation of destructive acts targeting national critical information infrastructure as well as encourage UN member States to prepare and adopt the instrument on procedure for exchange of information on best practices to strengthen the security of critical information infrastructure elements.[13]

The fourth priority is the creation of conditions to counter threats in the use of Information and Communication Technologies for extremist's purposes, including interfering with the internal affairs of sovereign States through the establishment of international mechanism for continuous monitoring.

The fifth priority is the promotion of effective international cooperation in countering CyberCrime through the adoption of the Convention on Cooperation in Combating CyberCrime at the UN level as well as at multilateral levels. This cooperation provides for the exchange of information between law enforcement agencies of States in the course of investigation of crimes as well as the exchange of judicial practices concerning crimes. It is also intended to promote the development of international programmes designed to bridge the gap between developed and developing countries as well as promote the expansion of National Information Infrastructure to realise a world community in the creation and use of Global Information Networks and Systems.[14]

5.2.3. Legislation

5.2.3.1 Criminal Code of the Russian Federation

The Criminal Code of the Russian Federation[15] establishes several provisions on CyberSecurity with regard to illegal access, misuse of computing devices, unauthorised system interference, unauthorised modifications and online pornography.[16] The Code prohibits unauthorised access to legally protected computer information,[17] conducts constituting the creation and dissemination

13 Russian Federation in the Field of International Information Security 2020 (note 6 above) 2.

14 (Russian Federation in the Field of International Information Security 2020 (See note 6 above) 4.

15 The Criminal Code of the Russian Federation No. 63-Fz of 13 June 1996 (amended in 2012).

16 Butler WE *Criminal Code of the Russian Federation* (1998) Simmonds & Hill art 242.

17 Art 272(1) Russian Criminal Code.

of computer viruses for purposes of causing intended changes to existing programmes and unauthorised system and data interference.[18] The Code further creates liabilities for the violation of intellectual property rights and prohibits acts constituting attempts at aiding, or abetting of CyberCrime offences.[19] These same offences are envisaged in the CyberCrime and CyberSecurity Bill,[20] ECT Act and the Copyright Act in South Africa.

Regarding the extradition of Russian nationals, the Russian Criminal Code does not create a legal basis for extradition of offenders, as it does not provide for extradition of Russian nationals who have committed CyberCrime offences in other States.[21] Regarding foreign or stateless persons, the Russian Criminal Code permits the extradition for persons who have committed CyberCrime offences in other countries where such persons are found within the territory of the Russian Federation.[22] The South African ECT Act[23] and CyberCrime and CyberSecurity Bill provide for extraterritorial jurisdiction, mutual assistance as well multilateral agreements with foreign States.[24]

5.2.3.2. International treaty positioning

In the international arena, the Council of Europe Convention on CyberCrime (COECC) remains the first major ground-breaking regional agreement, which has been adopted by thirty-nine mostly European countries — including the U.S. but not Russia — since its initiation in 2001. Russia, however, objects to ratification of the aforementioned treaty, as it views the treaty as an infringement on its sovereignty. Russia's objection to the European Convention on CyberCrime provides the inherent mandate that allows the police to open an investigation of suspected online crime originating in another country without first informing local authorities, thus, infringing on traditional ideas of territorial sovereignty. This, Russia believes, would invite demands for cooperation in identifying, for example, the perpetrators of the CyberAttacks on Estonia in 2007

18 Art 272(2) of Russian Criminal Code.

19 The Criminal Code of the Russian Federation No 63-Fz of 13 June 1996.

20 Section 2 of the CyberCrime and Cyber Security Bill.

21 Article 12(1) of the Russian Criminal Code.

22 Article 13(2) of the Russian Criminal Code.

23 Section 90 of ECT Act.

24 Section 23 & 59 of the Bill.

or Georgia in 2008, along with requests from foreign law enforcement agencies in shutting down the extensive CyberCriminal activity that originates from Russian territory.[25] Russia believes that international collaboration across law enforcement agencies should act a better deterrent to CyberCrime without threatening territorial integrity than the COECC.[26]

Russia has emphasised the need for a new international regime that more closely corresponds to its views on CyberSecurity. Unlike America, Russia favours an international treaty along the lines of those negotiated for chemical weapons and has pushed for that approach at a series of meetings this year and in public statements by high-ranking officials.[27] Russian officials and academics consistently espouse a position that existing international law is inadequate and that new accords are necessary to affirm National Sovereignty and to deter aggressive behaviour in CyberSpace. Markof asserts that the Russian government repeatedly introduced resolutions calling for CyberSpace disarmament treaties before the UN, which have vehemently been opposed by the United States from a philosophical perspective.[28] As an initiative to deal with unknown CyberAttacks, Russia has alongside the disarmament agenda sponsored proposals, which include the application of humanitarian laws banning attacks on non-combatants and a ban on deception in operations in CyberSpace. The Russians have also called for broader international government oversight of the internet, which has been perceived by other States as censorship.[29]

Legal and Regulatory Frameworks, dealing with Information Security are viewed as imperfect, with deterioration in the protection of State secrets and data privacy, which is further compounded by strategic budgeting fiscal constraint realities and insufficient coordination among authorities. Russia's internet is generally regulated under the Law on Mass Media[30] because the authorities interpret the internet as an extension of media space, with the consequence that bloggers and

---

25 Markof J & Kramer AE 'US and Russia differ on a treaty for CyberSpace' (2009) *The New York Times* 28.

26 Markof *et al* (note 25 above).

27 Markof *et al* (note 25 above) 3.

28 Markof *et al* (note 25 above) 3.

29 Markof *et al* (note 25 above) 2.

30 Law on Mass Media (No 2124-1).

website owners are responsible for their website contents. Russian politicians have often expressed their ambitions to have an overall control of the Russian CyberSpace in implementing the Chinese-style filtering method.[31]

5.2.3.3. Institutional Regulatory Mechanisms

The Russian threat analysis informs the institutional arrangements for compliance monitoring. The three threat dimensions to CyberSecurity that inform Russia's policy trajectory, criminal threats, terrorist threats and military/political threats have resulted in the creation of three Ministries that focus on the identified threats. The Ministry of Internal Affairs is responsible for countering CyberCrime, whilst the Ministry of Defence is responsible for CyberWarfare and the Federal Security Services is responsible for curbing CyberTerrorism, ensuring internal security and state control.[32]

Russia has a national Emergence Response Team that is mandated to deal with interventions to prevent computer incidents and provide response services to all Cyber Users where the incident relates to resources located within the territorial borders of the Russian Federation. The Team interacts with the Russian law enforcement agencies on CyberCrime issues and as such provides the relevant assistance.[33] Similar responsibility is mandated in Section 53 to 55 of the CyberCrime and CyberSecurity Bill to various structures. The CyberResponse Committee that has representation across all organs of State, the Computer Security Incident Response Centre that has been mandated for State Security as well as the Nodal point for the establishment of the Private Sector Computer Security Incident Response Team, which is mandated to the Executive Authority responsible for Telecommunications and Postal Services.[34]

---

31 Ministry of Foreign Affairs of the Russian Federation: Information Security Doctrine of the Russian Federation.

32 Orji 2012 (note 2 above) 355.

33 Orji 2012 (note 2 above) 356.

34 Section 54 & 55 of the Bill.

5.3. Concluding remarks

The three threats that inform the global information security agenda of the Russian Federation, criminal threats, terrorist threats and military/political threats are addressed in the Convention on CyberCrime, which Russia has not signed due to concerns for the protection of its sovereignty. Analysis of the initiatives reflected in the policy trajectory on International Information Security 2020, suggests the willingness of Russia to submit to an international regime on CyberSecurity. Russia's initiative to lead the International Information Security Agenda will be fast-tracked by its participation as a member State of the Council of Europe Convention on CyberCrime. Such an initiative will also drive the rationale that Russia's proposals are not aimed at securing an advantage over technologically advanced countries due to the perceived inferiority in their communication technology.

Russia as a member of BRICS and a global player within the CyberSpace has influenced the posture of the BRICS Framework on E-commerce which has profiled CyberCrime and CyberSecurity as a priority, with emphasis on Information Security and CyberSecurity. South Africa as a BRICS member needs to conduct the appreciation of the BRICS Framework, to ensure that the rationale for participation benefits South Africans.

CHAPTER 6: COMPARATIVE ANALYSIS

6.1. Introduction

Section 39(1) of the Constitution of the Republic of South Africa states that

> *"When interpreting the Bill of Rights, a Court, tribunal or forum—*
> *(a) must promote the values that underlie an open and democratic society based on human dignity, equality and freedom;*
> *(b) must consider international law; and*
> *(c) may consider foreign law*."[1]

This provision is at the heart of the approach adopted in this dissertation in analysing domestic law governing criminal investigation of CyberCrime with reference to international and foreign responses to crime prevention, detection and investigation. A prosecution Court, forum or tribunal must, while promoting values that underlie an open and democratic society, take into consideration international law and make note of foreign law.

In embracing the above, this dissertation offers to present the global trends and international best practice dealing with CyberCrime and CyberSecurity. The dissertation presented the meanings of the concepts that characterise the globalisation of CyberCrime and CyberSecurity operating in CyberSpace. The impact of the international treaties in promoting a multilateral response to CyberCrime as proclaimed by various academics is presented in Chapter 1(one). The impact of the first ever ground breaking treaty, the Council of Europe Convention (COECC) in respect of CyberCrime and criminal investigation of CyberCrime.

[1] Constitution of the Republic of South Africa, Act 103 of 1996.

Along the same lines this international multilateral landscape that affirms the transnational nature of CyberCrime is followed by the presentation of the evolution and maturity of the regulation addressing CyberCrime. Similarly criminal investigation from Common Law, through various legislative frameworks that regulate conduct in the CyberSpace is recognised.

As a result on line gambling, Cyber stalking, phishing, creation, distribution and possession of pornography, hate speech online to mention are offences that are provided for in the CyberCrime and CyberSecurity Bill.[2] In giving substance to recognition of foreign law, a presentation of Germany and Russian jurisdiction has been elucidated in Chapter 4 and 5 with the legislative provisions compared to similar provisions within the South African Context.

Below is the overview analysis and comparison of the approaches to CyberSecurity, risk appetite, governance posture and norms and standards to govern CyberSpace as gleaned from the perspectives of foreign jurisdictions, Germany and Russia. The implications for the South African CyberSecurity posture are also extrapolated. A summation of the strategic posture in relation to CyberCrime and CyberSecurity adopted by the two jurisdictions is herein presented. This posture bears similarity with the narrative the jurisdiction has adopted towards CyberCrime.

The Criminal Codes that inform the various jurisdictions will also be presented by way of comparison which has influence dimensions of National security, economic, political and social security. Consequently the analysis closes with the implication for the South African CyberCrime and CyberSecurity Landscape.

Recognition of the right to safe and secure CyberSpace is a *Sui Genesis* right and cross cutting domain is herein acknowledged. It is worth noting that the balance between embracing the international Human Rights Agenda while ensuring protection of National Interests and Critical Infrastructure. Inherent in the analysis is the role of the state in promoting international trade while protecting National Interests.

---

[2] Papadopoulos, S & Snail, SL *Cyberlaw @ SA III: The law of the Internet in South Africa* (2012) Van Schaik: Pretoria 333-334

The Chapter closes with the generic presentation of the Governance Risk and Compliance requirements to foreground and internal, external and allocative efficient CyberCrime and CyberSecurity legislative regime across Land, Air, Marine and OuterSpace dimensions.

6.2. Approaches to definition of CyberSecurity

In providing an alternative to the non-existence of a uniform definition for CyberSecurity, Lujif *et al* cited the initiative by the joint Russian-United States bilateral working group of the East West Institute (EWI) and Moscow University developed a framework that focuses on the harmonisation visibly demonstrated by an accepted definition of CyberSecurity.[3] According to them CyberSecurity is "a property of CyberSpace that has ability to resist intentional and unintentional threats and respond and recover"[4] Germany has opted for a definition that portrays a risk acceptance dimension as evidenced by its definition that situates 'Global CyberSecurity as an end state of the IT security situation characterised by risk of (global) CyberSpace that has been reduced to an acceptable minimum'.

6.4. Norms and standards for CyberSpace

6.4.1. Russia

In response to the COECC, Russia presented proposals, including the 2011 letter to the UN Secretary-General, which it co-authored with China, Tajikistan and Uzbekistan, highlighting three aims. The first aim is to constrain or limit competing US initiatives to develop norms in CyberSpace, which they view as a means of consolidating the US competitive advantage in CyberSpace. Secondly, to affirm the rights of countries to monitor and control the flow of information over the internet, which they see as essential ensuring domestic security. Thirdly, to prevent the further development or proliferation of offensive Cyber Weapons. This position lies in sharp contrast with the Western emphasis on commitment to the free flow of information,

---

3 Luiijf E, Bestselling K & De Graaf P 'Nineteen national CyberSecurity strategies' (2013) 9:1/2 *International Journal of Critical Infrastructures* 2.

4 Luiijf, Beselling & De Graaf (n 3 above) 3.

measures to combat CyberCrime, and State responsibility for internet activity occurring within a country's borders.

These differences might appear irreconcilable, thus limiting the odds of achieving consensus on an international framework for Cyber Operations. However, there are many points of agreement that provide a starting point for cooperation. These areas of concurrence situate within securing supply chains, protecting critical infrastructure, sharing information on threats, and combating internet use by drug traffickers.

Russia, with its focus on information security as a national and strategic interest, has adopted a Criminal Code[5] that provides for Crimes in the sphere of computer information. The Provisions criminalise illegal accessing of computer information[6], creation, use and dissemination of harmful Computer viruses,[7] violation of rules for the operation of computers, computer systems or networks[8] as well as crimes against the fundamentals of the constitutional system and state security.[9]

6.4.1.1. *Framework for BRICS E-Commerce Cooperation*

Geostrategic and international trade positioning has located South Africa within the BRICS, which is a group of emerging economies consisting of Brazil, Russia, India, China and South Africa. The objectives foregrounding the BRICS architecture entail development and strengthening of cooperation between the member nations for development, provide financial assistance provided through the New Development Bank (NDB), support of various projects, infrastructure rejuvenation. BRICS views E-commerce, as one of the most dynamic economic activities, that drives modern trade by generating employment, transforming and upgrading traditional industries, stimulating domestic demands, as well as facilitating global trade and investment growth and promoting supply chain efficiency. Russia and China have proposed the Framework which will

5 The Criminal Code of The Russian Federation No. 63-Fz Of June 13, 1996.

6 The Criminal Code (note 8 above) art 272.

7 The Criminal Code (note 8 above) art 273.

8 The Criminal Code (note 8 above) art 274.

9 The Criminal Code (note 8 above) art 275.

have an impact on the CyberCrime and CyberSecurity posture of the BRICS member states. South Africa, as a member will opt to embrace this framework which will present an opportunity loss to the ratification of the CoECC by South Africa.

6.4.2 Germany

Germany has ratified the Council of Europe's Convention on CyberCrime, thus adopting the substantive, procedural law measures and international cooperation provisions whilst South Africa, has not ratified the CoECC but has complied with the substantive provisions of the Convention, though it has not yet passed the essential legislation to ensure compliance with international obligations whilst protection the human rights provisions of privacy.

Germany regards internet as central to economic activity and economic growth and has adopted aggressive legislation against information technology crime. The German Criminal Code[10] has undergone amendments, as a result of case law, to provide for the different forms of modern crime. In which Section 184 of the Code criminalises the distribution of pornography, Section 202(a) criminalising espionage. Section 263 criminalises fraud in general, whilst 263(a) criminalises computer fraud. Section 303(a) & (b) criminalises data alteration and computer sabotage respectively. The legal interest protected against virus programs being the '*unimpaired disposability of data by the right holder'*[11]

6.4.3 South Africa

Within the South African Context, the ECT Act provided for criminalisation in Section 87 – 89 but the lack of implementation of the provision dealing with cyber inspectors has rendered enforcement of monitoring of compliance non-existent. The CyberCrime and CyberSecurity Bill[12] establishes CyberCrimes as Offences against the integrity, confidentiality and availability of data,

---

10 *Strafgesetzbuch* (StGB).

11 Papadopoulos S & Snail SL (note 2 above) 100.

12 Summary of CyberCrimes and CyberSecurity Bill 2017 available at: https://www.ellipsis.co.za/.../Summary-of-CyberCrimes-and-CyberSecurity-Bill-2017 6.

computer programs, data storage mediums and computer systems;[13] Offences committed or facilitated by means of data, computer programs and computer system.[14]

Lastly, the Bill criminalises malicious communications through data messaging[15] as well as compulsion to electronic communication service providers to assist the Courts by providing particulars of a person who distributed the malicious communication in order to ensure that the interim protection order can be served. Whilst reaffirming the provisions articulated in Sections 87 to 89, it creates many new offences. Some are related to data, messages, computers, and networks. This relates to hacking, unlawful interception of data, ransom ware, Cyber Forgery and uttering or Cyber Extortion, and gives Courts the jurisdiction to try these offences. The National Director of Public Prosecutions mandated to develop the database of the prosecutions for CyberCrimes and to include the information in the NDPP's Annual Report.[16]

6.5. Risk profiling

James argues that Political and strategic culture produce national styles and preferences in CyberSpace and this positioning, foregrounds the stance that Russia has adopted, which has integrated CyberWarfare into the grand strategy.[17] This is premise on the risk profiling as depicted by the stance that Russia holds a broad concept of Information Warfare, which includes intelligence, counterintelligence, deceit, disinformation, and Electronic Warfare, debilitation of communications, degradation of navigation support, psychological pressure, and degradation of Information Systems.[18]

From an economic point of view, Germany is apprehensive of the risk of stagnation of globalisation in the event that the CyberSecurity risk is not sufficiently addressed, while Russia

13 Section 2-7 of the Bill.

14 Section 8-10.

15 Section 17.

16 Summary of CyberCrimes and CyberSecurity Bill of 2017 (note 15 above).

17 Wirtz JJ 'CyberWar and strategic culture: The Russian integration of CyberPower into grand strategy' in Geers K *CyberWar in Perspective: Russian Aggression against Ukraine* (2015) 29-37

18 Wirtz (note 20 above) 29-37.

locates the risk within the Information Warfare space and declares Information Security as central to national security.[19]

6.6 Summary

Whilst Cyberspace has introduced a domain of high economic activity, CyberSecurity culture remains a huge strategic risk that demands quantification across all strategic thrusts that require consideration at outcome level, at output level, at activity, input as well as building for the future level of the foresight strategy map of States and Governments. Multilateral as well as regional collaborations remain the most efficient mechanisms to deal with the transnational attribute of cybercrime. South Africa has through the Cybercrime and Cybersecurity legislative developments created a platform for collaborative and partnership engagements to realise a safe and secure CyberSpace. It remains imperative that a global treaty to launch these collaborations is a non negotiable.

[19] Luiijf HAM *et al* 'Ten national CyberSecurity strategies: A comparison' (2011) *International Workshop on Critical Information Infrastructures Security Springer Berlin, Heidelberg*.

CHAPTER 7: CONCLUDING REMARKS AND RECOMMENDATIONS

7.1 Introduction

This concluding Chapter focuses on the South African perspective with the aim of distilling how South Africa has advanced or regressed in-so-far-as protecting citizens against CyberCrime, CyberTerrorism and CyberWarfare within CyberSpace is concerned. The approach adopted entails the analysis of the extent of compliance with international legal instruments as well as comparison of the proposed legislation, the CyberCrime and CyberSecurity Bill of 2017.[1]

Some recommendations are made on areas of focus to strengthen the implementation of the proposed legislation. The last section focuses on the extent to which the proposed legislation assists in providing safe and secure transactions within the other four domains. The section borrows from public hearings held by the Parliament of South Africa on the draft bill in the course of September 2017.

On 23 March 2012, South African Cabinet approved a National CyberSecurity Policy Framework for South Africa. Leading the presentation of the aforementioned Policy Framework, Minister Collins Chabane, Minister at the Presidency affirmed that, 'the framework was aimed at addressing national security threats in cyber space and it would combat CyberWarfare, CyberCrime and cyber-ills, as well as build confidence and trust in the secure use of information and communication technologies'.[2] The strategic question worth exploring is the implementation

---

1 CyberCrime and CyberSecurity Bill of 2017 Explanatory summary of Bill published in Government Gazette No 40487 of 9 December 2016.

2 ITWeb (2012) The Department of Communications (DOC) will present the National Cyber Security Policy Framework for South Africa to Cabinet in March. Available at: http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=23020: sa-to-announce-CyberSecurity-policy-in-march&catid=48: Information%20&%20 Communication %20 Technologies & Itemid (accessed: 16 November 2017).

evaluation on the extent to which the end state and foresight that foregrounds the policy have been achieved at systemic level. Such implementation evaluation should inform the system, process, organisational (POSTEDFIT) readiness to foreground the effective and efficient accountable promulgation of the CyberCrime and CyberSecurity Bill.

7.2 Overview

This dissertation has dissected the South African legislative Frameworks at aimed at embracing the end state National Development of ensuring that citizens are and feel safe in CyberSpace. The approach adopted has been through a six-layered trajectory.

The First layer has been the overview of the appreciation and recognition of CyberSpace as a sui generis and distinctive from Land, Air, Marine, and OuterSpace requiring its own distinct treaties to provide for the transnational attribute of the space. The presentation of the Genesis of the profiling of CyberSpace as well as the absence of consensus on the definition of terms that characterise the CyberSpace. The absence of consensus regarding the definition of CybeCrime, CyberSpace, CyberSecurity and CyberTerrorism was presented from various authors. Despite varied definitions, the attributes of, accountability, availability, authenticity, confidentiality, and integrity remain central in ensuring a safe and secure CyberSpace.

The Second layer as articulated in Chapter two entailed the dissection of the international landscape, wherein the role of the Budapest Convention in criminalising e offenses was profiled Continental and regional responses to the International Convention on CyberCrime were presented as well as the extent to which they embrace the human rights dimensions. The Chapter has presented continent of Africa, whose CyberSecurity developmental trajectory reflects that some African states have already established national legal and policy frameworks for CyberSecurity, while many others are developing such framework. These pro-active policies include the ECOWAS Directive on Fighting CyberCrime adopted in August 2011, the COMESA Model CyberCrime Law adopted in October 2011, and also within the SADC, the adoption of a Model Laws on Computer Crime and CyberCrime.

South Africa is a continental and regional player within SADC and the ECOSOC in promoting territorial integrity through land, air and marine border safeguarding, contributing to a safer Africa as well as a global player within the BRICS bloc. Its offensive posture within the CyberSpace must therefore, reflect these realities. Within the maritime industry, it is worth noting that South Africa is charged with the responsibility of ensuring that the maritime borders are safe for promoting trade.

The Third layer of analysis presented the South Africa's response to Budapest Convention as depicted by some domestication level in the Copyright Act, as well as Films and Publications Act. Further, the provisions contained in Section 86 to 90 of the ECT Act were also presented as an attempt to criminalise some conduct, beyond Common Law, with the delayed implementation of the enforcement provisions through cyber inspectors. On that note the role played by the National CyberCrime and CyberSecurity Framework in creating a sharper focus as well as form a basis for CyberCrime and CyberSecurity Bill.

In giving substance to Section 39(1) of the Constitution[3], recognition of German foreign law is presented the fourth layer. Admittedly ratification of the Convention of Europe on CyberCrime is reflected in the provisions of the German Criminal Code. To put it in another way the provisions of the German Criminal Code have been compared to the provisions of the CyberCrime and CyberSecurity Bill. Section 202(a) of the German Criminal Code criminalises espionage, a similar provision that is equally criminalised in the CyberCrime and CyberSecurity Bill. After all Section 263 of the German Criminal Code provides for criminalisation of fraud as well as computer aided fraud.

The same foreign law comparison is conducted for Russia as Fifth layer, a state that has not ratified the Budapest Convention as it views such as a threat to sovereignty. Russia as a member of BRICS is championing the move towards Global CyberSecurity Protocol on Peace and Security in CyberSpace. Russia focuses on information security as central to CyberSecurity.

A comparative analysis of the two jurisdictions in relation to ratification of multilateral agreements, as well as strategic positioning posture. From an economic point of view, Germany is

[3] Act 108 of 1996

apprehensive of the risk of stagnation of globalisation in the event that the CyberSecurity risk is not sufficiently addressed, while Russia locates the risk within the Information Warfare space and declares Information Security as central to national security.[4]

Chapter 7 provides the summary and recommendations regarding governance, risk and compliance to inform the implementation of the CyberCrime and CyberSecurity Bill. In an attempt to arrest the fragmented approach adopted in addressing CyberSecurity and CyberCrime exposure, South Africa initiated a process of developing a single coherent legislation. CyberCrime and CyberSecurity exposure, found expression at Common Law as well as in various legislative frameworks, notably the ECT Act,[5] which address the substantive and procedural aspects and the National Prosecutions Act[6] that deals with CyberCrime and CyberSecurity exposure.

Notwithstanding the protracted development process, whose genesis is the National CyberSecurity Policy Framework that was developed by the State Security Agency, several draft bills have been developed since 2015, coordinated by the Department of Justice and Constitutional Affairs under the leadership of the Justice Crime Prevention and Security Cluster in the Cabinet. South Africa has successfully developed the CyberCrime and CyberSecurity Bill of 2017 that was published for hearings in the course of September 2017.

Noting the inter-connectedness that exists between PAIA[7] (developed to give substance to Section 32 of the Constitution), POPIA and the CyberCrime and CyberSecurity Bill, the Information Regulator, through its submission to Parliament has recommended collaboration between the Office of the Regulator and the various organs of the State charged with the establishment and operational effectiveness of the Cyber hub, CyberCommand and the delineation of critical infrastructure and incident reporting.[8]

---

4 Luiijf HAM *et al* 'Ten national CyberSecurity strategies: A comparison' (2011) *International Workshop on Critical Information Infrastructures Security Springer Berlin, Heidelberg*.

5 Act 25 of 2002

6 Act 32 of 1998.

7 Act 2 of 2000.

8 Submission by Information Regulator (South Africa) on CyberCrime and CyberSecurity Bill of 2017 dated 14 September 2017.

The public hearings placed the essential requirement for the Bill to balance its purpose and the justiciable constitutional rights, which relate to access to information,[9] right to privacy[10] and freedom of expression.[11] The impact of multilateral cooperation on cross-border sharing of information of data subjects has sharply contrasted to the mandate of the Regulator in ensuring the protection of personal information of data subjects, and has culminated in the following proposals from the Information Regulator, which concurred with the submission by the Centre for Constitutional Rights (CCR).

a. The inclusion of the Information Regulator on the CyberSecurity Response as envisaged in Section 53 as well as the governance structures supporting CyberSecurity in terms of Section 54.
b. Reconsideration of information sharing provisions to comprehensively embrace the rights and obligations flowing from the PAIA and the POPIA.
c. Reconsideration of the provisions (Section 24 & 39) dealing with determinants of integrity of data, obtained on a computer, preservation and processing to give effect to the eight principles of data processing espoused in the POPIA.
d. Provision (Section 43) on receipt of Information by the SAPS without a warrant or due legal process to be consider rights to privacy and rights to protection of personal information.
e. General obligations of service providers to disclose certain information as provided for in Section 62 to embrace rights and duties of responsible parties as espoused in the POPIA.
f. Boundary Management as it relates to provisions (56 & 58) in relation to the declaration, identification and inspection of National critical information Infrastructures.[12]

It is of importance that the Comprehensive CyberSecurity and CyberCrime legislative framework covers the four domains, especially the maritime domain whose infrastructure forms the backbone

9 Section 32 of the Constitution.

10 Section 16 of the Constitution.

11 Section 16 of the Constitution.

12 Information Regulator South Africa Submission to Public Hearings on the CyberCrime and CyberSecurity Bill of 2017 5-6.

of global networks. This is of essence, as the Convention on the Law of the Sea does not cover crimes committed in the CyberSpace.

The Cyber Response Committee, which is functionally supported by the CyberSecurity Hub and charged with promoting CyberSecurity within the private space as is located in the Department of Telecommunications and Postal Services. Thus the CyberCommand charged with promoting CyberSecurity within the military space, located within the statutory mandate of the South African National Defence Force. The hub CyberSecurity is responsible for the collection of incidents as well as e-detection, identification and declaration of critical infrastructure and prevention, investigation or mitigation of CyberCrime, located within the State Security and the South African Police Service. It is also primarily involved with the detection, prevention and investigation of CyberCrimes.

The Chapter further presents the conclusion and wraps-up with key recommendations. The littoral posture of Africa further demands a closer focus on strengthening CyberSecurity governance and operations within the maritime domain as irreversible damage could manifest as a result of CyberAttacks as was evidenced by the Petya virus attack.

7.3 Compliance with International legal instruments

Geopolitical and Geo strategic considerations continue to define South Africa's response to multilateral treaties. South Africa adopted the COECC treaty, which provides for law enforcement to deal with trans-border CyberCrime, but has not ratified the treaty and is most likely not to, in the light of membership within BRICS and potential conflicts with ECTA provisions.[13] Within the BRICS bloc, there has been a shift in focus from the BRICS agenda to the RIC agenda on a range of issues, including security in the use of ICTs, where the emphasis is on 'adherence to universally recognised principles of international law in the use of ICTs. In particular, the principles of political independence, territorial integrity and sovereign equality of states, consequently respect for state sovereignty, non-intervention into the internal affairs of other states'. These considerations have shaped South Africa's CyberCrime and CyberSecurity Agenda.

---

[13] Watney MM 'The way forward in addressing CyberCrime regulation on a global level' (2012) 1:1/2 *J Internet Technol Secur Trans*.

South Africa, in recognition of the incoherent approach to CyberSecurity, embraced the imminent rights and duties flowing from the African CyberSecurity and Data Convention. That is resolved in 2015 to develop a South African CyberSecurity Policy, on the National CyberSecurity Policy Framework. Along the same limes the policy was criticised for reflecting the British, German and American CyberSecurity Policies without embracing privacy provisions of the Bill of Rights of the Constitution of South Africa.[14]

The Convention on CyberCrime (ETS No 185) (ECCC) is the first international treaty addressing crimes committed via the internet and other computer networks. The treaty was signed by member States of the Council of Europe and also by non-member states in Budapest on 23 November 2001 and came into force on 1 July 2004. Its main objective as set out in the preamble is to pursue a common criminal policy aimed at the protection of society against CyberCrime, especially by adopting appropriate legislation and fostering international co-operation. Its coverage includes infringements of copyright, computer-related fraud, child pornography and violations of network security as articulated in articles 2-6, which addresses offences against the confidentiality, integrity and availability of computer data and systems.[15] The Convention also provides for a range of powers and procedures relating to the search of computer networks and interception of computers. An international 24/7 network of contacts requires all participating countries to establish points of contact for transnational investigations that are accessible 24 hours daily and 7 days a week. South Africa is the only African country to sign the European Convention on CyberCrime (ECCC) and awaiting ratification and accession. The treaty is estimated to garner global support through international co-operation in fighting Cyber terrorism.[16]

Snail kaMtuze notes that the pseudo domestication of the provisions of the Budapest Convention, as demonstrated by the ECT Act, the Copyright Act 98 of 1978 as well as the Films and Publication Act 65 of 1996 illustrate South Africa's commitments to institutionalising compliance

---

14 Information Regulator (South Africa) submission on the CyberCrime and CyberSecurity Bill of 2017 dated 14 September 2017.

15 Cassim F 'Addressing the spectre of cyber terrorism: A comparative perspective' (2012) *PER* 27.

16 Cassim (note 14 above) 27.

with the provisions of the Treaty.[17] Watney argues that even though South Africa signed the Budapest Convention in 2001, its alignment with BRICS will render ratification impossible, notwithstanding the incorporation of the provisions of the Convention in various legislative frameworks as alluded to also by Snail. [18]

The establishment of the Computer Security Incident Response Team (CSIRT) signifies that South Africa's consciousness on the urgent need to tackle CyberCrime is gathering momentum. The Information Regulator mandate as ushered in by the POPIA forces deeper consideration of boundary management issues.

7.4 CyberTerrorism: Drawing linkages

South Africa's national security strategy and legislative framework, resembles the German strategic focus by every indication as the two nations focus on strategic security areas rather than objectives. These strategic security areas have become the pillars of the national security strategy. They include the protection of critical infrastructures, the creation of secure IT systems, the strengthening IT security in public administration, the establishment of the National CyberResponse Centre, the creation of the National CyberSecurity Council, Effective crime control in CyberSpace, effective coordinated action to ensure CyberSecurity nationally, continentally and worldwide, the use of reliable and trustworthy IT systems and infrastructure, personnel development in federal authorities as well as the development of just-in-time tools to respond to CyberAttacks.[19] South Africa has ratified numerous international instruments on terrorism such as the International Convention on the Suppression of the Financing of Terrorism, which was adopted by the United Nations in 1999 and ratified by South Africa in May 2003.

South Africa has also entered into bilateral agreements with other Southern African States such as Lesotho, Swaziland and Namibia regarding financial policy measures implemented in the

---

17 Snail kaMtuze S 'Cyber Crime in South Africa–Hacking, cracking, and other unlawful online activities' (2009) 1 *Journal of Information, Law and Technology* 5.

18 Watney (note 12 above) 66.

19 Luiijf E, Bestselling K & De Graaf P 'Nineteen national cyber security strategies' (2013) 9:1/2 *International Journal of Critical Infrastructures* 3-31.

Southern African region including the prevention of terrorism. Thus, South Africa is taking steps to address the spectre of terrorism.[20] On that note, it is worth highlighting that the Computer Security Incident Response Team (CSIRT) has been established to address CyberCrime, to avert CyberAttacks and to apprehend computer criminals.[21]

7.5. CyberTerrorism

7.5.1. Overview

The commonality of approach between South Africa's CyberSecurity posture and the German one is worth recognition, given that Germany is one of the few states that prioritise skills and competency match (POSTEDFIT). German's NCSS highlights the threat of mismatches between functional ICT developments and an appropriate level of CyberSecurity related to those developments. Interestingly, none of the other nations addresses this important global topic of threats due to ICT innovation.[22]

The global nature of computer technology presents a challenge to nations to address CyberCrime. Domestic solutions are in adequate because the CyberSpace has no geographic or political boundaries, and many computer systems can be easily accessed from anywhere in the world. It is difficult to obtain accurate CyberCrime statistics because an unknown number of crimes go undetected and unreported. It is also costly to develop and maintain security and other preventative measures. International financial organisations are also common targets for computer fraud and embezzlement schemes.

Although technological advancement is welcome, it has created numerous challenges. There is a need for security-related features on the internet to respond to these challenges. Countries

---

20 Cassim (note 14 above) 27.

21 Orji UJ *CyberSecurity Law and Regulation* (2012) Wolf Legal.

22 Luiijf *et al* (note 18 above) 3-31.

should strive to strike a balance between protecting the safety and security of individuals and guaranteeing the free dissemination of information and opinion. [23]

Attacks via the internet infrastructure are increasingly becoming a daily occurrence and South Africa is no exception. In response, certain governments have published strategies pertaining to Information Security at national level. These policies aim to ensure that critical infrastructure is protected, and that there is a move towards a greater state of Information Security readiness. This is also the case for South Africa, where a variety of policy initiatives have started to gain momentum. While it is essential to establish strategy and policy, ensuring its implementation is often difficult and dependent on the availability of resources. This is even more so, in the case of Information Security since virtually all standardised security improvement processes start-off with specifying that a proper inventory is required of all hardware, software, people and processes. While this may be possible to achieve at an organisational level, it is far more complex and challenging at the national level.[24]

Countries should encourage reconciliation and respect for diversity, bridge gulfs between different countries in the broader international community to counteract terrorist threats, hence the proposal for a Global Protocol on CyberSecurity and CyberCrime as mooted in a paper presented in 2009 by Schjølberg and Ghernaouti-Hélie, view that is concurred by Russia. Global CyberCrime Treaty will provide for a code of conduct that will identity the rights and responsibilities of all nation-states in respect of the information space, which will culminate in a more coordinated effort to make the internet safer, especially in respect of CyberAttacks and terrorist activities.[25]

All nation-states should agree that CyberCrime, CyberAttacks and terrorist activities might end the economic and social advantages that the CyberSpace holds for generations to come, hence the need for the multilateral transnational CyberCrime legislation that will provide platforms for:

---

23 Orji UJ 'Regionalising CyberSecurity governance in Africa: An assessment of responses' (2016) *Securing CyberSpace* 203.

24 Swart I, Irwin B & Grobler M 'Towards a platform to visualise the state of South Africa's Information Security' (2014) *Information Security for South Africa (ISSA)* 2014.

25 Watney (note 12 above) 66.

1. Ensuring that all states have CyberCrime laws in place on national and transnational levels;
2. Harmonisation of state's CyberCrime laws specifically pertaining to multi-jurisdictional crimes;
3. Conceptualisation of the legal position regarding certain forms of CyberCrime such as the launch of a CyberAttacks as well as provide mechanisms for monitoring and evaluation of enforcement mechanisms.[26]

South Africa, like Russia views the global treaty on CyberCrime as a non-negotiable and has thereby legislated for mutual assistance across jurisdictions to align with the transnational feature of the CyberSpace. Abdul Rauf presents the following recommendations, to facilitate the achievement of CyberSecurity objectives as these relate to national security, economic security and human security globally:

(a) Government services;
(b) Information Communication Technologies;
(c) Emergency and rescue services;
(d) Energy and health services; and
(e) Logistic services and water services.[27]59

These recommendations are gleaned from the draft proposal for an international Convention on CyberCrime and Terrorism entailing various economic sectors, which include but are not limited to the banking and finance sectors.

7.5.2. Ratification of international legal instruments and domestication

In dealing with the transnational feature of CyberSpace, the UN Convention on CyberSpace initiative remains a non-negotiable. Watney further assets that the call for a code of conduct will not necessarily bring about better 'laws', but will identity the rights and responsibilities of all nation-

[26] Watney (note 12 above) 66.

[27] Orji 2012 (note 122 above) 376.

states in respect of the information space and may result in a more coordinated effort to make the internet safer, especially in respect of CyberAttacks and terrorist activities.[28]

Countries should ensure that their CyberTerrorism legislation is compatible with international human rights instruments. While the protection of CyberSystems is a major concern, this security should not prejudice the fundamental rights and freedoms enshrined in our Constitution and human rights instruments.[29] Countries should educate the public about the threat of CyberTerrorism, as vigilance is a key factor in addressing the potential threat of CyberTerrorism. Users of the internet should also be encouraged to adopt stronger security measures. Watney further argues that the geopolitical considerations that have positioned South Africa within the BRICS have rendered the possibility of ratification of the COECC less probable. Participation within the BRICS, E-commerce Cooperation Agreements together with the UN Convention on CyberSpace provides better political and economic opportunities for South Africa.

7.5.3. Empowerment and skills development programs to improve citizen's Cyber Astuteness

Internet users should also be encouraged to share the burden of securing informational privacy where feasible. Computer ethics education should be taught in schools to educate children about the negative consequences of committing CyberCrimes. Cyber Astuteness needs to be improved by introducing specialised law enforcement and training skills and improving computer forensic capabilities, initiating skills development, and empowerment programmers within government, with the help of the private sector and international enterprises.[30]

Cyber Intelligence should be underpinned by coordinated governments that are informed by partnerships with other countries to provide technical and material support and also increase cooperation among the intelligence agencies of different countries to facilitate the exchange of sensitive information to counter CyberTerrorist threats. International cooperation is important to

---

28 Watney (note 12 above) 67.

29 Abdulrauf LA & Fombad CM 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8:1 *Journal of Media Law.*

30 Cassim F 'Protecting personal Information in the era of identity theft: just how safe is our personal Information from identity thieves?' (2015) 8:2 *PER: Potchefstroomse Elektroniese Regsblad* 69-110.

ensure the integrity of the internet and security of networks.[31] Countries should explore the feasibility of introducing internet-filtering measures to control access to websites that pose serious threats to their national security. [32]

The role of the media is critical in the fight against CyberTerrorism. The media should follow a concise and sensible approach rather than exploit the fears of the ordinary public[33] and existing initiatives in South Africa. Okuku *et al* argue that within the South African context, various inter-governmental collaboration and initiatives have advanced the need for the inclusion of CyberSecurity awareness as part of the education curriculum. A notable initiative in this regard is the Reid and Van Niekerk's annual education campaigns, initiated in 2011, which focuses on imparting educational astuteness to South African youths about Cyber issues. These campaigns, encapsulate various topics, including e-transacting activities, CyberCrime, social networking, password and hardware security, malware, CyberBullying, CyberIdentity management among others. A voluntary handcrafted or digitally created poster contest was proposed, aimed at measuring the campaign's impact on the level of awareness on the security issues covered for the youths involved.

The campaigns have reportedly improved youth participation, CyberSecurity awareness and the inclusion of teachers who positively contributed to the study. An interdisciplinary approach is recommended where CyberSecurity experts determine what users are taught while other experts such as teachers construct the message to be taught.[34]

7.5.4. Cultivating a CyberSecurity culture

Central to the creation of a Cyber Astute citizen protected by CyberWarrior with hacking back skills and competencies, is a South African CyberSecurity policy framework founded on (i) political

---

31 Cassim (note 14 above) 1.

32 Cassim (note 14 above).

33 Orji UJ 'Deterring CyberTerrorism in the global Information Society: A case for the collective responsibility of states' (2014) 6:1 *Defence against Terrorism Review* 31-46.

34 Okuku A, Renaud K & Valeriano B 'CyberSecurity strategy's role in raising Kenyan awareness of mobile security threats' (2015) 32:2 *Information & Security* 1.

will, (ii) adapted organisational structures, (iii) identifying accurate proactive and reactive measures, (iv) reducing criminal opportunities and (iv) education and awareness. It is argued in concurrence with Grobler *et al* that these foundational elements are central to developing and implementing a national strategy for an effective CyberSecurity approach and culture.[35]

The utilisation of an outcome-based approach to the agenda of keeping the CyberSecurity culture remains central to comprehensive results based approach. These results-based approaches must be premise on a foresight stakeholder and responsibility matrix that enables the full appreciation of the following:

1. People/entities/organs of state that have a role to play in cultivating the culture;
2. Role definition and functions of each that need to take place;
3. Functional resource appreciation
4. The proposed and costed stakeholder based means and ways to enable cultivating the culture; and
5. The influences associated with the group in which the envisaged culture will be promoted, i.e. the level of connectivity, age and digital literacy.
6. Strategic and operational risks that are inherent in each of the above and proposed risk treatment.[36]

7.5.5. Strengthening collaborations across States

Watney argues, strongly that the CyberSpace ultimately belongs to the global world. Despite the difference, and in some instances opposing views rooted in the protection of territorial integrity and sovereignty, as depicted by Russia's refusal to sign the CyberCrime Convention and its rejection of a draft Declaration on Fundamental Freedoms in the Digital Age sponsored by the US

---

35 Grobler M, Van Vuuren GM & Leenen JJI 'Implementation of a CyberSecurity policy in South Africa: Reflection on progress and the way forward' (2012a) *IFIP International Conference on Human Choice and Computers Springer* 215-225.

36 Gcaza N *et al* 'A general morphological analysis: Delineating a cyber-security culture' (2017) 25:2 *Info and Computer Security* 259-278.

Secretary of State at the Organisation of Security and Co-operation in Europe Summit (OSCE) in 2011.[37]

Interpretation of a Cyber-attack is context-based, as it can be between governments and their military. Governments and the militaries are not the only targets of CyberAttacks; CyberWarfare have equally reached public, corporate and private networks. Former UN Secretary General, Ban Ki Moon confirmed in 2013, the potential of CyberAttacks in causing global destabilisation and hence the need to profile CyberSecurity as a matter of global concern.[38]

For this reason, the CyberWarrior does not only present the soldier fighting against CyberAttacks, but also a Cyber Empowered citizen, whose personal information and interactions with cloud computing must guarantee less exposure to vulnerabilities.[39] Unlike airspace, CyberSpace does not have borders and therefore, the origin of threats, the identity of the threat actors and where the battle takes place often remains unknown. The multiplicity of methods to launch a CyberAttacks renders it difficult to attribute an attack to a State or non-state actor where direct combat does not exist in the CyberSpace.[40]

7.6 Boundary Management and Accountability

The draft Bill on CyberCrime and CyberSecurity places specific regulatory responsibilities on each of the governance structures. For these structures to operate optimally, boundary management requires sharper attention. The interoperability of systems is a necessity for instant responses. Further, high level of accountability is critical across each Member State within the Computer Security Incident Response Team (CSIRT), which is establish to address CyberCrime, avert CyberAttacks and apprehends computer criminals.

Countries should keep pace with evolving technology to counteract potential CyberTerrorist threats and these should be continually developed and enhanced in the global fight against

---

37 Watney (n 12 above) 66.

38 Thibodeaux, A ‘Hacking back: Surviving in the digital age' (2015) dissertation Utica College.

39 Thibodeaux (note 37 above) 3.

40 Thibodeaux (note 37 above) 4.

terrorism. Such an approach will facilitate a mind shift from a posture of CyberSpace that is unavoidable, yet unreliable to a CyberSpace that has the potential to be the most fully and extensively regulated space that we have ever known anywhere, at any time in our history.[41]

7.7 Accelerated prioritisation of CyberCrime Legislative Frameworks within SADC

Article III 1-1 of the 'Draft African Union Convention on the Establishment of a Credible Legal Framework for CyberSecurity in Africa' enjoins member States to adopt legislative measures deemed effective to set up material criminal offences as acts, which affect the confidentiality, integrity, availability and survivability of ICT systems and related infrastructure networks; as well as effective procedural measures for the arrest and prosecution of offenders. Members are required in Article III 1-19 to ensure that the legislative measures adopted in respect of material and procedural provisions on CyberSecurity reflect international best practices and integrate the minimum standards contained in extant legislation in the region at large so as to enhance the possibility of regional harmonisation of the said legal measures.[42] Inherent in the aforementioned provisions is the non-negotiable requirement for States to develop laws against CyberCrime as well as ensure harmonisation at regional and continental level.

South Africa is a member of SADC as well as a member of AU. The transnational feature of CyberCrime demands an aggressive multilateral approach to CyberCrime and CyberSecurity issues. The environmental scan as depicted by Orji presents a scenario wherein, as of January 2016, six SADC members, including Angola, the Democratic Republic of Congo, Lesotho, Malawi, Mozambique and Swaziland did not have CyberCrime laws[43]. The efficacy of the South African CyberCrime and CyberSecurity Bill in ensuring that citizens claim a safe and secure CyberSpace is collaterally dependent on other member States' commitment in accelerating the finalisation of their respective domestic legislative frameworks.

---

41 Lessig L 'The laws of CyberSpace' (1998) *Readings in CyberEthics* 134, 136.

42 African Union 'Draft African Union Convention on the Establishment of a Credible legal Framework for CyberSecurity in Africa' available at: https://au.int/en/cyberlegislation (accessed: 16 November 2017).

43 Orji UJ 'Regionalising CyberSecurity governance in Africa: An assessment of responses' (2016) *Securing CyberSpace* 207.

Nation States have documented their Cyber Strategies and executed them in the form of Cyber Commands. The military dimension has experienced CyberSpace witnessing the beginnings of a race for the development and deployment of Cyber Weapons. An arms control regime, the Wassenaar Arrangement has enlarged its controls list in consonance by way of CyberSpace has altered the present-day security landscape. The development of Cyber Weapons and their potential usage against high-value targets has been one of the major security concerns for nation States. This trajectory should equally inform the aggressive implementation of the South African Defence Review, beyond the phase of arresting the decline to developing Cyber Capabilities that will guarantee the protection of land, maritime, airspace as well CyberSpace.

The sharper focus on the ocean economy as a strategic lever, demands that a Regional Protocol on CyberCrime within the Maritime Space receives urgent attention. It is imperative that the CyberCrime and CyberSecurity legislative frameworks reflect this geostrategic foresight. Unfortunately, CyberCrime defies the conventional three layers approach to Defence.

The Commitments reflected in the July 2015 BRICS Declaration at the Ufa Summit regarding the development of accelerative development of measures to prevent conflict in CyberSpace and further develop norms, standards and principles of responsible conduct remain central and urgent to realise accountable Global CyberSapce Governance.[44] .

[44] Kulikova A Working out the rules of Global CyberSpace Governance. *Securing CyberSpace* (2016) 81.Ufa Declaration (Article 34) BRICS, Documents available at: http://en.brics2015.ru/documents/ (accessed: 16 November 2017).

BIBLIOGRAPHY

Primary sources

Case law – Germany

D

Die 'Lufthansa-Blockade' 2001 – eine (strafbare) Online-Demonstration AG Frankfurt a.M, Urt. v. 1.7.2005 – 991 Ds 6100 Js 226314/01 = MMR 2005, 863 (864) Decision by the Frankfurt Appellate Court (in German only, 2.05.2006) English (2.06.2006).

S

Scarlet Extended SA v Société Belge des Auteurs, Compositeurs et Editeurs SCRL (SABAM) ECLI: EU: C: 2011:771: Case C70/10.

Case law – South Africa

N

Ndlovu v Minister of Correctional Services and another 2006 All SA 165 (W).

Ndiki 2008 (2) SACR 252 (Ck) 261d-h.

Narlis v. South African Bank of Athens 1976 (2) SA 573 (A).

S

S v Van den Berg 1991 (1) SACR 104 (T).

S v Tandwa and Others 2008 (1) SACR 613 (SCA),

T

Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others [2008] ZACC 13; 2009 (1) SA 1 (CC)

Foreign Case law

International Legal Instruments

A

African Union Convention on Cyber Security and Personal Data Protection ECOWAS Directive on fighting CyberCrime, 2011.

C

Council of Europe Convention on CyberCrime (CoECC, 2001).

COMESA Model Law on Computer Crime and CyberCrime, 2011.

Draft International Convention on CyberCrime and Terrorism.

D

Draft African Union Convention on the Establishment of a Credible Legal Framework for CyberSecurity in Africa 2014.

Draft EAC Legal framework for CyberLaws (2008).

European Union (EU) Directive

E

2000/31/EC of the European Parliament and of the Council of 8 June 2000 ('Directive on electronic commerce').

2001/29/EC of the European Parliament and of the Council of 22 May 2001.

2004/48/EC of the European Parliament and of the Council of 29 April 2004.

95/46/EC of the European Parliament and of the Council of 24 October 1995.

2002/58/EC of the European Parliament and of the Council of 12 July 2002 (Directive on privacy and electronic communications).

F

Framework for CyberLaws, Phase II (UNCTAD, 2011).

G

Global Protocol on Cyber-security and Cyber-crime.

I

International Telecommunication Union (ITU).

NATO Convention

N

NATO Cyber Defence Pledge, 08-Jul.-2016

S

SADC Model Law on Computer Crime and CyberCrime, 2012.

T

Talim Framework- NATO Cooperative Cyber Defence Centre of Excellence 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' (2013) *Cambridge University Press* available at: https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual (accessed: 3 August 2017).

U

United Nations Framework Convention on Climate Change – the Kyoto Protocol, Kyoto.

Legislation – South Africa

C

Constitution of the Republic of South Africa Act 103 of 1996.

Computer Evidence Act 57 of 1983.

Copyright Act 98 of 1978.

Critical Infrastructure Bill 2017 Government Gazette No 41114 of 15 September 2017

CyberCrime and CyberSecurity Bill of 2017.

E

Electronic Communications and Transactions Act 25 of 2002 (ECT).

Electronic Communications Act 36 of 2005.

F

Films and Publications Act 65 of 1996.

Financial Intelligence Centre Act 38 of 2001 (FICA) as amended.

N

National Prosecutions Act 32 of 1998.

M

Monitoring and Prohibition Act 127 of 1992.

P

Prevention of Organised Crime Act 38 of 1999 (POCA).

Promotion of Access to Information Act 25 of 2002(PAIA).

Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004 (PCDTRA).

Protection of Personal Information Act 4 of 2013(POPIA).

R

Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002 (RICA).

Legislation - Germany

German Criminal Code: Translation of the German Criminal Code 1876 provided by Prof. DrMichael Bohlander and accessed from https://www.gesetze-im internet.de/englisch_stgb/englisch_stgb.html on 14 Sept 2017.

Legislation - Russia

The Criminal Code of the Russian Federation No. 63-Fz Of June 13, 1996(amended 2012) accessed from http://legislationline.org/documents/Section/criminal-codes/country/ English version (accessed: 14 September 2017).

Policies

D

Department of Defence 'South African Defence Review 2015' available at: http://www.dod.mil.za/documents/defencereview/defence%20review%202015.pdf (accessed: 04 November 2017).

N

National Development Plan Vision 2030.

National CyberSecurity Policy Framework for South Africa in the South African Government Gazette No 39475 of 4 December 2015.

National Broadband Policy 2013: South Africa Connect: Creating opportunities, ensuring inclusion.

M

Medium Term Strategic Framework: A framework to guide Government's Programme in the Electoral Mandate Period (2009-2014)

Secondary Sources

Books

J

Janczewski, L (ed) Cyber Warfare and CyberTerrorism (2007) IGI Global.

L

Lewis, JA *Assessing the Risks of CyberTerrorism, CyberWar and other CyberThreats* (2002) Center for Strategic & International Studies: Washington DC.

M

Majid, Y *CyberCrime and Society* (2013) Sage: London.

O

Orji, UJ *CyberSecurity Law & Regulation* (2012) (Wolf Legal Publishers: Netherlands).

P

Papadopoulos, S & Snail, SL Cyberlaw @ *SA III: The law of the internet in South Africa* (2012) Van Schaik: Pretoria.

S

Samuel, C & Sharma, M *Securing CyberSpace: International and Asian Perspectives* (2016) Institute for Defence Studies and Analyses (Pentagon Press: New Delhi).

Schjølberg, S *Wanted: A United Nations CyberSpace Treaty' Global CyberDeterrence: Views from China, the US, Russia, India, and Norway* (2010) East West Institute New York.

Schwikkard, P-J & Van der Merwe, SE *Principles of Evidence* (Juta: 2009).

Sofaer AD, Goodman SE, Cullar M, *et al A Proposal for an International Convention on Cyber Crime and Terrorism* (2010) Stanford University, Centre for International Security and Cooperation: Stanford University.

Tushabe, F *et al The Launch of the African Centre for CyberLaw and CyberCrime Prevention (ACCP)* (2010) UNIAFRI Secretariat, Kampala.

V

Van der Merwe, D, and Roos A, Pistorius T, Nel S and Eiselen S *information and communications technology law* (2008) *LexisNexus*.

Journal Articles

A

Abdulrauf, LA & Fombad, CM 'Addressing the spectre of cyber terrorism: A comparative perspective' (2012a) 15:2 *Potchefstroom Electronic Law Journal* 380-415.

Abdulrauf, LA & Fombad, CM 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8:1 *Journal of Media Law* 67 -97.

Abraham, D Sofaer & Seymour, E. Goodman. 'CyberCrime and security: The transnational dimension' (2001) *The Transnational Dimension of Cyber-Crime and Terrorism* 1-34.

C

Cassim, F 'Formulating specialised legislation to address the growing spectre of CyberCrime: A Comparative Study' (2009) 12:4 *Potchefstroomse Elektroniese Regsblad* 36-79.

Cassim, F 'Addressing the spectre of Cyber Terrorism: A comparative perspective' (2012b) 15:2 *Potchefstroomse Elektroniese Regsblad* 380-415.

Cassim, F 'Formulating specialised legislation to address the growing spectre of CyberCrime: A comparative study' (2009) 12:4 *Potchefstroomse Elektroniese Regsblad* 36 -79.

Cassim, F 'Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?' (2015) 18:2 *Potchefstroomse Elektroniese Regsblad* 69 -110.

Cassim, F 'Addressing the Growing Spectre of CyberCrime in Africa' (2011) 44:1 *Comparative and International Law Journal of Southern Africa* 123 -38.

Cohen, Aviv. 'CyberTerrorism: Are We Legally Ready' (2010) 9 *Journal of International Business & Law* 1-41.

Cole, K *et al* 'CyberSecurity in Africa: An assessment' (2008) *Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology* 1-33**.**

D

Delaney, DG 'CyberSecurity and the administrative national security state: Framing the issues for federal legislation' (2013) 40 *Journal of Legislation* 251-279.

Dimitrakopoulou, Sophia, and Andrew Liaropoulos. "Russia's National Security Strategy to 2020:A Great Power in the Making?." Caucasian Review of International Affairs 4.1 (2010): 35-41.

G

Gcaza, N; Rossouw, VS; Grobler, MM and Joey Jansen, VV 'A general morphological analysis: Delineating a CyberSecurity culture' (2017)25:3 *Info and Computer Security* 259-278.

Gorr, D & Schünemann, WJ 'Creating a secure CyberSpace–Securitization in internet governance discourses and dispositives in Germany and Russia' (2013) 20:12 *International Review of Information Ethics* 37-51.

Grobler, M; Van Vuuren, JJ & Leenen, L 'Implementation of a CyberSecurity policy in South Africa: Reflection on progress and the way forward' (2012) *IFIP International Conference on Human Choice and Computers Springer* 215-225.

Grobler, M *et al* 'Preparing South Africa for CyberCrime and cyber defence' International Institute of Informatics and Cybernetics' (2013) 11:7 *Journal of Systemics, Cybernetics Informatics* 32-41.

Guitton, C 'Cyber insecurity as a national threat: Overreaction from Germany, France and the UK?' (2013) 22:1 *European Security* 21-5.

H

Hoisington, M 'CyberWarfare and the use of force giving rise to the right of self-defence' (2009) 32 *BC Int'l & Comp. L. Rev.* 439.

K

Kabano, Y 'Information (Cyber-) Security discourses and policies in the European Union and Russia: A comparative analysis' (2013) *Foresight* 7-9.

L

Lessig, L 'The laws of CyberSpace' (1998) *Readings in CyberEthics* 134-136.

Luiijf, E Bestselling, K & De Graaf, P 'Nineteen national CyberSecurity strategies' (2013) 9:1/2 *International Journal of Critical Infrastructures* 3-31.

M

Makulilo AB 'Data protection regimes in Africa: Too far from the European 'adequacy' standard?' (2013) 3:1 *International Data Privacy Law* 42–50**.**

Makulilo, Alex B. "Myth and reality of harmonisation of data privacy policies in Africa." *Computer Law & Security Review* 31.1 (2015): 78-89.

O

Okuku, A Renaud, K & Valeriano, B 'CyberSecurity strategy's role in raising Kenyan awareness of mobile security threats' (2015) 32:2 *Information& Security* 1.

O'Reilly, K 'South African Law coming to grips with CyberCrime: News' (2013) 530 *de Rebus* 14-15.

Orji, UJ 'Deterring CyberTerrorism in the global Information Society: A case for the collective responsibility of states' (2014) 6:1 *Defence against Terrorism Review* 31-46.

Orji, UJ 'Multilateral legal responses to CyberSecurity in Africa: Any hope for effective international cooperation?" CyberConflict: Architectures in CyberSpace (CyCon) (2015) *7th International Conference on IEEE*.

Orji, UJ 'Regionalising CyberSecurity governance in Africa: An assessment of responses' (2016) *Securing CyberSpace* 203-218.

Orji, UJ 'Multilateral legal responses to CyberSecurity in Africa: Any hope for effective international co-operation?' (2015) *African Centre for Cyber Law and CyberCrime Prevention (ACCP)*) 105-118.

P

Papathanassiou, A *et al* 'Legal and social aspects of CyberCrime in Greece' (2013) *International Conference on e-Democracy Springer, Cham* 5.

Parks, RC & Duggan, DP 'Principles of CyberWarfare' (2011) 9:5 *IEEE Security and Privacy* 30-5.

Pistorius, Monitoring, interception and Big Boss in the workplace: is the devil in the details?' (2009) 12:1 *PER: Potchefstroomse Elektroniese Regsblad* 1-26.

R

Russel Luck RICA: walking a fine line between crime prevention and protection of rights."
De Rebus, Jan/Feb 2014:30 [2014] DEREBUS 6

S

Schjølberg, S & Ghernaouti-Hélie, S 'A global treaty on CyberSecurity and CyberCrime' (2011) 97 *CyberCrime Law* 1-67.

Schmitt, MN 'Rewired Warfare: Rethinking the law of cyber-attack' (2014) 96:893 *International Review of the Red Cross* 189-206.

Shackelford, SJ Scott, R & Kuehn, A 'Unpacking the international law on CyberSecurity due diligence: Lessons from the public and private sectors' (2016) *Chicago Journal of International Law 1-51.*

Shannon, CS 'Global internet regulation: The residual effects of the ILoveYou computer virus and the Draft Convention on Cyber-Crime' (2001) 25 *Suffolk Transnational Law Review* 491.

Snail kaMtuze, S L 'CyberCrime in the Context of the ECT Act' (2008) 162 *Juta's Business Law* 63-69

Snail kaMtuze, SL & Matanzima, S 'CyberSecurity in Africa: CyberLaw' (2014) 14:9 *Without Prejudice* 88-89

Snail, SL 'CyberCrime in South Africa–Hacking, cracking, and other unlawful online activities' (2009) 1 *Journal of Information, Law and Technology* 1-13.

Snail, SL & Madziwa, S 'Hacking, cracking and other unlawful online activities: Communications law' (2008) 8:2 *Without Prejudice* 30-31.

Sprinkel, SC 'Global internet regulation: The residual effects of the ILoveYou computer virus and the Draft Convention on Cyber-Crime' (2001) 25 *Suffolk Transnational Law Review* 491.

Swart, I; Irwin, B & Grobler, M 'Towards a platform to visualize the state of South Africa's Information Security' (2014) *Information Security for South Africa IEEE* 1-8.

T

Tara Davenport, Submarine Cables, CyberSecurity and International Law: An InterSectional Analysis' (201) 24 *Catholic University Journal of Law & Technology* 89-104.

Tikk, E 'Global CyberSecurity: Thinking about the niche for NATO' (2010) 30:2 *SAIS Review of International Affairs* 105-119.

V

Van Epps, G 'Common ground: US and NATO engagement with Russia in the Cyber Domain' (2013) 12:4 *Connections: The Quarterly Journal* 16-19.

Von Solms, Rossouw, & Van Niekerk J 'From Information Security to cyber security' (2013) 38 *Computers & Security* 97-102.

W

Watney, M 'Admissibility of electronic evidence in criminal proceedings: an outline of the South African legal position' (2009) 1 *Journal of Information, Law and Technology* 1-10.

Watney, MM 'The way forward in addressing CyberCrime regulation on a global level' (2012) 1:1/2 *Journal of Internet Technology and Secured Tran*sactions 61-67.

Weber, AM 'The Council of Europe's Convention on CyberCrime' (2003) 18:1 *Berkeley Technology Law Journal* 425-446.

Y

Yar, M 'The Novelty of "CyberCrime": An assessment in light of Routine Activity Theory' (2005) 2:4 *European Journal of Criminology* 407-427.

Dissertations

A

Ashmore, WC 'Impact of alleged Russian Cyber attacks' Army Command and General Staff College, Fort Leavenworth KS, School of Advanced Military Studies 2009.

S

Snail kaMtuze, Sizwe. A comparative review of legislative reform of electronic contract formation in South Africa. Diss 2015.

Schultz, C.B, CyberCrime: An analysis of the current legislation in South Africa, Diss 2017.

T

Thibodeaux, A 'Hacking back: Surviving in the digital age' dissertation Utica College 2015.

V

Van Tonder G.P. The admissibility and evidential weight of electronic evidence in South African legal proceedings: a comparative perspective,2013.

Conference, Convention and Workshop Papers

G

Grobler, M Jansen van Vuuren, J & Leenen, L 'Implementation of a CyberSecurity policy in South Africa: Reflection on progress and the way forward' (2012) Paper presented at the IFIP International Conference on Human Choice and Computers Springer Berlin Heidelberg 215-225**.**

I

Information Regulator South Africa Submission to Public Hearings on the CyberCrime and CyberSecurity Bill of 2017.

K

Kulikova, A. Working out the rules of Global CyberSpace Governance: Securing CyberSpace' (2016) 81-94.

L

Luiijf, HAM *et al* 'Ten national CyberSecurity strategies: A comparison' (2011) International Workshop on Critical Information Infrastructures Security Springer, Berlin, Heidelberg 3-31.

M

Ministry of Foreign Affairs of the Russian Federation: Information Security Doctrine of the Russian Federation.

Muyowa, M Mtsweni J & Mkhonto, N 'Developing a CyberThreat Intelligence Sharing Platform for South African Organisations' (2017) Paper presented at Information Communication Technology and Society (ICTAS), Conference on IEEE.

O

Orji, UJ 'CyberTerrorism and the collective responsibility of States to Secure the Global Information Society' (2012b) Paper presented at CyberSecurity Summit (WCS) Third Worldwide IEEE 1 - 10.

Orji, UJ Regionalising CyberSecurity Governance in Africa: An Assessment of Responses Securing CyberSpace 203.

R

Rivera, J 'Achieving Cyber Deterrence and the Ability of Small States to Hold Large States at Risk' (2015) Paper presented at 7th International Conference on Cyber Conflict: Architectures in CyberSpace (CyCon) IEEE7-24.

S

Sofaer A, Clark D & Diffie W. CyberSecurity and international agreements' (2009) National Research Council Proceedings of a Workshop on Deterring Cyberattacks.

W

Wirtz, JJ 'CyberWar and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy' K. Geers, Cyber War in Perspective: Russian Aggression against Ukraine, c 3 (2015): 29-37.

Internet Sources

Critical Infrastructure Bill 2017 Government Gazette No 41114 of 15 September 2017 Available on https://www.parliament.gov.za/. (accessed on October 2017).

Department of Defence 'South African Defence Review 2015' available at: http://www.dod.mil.za/documents/defencereview/defence%20review%202015.pdf (accessed: 3 August 2017).

Draft EAC Legal framework for Cyberlaws (2008) available at: <www.eac.int/index.php?option=com_docman&task=doc_view&gid=632&Itemid=148> (accessed on 23 October 2017).

Framework for Cyberlaws, Phase II (UNCTAD, 2011) available at: <http://r0.unctad.org/ecommerce/docs/EAC_Framework_PhaseII.pd accessed on 23 October 2017.

Gous N 'Private Information of about 31.6m South Africans breached and still online' Herald Live available at: http://www.heraldlive.co.za/news/2017/10/18/private-Information-31-6m-south-africans- (accessed: 18 October 2017).

Kelly, S, Cook, S & Truong, M 'Freedom on the Net 2011. A global assessment of internet and the digital media' (2011) *Freedom House* Available at: http://www. Freedom house. Org/uploads/font/2011/FOTN2011. Pdf, updated on 14.04 (2011): 2011 accessed on 23 October 2017.

Ministry of Foreign Affairs of the Russian Federation: Information Security Doctrine of the Russian Federation available at :) http://scholarship.law.edu/jlt/vol24/iss1/4 (accessed: 9 Sept 2017).

NATO Cooperative Cyber Defence Centre of Excellence 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' (2013) *Cambridge University Press* available at: http://www.nato.int/cps/en/natohq/topics_78170.htm (accessed: 3 August 2017).

NATO Review 'Spending for success on Cyber Defence' available at: http://www.nato.int/docu/review/2017/Also-in-2017/nato-priority-spending-success-cyber-defence/EN/index.htm (accessed: 3 August 2017).

NATO Cooperative Cyber Defence Centre of Excellence 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' (2013) *Cambridge University Press* available at: https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf (accessed: 3 August 2017).

Schjølberg, S & Ghernaouti-Hélie, S 'A global protocol on CyberSecurity and CyberCrime' (2009) CyberCrimelaw.net.

Summary of CyberCrimes and CyberSecurity Bill 2017 available at: https://www.ellipsis.co.za/.../Summary-of-CyberCrimes-and-CyberSecurity-Bill-2017. (Accessed: 4 August 2017).

Republic of South Africa *CyberCrime and CyberSecurity Bill* [B 6-2017] published in Government Gazette No 40487 of 9 December 2016 available at: http://www.justice.gov.za/m_speeches/2017/20170119CyberCrimeBillBriefing.html (accessed: 4 August 2017).

Watson, F & Williams, 'Briefing: The New German IT Security Act' February 2016, http://www.wfw.com/wp-content/\uploads/2016/02/WFW-Briefing-Germany-IT-Security-Feb-2016-EN-15-Feb.pd accessed on 23 October 2017.

2017 Midyear CyberSecurity Risk Review: Forecast and Remediation Executive Summary available at: www.accenture.com/za-en/insight-cyber-threat-scape-report-2017 (accessed: 23 October 2017).

2 Chronicles 20:20 (KJV)

‘And they rose early *in* the morning, and went forth into the wilderness of Tekoa: and as they went forth, Jehoshaphat stood and said, Hear me, O Judah, and ye inhabitants of Jerusalem; *Believe in* the Lord your *God*, so shall ye be established; *believe* his prophets, so shall ye prosper.’