THE CHALLENGE OF LEGISLATING MORAL AND CIVIL WRONGS IN THE CYBERSPACE: A THEORY FOR INTERNET REGULATORY POLICY

Submitted in partial fulfillment of the requirements of the Bachelor of Laws Degree, Strathmore University Law School

By

Lynda Kinya Kaimenyi

078157

Prepared under the supervision of

Mr. Humphrey Sipalla

January 2017

Table of Contents

Acknowledgments

My sincerest gratitude goes to Mr. Humphrey Sipalla for his guidance throughout this work, Professor Nii Quaynor whose insight was invaluable in the writing of this paper.

Declaration

I, LYNDA KINYA KAIMENYI, do hereby declare that this research is my original work and that to the best of my knowledge and belief, it has not been previously, in its entirety or in part, been submitted to any other university for a degree or diploma. Other works cited or referred to are accordingly acknowledged.

Signed: ....

Date: ....

This dissertation has been submitted for examination with my approval as University Supervisor.

Signed: ....

Mr. Humphrey Sipalla

Abstract

The internet's meteoric rise has provided vast areas of new opportunity and potential sources of efficiency for organizations of all sizes. It has however, also transformed the behaviour of the criminal element within that society. These new opportunities come saddled with unprecedented threats. Ranging from attacks on the system; unauthorised access, denial of service, malware to data breaches; that affect the integrity and confidentiality of data as well as child pornography, hate speech, cyber bullying, theft, fraud etc.

This paper's objective is to come up with a theory for internet regulatory policy. By taking into consideration the unique challenges posed to legislation, the different models of laws and incorporating the merits of various philosophies. This theory is aimed at guiding the creation of effective cyber legislation and guiding any new developments as it is clear that innovations in the cyberspace will always outpace the law-making process. Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. If neither of these is achieved then the entire undertaking becomes worthless.

List of Abbreviations

ACORN – Australian Cybercrime Online Reporting Network

CAS - Complex Adaptive Systems

COE- Council of Europe

CECC – Council of Europe Convention on Cyber Crime

CERT - Computer Emergency Readiness Teams

CRC - Convention on the Rights of the Child

FISA- Foreign Intelligence Surveillance Act

GII - Global Information Infrastructure

ICANN – Internet Corporation of Assigned Names and Numbers

ICCPR – International Covenant on Civil and Political Rights

ICESR - International Covenant on Economic, Social and Cultural Rights

IEP – Internet Encyclopedia of Philosophy

IETF - Internet Engineering Taskforce

IGF – Internet Governance Forum

IRTF – Internet Research Task Force

IT - Information Technology

OWASP – Open Web Application Security Project

UDHR – Universal Declaration on Human Rights

List of Statutes and Instruments

African Union Convention on Cyber security and Data Protection

Constitution of Kenya 2010

Convention of Cybercrime ETS No. 185

Convention on the Rights and Duties of the State

Convention on the Rights of the Child

Electronic Communications and Transactions Act of South Africa

Foreign Intelligence Surveillance Act

International Covenant on Civil and Political Rights

International Covenant on Economic, Social and Cultural Rights

Kenya Cyber Security and Protection Bill

Universal Declaration on Human Rights

List of Cases

American Banana Company v United Fruit Company (1909) 213US 347-357.

Authors Guild v Google U.S. Court of Appeals for the Second Circuit, 2015.

S v Ndiki, 2008 2 SACR 252.

S v Mayisi

United States v Morrison, Court of appeal, Judgement on 7 March 1991, 1

CHAPTER ONE
Introduction

The Internet has revolutionised the computer and communications world like nothing before. Invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location. It represents one of the most successful examples of the benefits of sustained investment and commitment to research and development of information infrastructure.[1]

A non-physical complex environment resulting from the interaction of people, software and services over the internet by the means of technology devices and networks hereon referred to as the cyberspace has been created.[2] The cyberspace is the subject of this paper as it is where all interactions both the legitimate and illegitimate takes place.

The internet's meteoric rise has provided vast areas of new opportunity and potential sources of efficiency for organisations of all sizes. It has however, also transformed the behaviour of the criminal element within that society. The Internet's new opportunities come saddled with unprecedented threats. Ranging from attacks on the system; unauthorised access, denial of service, malware to data breaches; that affect the integrity and confidentiality of data as well as child pornography, hate speech, cyber bullying, theft, fraud etc.[3]

The features of the cyberspace that pose a challenge to governance stem from the disintegration of traditional sovereignty paradigms and emergence of network sovereignty.[4] Legal rules are

[1] Internet Society, 'Brief history of the internet' http://www.internetsociety.org/internet/what-internet/historyhttp://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internetinternet/brief-history-internet on 20 January 2017.

[2] Serianu, *Rethinking cyber security- An integrated approach: Process, Intelligence and Monitoring,* (2014), Kenya Cyber Security Report, 9

[3] Australian Cybercrime Online Reporting Network, ACORN ' Attacks on Computer Systems' https://www.acorn.gov.au/learn-about-cybercrime/attacks-computer-systems 20 January 2017.

[4] Reidenberg J, 'Governing networks and rule-making in cyberspace', 913, 917.

generally made to govern distinct subject areas for defined territories.[5] These substantive areas and territorial sovereignty are what which justify the regulatory authority and policymaking for states. Criminal law, administrative law belong to the realm of public law, intellectual property rights protect certain aspects of information and its economic value. These laws are enforced by the relevant regulatory agencies in corresponding territories. The cyberspace is designed so that persons from different geographical locations are able to interact under one roof, without the physical inhibitions of space and time these interactions range from contract, social media, publishing content, ecommerce etc.[6] Such interactions touch and sometimes blur various substantive areas of the law.

Cyberspace is driven by the actions of the individual members of human society; it is a powerful medium for social change precisely because it empowers individuals, which is why it is used so much.[7] The exponential rate of evolution in the cyber domain outpaces the speed of legal and judicial processes. This can be compared with whack- a –mole[8] whereby each new defense strategy leads to co-adaptation by a corresponding set of attacks.

States have faced these threats since the advent of the internet as evidenced by the Morris worm in 1988.[9] The first attempt to formulate regulations specific to computer crimes began at the international level with the Convention on Cybercrime by the Council of Europe.[10] It seeks to address internet and computer crime by harmonising national laws, improving investigative

[5] *American Banana Company v United Fruit Company* (1909) 213US page 347and 357. (Holding that as a general rule of construction, any statute is presumed to be intended to operate within the territorial limits of the sovereign).

[6] Johnson D, Post D, 'Law and borders, the rise of law in Cyberspace', 1.

[7] Ghanea-Hercock R, 'Why cyber security is hard' *Georgetown Journal of International Affairs* (2012),

[8] Whack- a- mole is an arcade game in which players use a mallet to hit toy moles, which appear at random, back into their holes.

[9] Radware, 'Morris Worm' https://security.radware.com/ddos-knowledge-center/ddospedia/morris-worm/ on 20 January 2017. The Morris Worm was a self-replicating computer program (worm) written by Robert Tappan Morris, a student at Cornell University, and released from MIT on November 2, 1988. It was was a self-replicating computer program causing computers to run out of resources and malfunction.

[10] Weber A, 'The Council of Europe's Convention on Cybercrime' 18 *Berkeley Technology Law Journal* 1 (2003), 428- 430.

techniques, and increasing cooperation among nations.[11] Subsequent legislations have been modelled along the Budapest Convention while some others have marked a departure from it. The AU Convention on Cyber security and Data Protection has been criticized particularly because it does not explicitly establish a model legal framework which African countries can adopt. The Convention merely creates guidelines for African states in the establishment their cyber security laws. The language of the draft Convention does not intend these directives to create an explicit legal framework for the criminalisation of cybercrime or for cyber security. As such the adoption and ratification of the draft Convention by African states will not suffice unless states individually establish cyber security laws in accordance with the guidelines contained in the Convention.[12] Unlike the Convention on Cybercrime which upon ratification or accession by member states forms binding law.

Many developing countries are often recommended to implement a conglomeration of existing rules and regulations found in other countries especially in European countries and in the United States. Developing countries are also recommended to create national Computer Emergency Readiness Teams,(CERTs) organizations of cyber security experts to coordinate a nation to respond to cyber incidents.[13]

This is done without acknowledging that inasmuch as the cybercrime phenomenon is universally shared, it manifests itself differently and uniquely in states.[14] For example in Kenya data exfiltration was ranked as the top cyber security threat in 2015 – this is mainly by top employees and cybercriminals, this is followed by social engineering and database breaches. These threats are to the integrity and confidentiality of data.[15] As a result, the African Union regulation- African

[11] Clough J, 'A World of difference: The Budapest Convention on Cybercrime and the challenges of harmonization' 40 *Monash University Law Review* 3 (2014), 700.

[12] Orji Uchenna J, 'A discourse on the perceived defects of the draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber security' *Communications Law*, (2012) 2.

[13] Tagert A, 'Cyber Security Challenges in Developing Nations' unpublished Doctoral Thesis, Carnegie Mellon University Pittsburgh, December 2010, 2.

[14] Tagert A, 'Cyber Security Challenges in Developing Nations' unpublished Doctoral Thesis, Carnegie Mellon University Pittsburgh, December 2010, 5.

[15] SERIANU, Kenya Cyber security Report 2015, Nairobi, 15.

Convention on Cyber security and Data Protection is alive to this reality and this is reflected in its provisions targeted to securing the cyberspace for the purposes of development in ecommerce.[16] Whereas in the developed world e-commerce is well established and the threats they face are complex and more politically motivated such as the Sony Pictures Attack from North Korea as a retaliation for creating a movie depicting the assassination of the North Korea leader, the Bowman dam infrastructure attack where Iranian hackers reportedly gained control of this New York Dam's sluice system in 2013.[17] More recently the Russian hack and US 2016 elections.[18]

This situation is further complicated by different philosophies as regards the regulation of the cyberspace. Cyber libertarians believe that states have no authority whatsoever in the cyberspace and that it should be left alone to address and resolve any real conflicts that may arise with their own means.[19] This position is motivated by the misguided belief that the cyberspace is a lawless place.[20] There is a system of protocols, code and engineering which forms the cyberspace and determines what people can do, how they access the system etc. This is further governed by various internet bodies, IETF, ICANN IGF etc.

This paper's objective is to come up with a theory for internet regulatory policy. By taking into consideration the unique challenges posed to legislation, the different models of laws and incorporating the merits of various philosophies. This theory is aimed at guiding the creation of effective cyber legislation and guiding any new developments as it is clear that innovations in the cyberspace will always outpace the law-making process. Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. If neither of these is achieved then the entire undertaking becomes worthless.

[16] Preamble, article 2, African Union Convention on Cyber Security and Data Protection.

[17] 'Riley Walters: Cyber Attacks on US Companies in 2016' *The Heritage Foundation*, 2 December 2016 http://www.heritage.org/research/reports/2016/12/cyber-attacks-on-us-companies-in-2016 on 9 January 2017.

[18] 'Jeremy Diamond: Russian hacking and the US election; what you need to know' *CNN*, 16 December 2016 http://edition.cnn.com/2016/12/12/politics/russian-hack-donald-trump-2016-election/ on 9 January 2017.

[19] Barlow Perry J, A declaration of the independence of cyberspace, Electronic Frontier Foundation.

[20] Reidenberg J, 'Governing networks and rule-making in Cyberspace' 45 *Emory Law Journal*, (1996), 912.

Internet governance, if taken as the investigation of the regulation of all activities that took place on (or were significantly affected by) the Internet, then 'Internet governance' would be more or less equivalent to 'law and politics'. This approach is too broad and ill-defined to be useful.

As such it is important to present Internet governance from two perspectives.[21] The first is internet governance as ordering of whatever technical systems enable the operation of the global network of networks as a platform for applications. It is regulation of Internet infrastructure, its current operation, and the processes by which it develops and changes over time. This is done by various international agencies; IETF, ICANN, ITU, IGF etc.[22] This regulation is well established and matters most only to network engineers. What matters then is the regulation of human activities and behaviour within the cyberspace. As such formulation of any regulatory policies needs to focus on the relationship between the technical infrastructure, internet architecture and broad policy considerations.[23]

1.1 Statement of the Problem

Enforcing laws in the cyberspace is complicated by the disintegration of traditional sovereignty paradigms and emergence of network sovereignty. This brings about issues of jurisdiction, investigation and adjudication. The existing legal framework is varied yet the nature of these crimes calls for international cooperation. But the cybercrime phenomenon manifests itself differently in different states and they have various goals for their countries in the cyberspace and applying standard already EU or US cyber laws may not be suitable. Moreover, there exists divergent philosophies on how regulation on the cyberspace should be dealt with both of which have merit.

1.2 Justification of the Study

This study is justified by the combination of problems that face law enforcement in the cyberspace. There is a need to develop a comprehensive strategy to guide creation and enforcement of laws globally while appreciating that different states and governments encounter different challenges,

[21] Solum L, 'Models of Internet governance' *Social Science Research Network* (2008), 50-51.

[22] https://www.ietf.org/ Internet Engineering Taskforce, https://www.icann.org/ Internet Corporation for Assigned Names and Numbers, http://www.itu.int/en/about/Pages/default.aspx Internet Telecommunication Union, http://www.intgovforum.org/multilingual/ Internet Governance Forum on 16 December 2016.

[23] Solum L, 'Models of Internet governance', 52.

have various goals and capacities. This is especially crucial because laws evolve at a much slower pace than any innovations in the cyberspace. Having a place to go to for guidance when formulating cyber laws is the goal of this study.

1.3 Statement of Objectives

This paper's objective is to come up with a theory for internet regulatory policy. By taking into consideration the unique challenges posed to legislation, the different models of laws and incorporating the merits of various philosophies. This theory is aimed at guiding the creation of effective cyber legislation and guiding any new developments as it is clear that innovations in the cyberspace will always outpace the law-making process. Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. If neither of these is achieved then the entire undertaking becomes worthless.

1.4 Research questions

What is the cyberspace?

What features of the cyberspace make it difficult to regulate?

What philosophies underlie/fuel regulation in the cyberspace?

How legislative power should be exercised?

Is the cyberspace a lawless place?

Which bodies 'govern' the cyberspace?

Approaches taken by other states towards cyber regulation

Legal versus technical regulation

1.5 Literature review

Lawrence Lessig, 'The law of the horse: What cyber law might teach', *Harvard Literature Review* (1999)

Lessig contrasts the 'Law of the horse' and cyber law an analogy previously used by Judge Frank Easterbrook. Easterbrook who posits that there is no more a 'law of the cyberspace' than there is a 'law of the Horse' and that to speak as if there was such a law would muddle rather than clarify. He argued that courses in law school should be limited to subjects that illuminate the entire law. That the best way to learn the applicable law to specialised endeavours is to study the general rules. The law of cyberspace conceived as torts in the cyberspace, contracts in the cyberspace and property in the cyberspace was not.

Lessing however makes a claim that is specific to the cyberspace. This claim illustrates a merit of seeing cyber law as its own discipline as regulation in the cyberspace shows something other areas would not. He gives an example of *zoning speech* whereby in the real space porn is zoned from kids. Such that whether because of laws (banning the sale of porn to minors) or norms (telling us to shun those who sell to minors) or the market (Porn costs money) It is hard not impossible in the real space for kids to buy porn.

These real-space regulations depend upon certain features in the design of the real space. It is hard in the real space to hide the fact that you are a kid because age is a self-authenticating fact. In cyberspace age is not self-authenticating. Even if the same laws and norms did apply in the cyberspace, and even if the constraints on the market were the same, any effort to zone porn in the cyberspace would face a very difficult problem. To a website accepting traffic all requests are equal. There is no way for a website to distinguish adults from kids. It is a feature in the cyberspace that interferes with the ability to zoning porn. Law faces a choice –whether to change this architectural feature or to leave the cyberspace alone and disable this collective goal. If the former approach is to be taken, what constraints should there be on the law's effort to change the cyberspace's nature?

Lawrence Lessig *Code is Law* (1999) *and Code 2.0* (2006)

Lessig builds on ideas from ‘The law of the horse’ in his subsequent works in Code is Law 1999 and its second edition in 2006. He expounds on the architecture of the cyberspace as a function of its design – or code. This code can change, either because it evolves in a different way or because government or business pushes it to evolve in a particular way. He describes the cyberspace as many places. The character of these many places is not identical. They instead differ in ways that are fundamental. These differences come, in part, from the differences in the people who populate these places. But the demographics alone do not explain the variance. The exchanges and interactions of these people form 'virtual communities' that differ from the communities that they occupy in real space.

The architecture of the Internet equalises people, embodying them with attributes that they may or may not have in real space. Features provided by the architecture of cyberspace can enable classes of people, who were previously considered disabled in real space. For example, deaf people and mute people using computer terminals on the Internet cannot be distinguished from anyone else using it. And with Braille hardware and adaptive software, the blind can 'see' too. It's the closest thing to a parallel world that I've ever experienced. He proposes a constitution not to mean just a legal text but a way of life—that structures and constrains social and legal power, to the end of protecting fundamental values. He uses a metaphor of a constitution as lighthouse—a guide that helps anchor fundamental values.

David Johnson and David Post, ‘Law and borders- The rise of law in the cyberspace’ *Stanford Law Review* (1996)

David Johnson and David Post discuss how physical borders determine to what extent states can exercise their sovereignty and powers. Computer based communications cut across territorial borders and limit a state’s capacity to exercise their authority to make laws and enforce them. They assert that the cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying 1) The power of local governments to assert control over online behaviour; 2) the effect of online behaviour on individuals or things; 3) the legitimacy of a local sovereigns efforts to regulate global phenomena; and 4) the ability of physical location to give notice of which set of rules apply. The

Net thus subverts the system of rulemaking based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules. The rise of an electronic medium that disregards geographical boundaries throws law in to disarray by creating entirely new phenomena that need to become the subject of clear rules that cannot be governed, satisfactorily, by any current territorially based sovereign.

Joel Reidenberg 'Governing networks and rule-making in the cyberspace' ***Emory Law Journal*** **(1996)**

Reidenberg begins by stating that the global network environment defies traditional regulatory theories and policymaking practices**.** Most attempts to define new rules for the development of the Global Information Infrastructure (GII) rely on disintegrating concepts of territory and sector, while ignoring the new network and technological borders that transcend national boundaries. The GII creates new models and sources for rules. He suggest that policy leadership requires a fresh approach to the governance of global networks. Instead of foundering on old concepts, the GII requires a new paradigm for governance that recognises the complexity of networks, builds constructive relationships among the various participants (including governments, systems operators, information providers, and citizens), and promotes incentives for the attainment of various public policy objectives in the private sector.

Philip Weisner, 'Internet governance, standard setting, and self-regulation' ***Northern Kentucky Law Review*** **(2001)**

Weisner affirms that the most formidable regulatory regime that has governed the Internet to date is the institution of open standards. It has allowed the internet to grow exponentially as a network of networks. A series of open protocols, such as the basic protocol that facilitates data transport, the Transport Control Protocol/Internet Protocol (TCP/IP) and others such as HTML, have gained wide acceptance enabling millions to use the internet. It is possible because the standards were open and endorsed by trusted standard setting committees. This, he asserts, helped drive the development of new applications and encouraged the increased usage of the internet. The internet's openness created a virtuous cycle where members of the internet community continued to improve upon it basic architecture adding new functionalities that were placed in the public domain thereby making a more valuable network. It is argued that the shift in the internet from an entirely open standards model to one where there are increasing uses of proprietary standards for critical functions raises a weighty question for internet governance.

As long as the basic standards were in the public domain, the internet's architecture contained a form of self-control that ensured that individuals and developers could easily access critical functions. But as the internet moved to accommodate commerce, the incentives for developing proprietary applications and the increased difficulty in maintaining a categorical commitment to openness were going to be difficult to contain. Consequently the internet community becomes difficult to maintain as a 'commons' model. Before the internet became big business, private standard setting bodies like the IETF could focus on the technical merits of the proposed standard without distorting influence of private companies that would benefit depending on the ultimate outcome.

These works altogether exhibit the ideas embodied in this paper. The first being the fact that the design of cyberspace regulates behaviour of people and cyber law thus merits an independent academic study.[24] It is further acknowledged that the architecture which is a function of design is not immutable and laws can be used to adjust this space but whether that should be done and how it should be done is a difficult and controversial matter. Second the emergence of the GII throws law in to disarray by creating entirely new phenomena that need to become the subject of clear rules that cannot be governed, satisfactorily, by any current territorially based sovereign. This affects the power of localised governments to assert control over online behaviour and the effect of online behaviour on individuals or things.[25] Third that there needs to be a new approach towards internet governance and policy. That the state on its own can never effectively govern the cyberspace and neither can there be no laws at all.

Proper internet governance can only be achieved by cooperation by all the stakeholders.[26] From private entities, users, technical bodies and government. Fourth is that open standards – open access is what has culminated in the meteoric success of the internet. This is made possible by

[24] Lessig L, 'The Law of the Horse: What Cyber law Might Teach', *Havard Literature Review* (1999), 5.

[25] Johnson D, Post D, 'Law and Borders- The rise of Law in the Cyberspace' *Stanford Law review* (1996), 67.

[26] Reidenberg J, 'Governing networks and rule-making in the Cyberspace' *Emory Law Journal* (1996), 912.

endorsed by trusted standard setting committees. However the evolution of the internet to accommodate commerce, the incentives for developing proprietary applications is gradually undermining the open-standards model. Technical bodies are therefore in a dilemma where adopting certain protocols would benefit or undermine certain private companies. That being said technical bodies could be very instrumental in endorsing certain values that governments would like to implement such as free speech – with caveats on hate speech, free-trade etc.[27]

1.6 Theoretical framework

Locke's account of the origins of government and the extent of legislative power in the second treatise for the theoretical framework for this paper. According to Locke, humans were initially in a state of nature. In this state, men are perfectly free to order their actions, and dispose of their possessions and themselves, in any way they like, without asking anyone's permission subject only to limits set by the law of nature.[28] This state was inherently unstable and insecure. Individuals were constantly under threat of physical harm from each other. It became difficult to pursue any goals and endeavours which require stability, peace and cooperation among human beings. It is in this context that government arose. Locke's state of nature is contrasted with cyberspace's state of nature. They are similar in that despite not having a political power in the form of government, there is still some underlying 'law' that determines how things are ordered and coordinated. Laws made need to therefore acknowledge and this existing design in the cyberspace.

In exercising their legislative power governments' should confine themselves to conduct that would be prejudicial to the society's safety, order, and morality.[29] As such any conduct within the cyberspace that only affects the individual in his personal capacity should not be subject to political power. In as much as individuals relinquished some of their rights to a political power, it was so

[27] Weisner P, 'Internet Governance, Standard Setting, and Self-Regulation' *Northern Kentucky Law Review* (2001), 358.

[28] Locke J, *Second Treatise of Government 1689*, Early Modern Texts, 2008, 3. Limits of the law of nature alludes to the idea that we are all equal and no one would be justified to wilfully cause harm to another human being. However should anyone violate this law, then everybody in the state of nature would have a right punish the offender in order to prevent further violations.

[29] Article 50(9), 66, Constitution of Kenya 2010.

that they are able their lives, liberty and fortunes. Any departure from this is an affront to the purpose for which government is established. [30]

It also borrows from Epstein that enacting more laws and regulation may not offer answers or solution to all social or economic problems.[31] This is true both in the physical world as well as in the cyberspace, however within the cyberspace the complexities are even more since the underlying system of how things operate is established by engineering.[31] As such, there may be something to gain by reducing the scope of law[32] and allowing all the stakeholders to come up with solutions to various problems arising in the cyberspace.[33]

1.7 Hypothesis

This paper proceeds on the assumption that any effective policy on internet regulation needs to acknowledge the architecture of the cyberspace which by design is through code. Since code is not immutable, it can be altered to reflect certain desired values and laws. Effective regulation of the cyberspace will arise from a combination of effective laws, a constitution of values and stakeholder cooperation.

[30] Locke J, Second Treatise on Government 1689, 44. This is especially clear in Media Law as regards classification of film. Where the classification board role is to categorize forms of broadcasts. However recently it has gone on to stretch its mandate; acting as content regulator and moral police by banning certain broadcasts. While its role is to guide citizens on which material is suitable for them, they cannot then make that decision for them. [31] Epstein R, *Simple rules for a complex world*, Havard University Press, 1995, 17

[31] Solum L, 'The layers principle: Internet architecture and the law', 815.

[32] Epstein R, Simple rules for a complex world, https://www.commentarymagazine.com/articles/simple-rules-for-ahttps://www.commentarymagazine.com/articles/simple-rules-for-a-complex-world-by-richard-a-epstein/complex-world-by-richard-a-epstein/ on 6 December 2016.

[33] Reidenberg J, 'Governing networks and rule-making in *cyberspace*' 45 *Emory Law Journal* (1996), 912.

1.8 Research methodology

This research was carried out using the following methods, library research, internet searches, as well as interviews with key informants. Such as;

Professor Nii Quaynor is a scientist and engineer who has played an important role in the introduction and development of the internet in Africa. He is a member of the ITU Telecom Board, Chair of the OAU Internet Taskforce and President of the Internet Society of Ghana.

Michael Murungi is Google's East Africa Policy and Government Relations Manager. Before joining Google, he was the CEO of the National Council for Law reporting. He has held several talks in Strathmore Law School on Internet Governance and policy emphasizing on the importance of stakeholder participation.

The Library and internet searches will consist of strategies pursued by various states in with regard to cybercrime. This research will also involve reports, journal articles, and newspaper articles on emerging trends within the cyberspace and scholarly opinion on how challenges may be effectively dealt with.

Interviews will be conducted with key scholars within the industry with a view to develop understanding the phenomenon and finding solutions to emerging issues within the parameters of the research problem.

CHAPTER TWO
Theoretical Framework

2.0 Introduction

This paper attempts to chart a course for governance in the cyberspace. To do this it becomes necessary to interrogate the origins and theories that inform various systems of governance. In doing this the paper borrows from Locke's state of nature in a bid to come with a guide to formulating laws and governance in the cyberspace. The theory departs from the origins of government in the state of nature which came from a poor quality of life which motivated people to relinquish some of their rights to a central authority who would protect them but only to the extent to which they permit. It particularly hinges on the idea that in as much that there was no defined government in the state of nature there was still some sort of law and this is the same for the cyberspace. The cyberspace is not lawless and its architecture by design acts as some kind regulation which can be tweaked depending on market forces or social norms if it is desirable.

Nozick and Mill's propositions on government: that it exists so that people are free to define the good life for themselves and to restrict only behaviour that would be prejudicial to society form the basis on how legislative power should be exercised.

This chapter also stresses on the importance of participation of all stakeholders in coming up with solutions for problems that arise within the cyberspace. This is important first because the pace of law-making will never be as first as evolution and innovation in the cyberspace. Secondly because laws may not always provide the most compelling solutions to challenges that arise.

These ideas altogether form the foundation for further exploring how internet regulatory policies should be formulated. Subsequent chapters will keep referring back to these central ideas and building upon them in order to come with effective strategies for cyberspace regulation.

2.1 Origin of Government

In the *Second Treatise*, Locke offers an account of the origin of government which was a departure from Filmer who posited that humans had always been subject to a political power.[34] According to Locke, humans were initially in a state of nature. In this state, men are perfectly free to order their actions, and dispose of their possessions and themselves, in any way they like, without asking anyone's permission—subject only to limits set by the law of nature.[35] This state was inherently unstable and insecure. Individuals were constantly under threat of physical harm from each other. It became difficult to pursue any goals and endeavours which require stability, peace and cooperation among human beings. It is in this context that government arose. Men saw that it was important to relinquish some of their rights to a central authority in exchange for a guarantee of safety and security of their person their property and interactions with other men in a stable environment.[36] This is the source of political power.[37] *Political Power* being the right to make laws for enforcement of punishment, regulating and preserving property and to employ the force of the community in enforcing the laws for the public good.[38]

Locke thereby draws a distinction between law and government. That even before men relinquished their rights in contract to a central entity and establish Government, there was still a system of law in existence. That there being a state of 'liberty' did not mean that it was a state of 'license' where there are no constraints on how people behave.[40] Men were still governed by law although it did not come from a political source – natural law. Consequently, Aquinas affirms that any positive laws that are made derive from natural law as their foundation.[41]

[34]Internet Encyclopedia of Philosophy, http://www.iep.utm.edu/locke/#SH4a on 7 December 2016, Robert Filmer argued that the monarchy acquired the power to rule and exercised dominion of the rest of the people from God through Abraham, and that this power had been passed in an unbroken chain through the ages. *The Internet Encyclopedia of Philosophy (IEP*) (ISSN 2161-0002) scholarly publication.

[35] Locke J, *Second Treatise of Government 1689*, Early Modern Texts, 2008, 3. Limits of the law of nature alludes to the idea that we are all equal and no one would be justified to willfully cause harm to another human being. However should anyone violate this law, then everybody in the state of nature would have a right punish the offender in order to prevent further violations.

[36] See IEP http://www.iep.utm.edu/locke/#SH4a on 6 December 2016.

[37] Locke, *Second treatise of government* 1689, 2-4.

[38] Locke, *Second treatise of government 1689*, 2.

In looking for a governance system for the cyberspace Locke's theory becomes crucial. His distinction between law and government is particularly pivotal. The absence of a political power-government does not mean that it is a lawless place. The cyberspace has a particular 'state of nature'. A state of nature here means that there is a particular way in which the cyberspace is ordered. The internet architecture layers principle and several protocols is system that arises due to the nature of how the internet was created just as the state of nature arises due to how beings have been created.[39]

Locke's state of nature and the cyberspace's state of nature are similar in that despite not having a political power in the form of government, there is still some underlying 'law' that determines how things are ordered and coordinated. However, a form of government is needed to regulate human behaviour within both environments. Failure to which it will become unstable and insecure for the people in it.[40] This is what justifies governments' involvement in the governance of the cyberspace. Some spheres believe that governments have no authority to make laws and policies within the cyberspace alleging that the internet can regulate itself and through some invisible hand[41] rectify any problems that arise.[42]

Both the cyberspace and the physical space are similar in that they can both be modified by human activity, there is however a striking difference in the cyberspace because its fundamental nature is shaped by engineering.[43] How the Internet runs or cyberspace operates is completely dependent on the code that implements it. As such any form of regulation by government should respect this or risk being ineffective.

[39] Solum L, 'The Layers Principle: Internet Architecture and the Law' 4 *Notre Dame Law review* 1, (2004), 815.

[40] Locke, *Second treatise of government* 1689, 7.

[41] Smith A, *The Wealth of Nations*, MetaLibri, Lausanne, 2007, 349.

[42] Barlow J, *A Declaration of the Independence of the Cyberspace,* 5. Cyber libertarianism purporting to lock any kind of government intervention is completely untenable. For the same reason that Locke gives that: It is unreasonable for men to be judges in their own cases.

[43] Solum L, 'The layers principle: Internet architecture and the law', 827.

state of 'license' where there are no constraints on how people behave.[44] Men were still governed by law although it did not come from a political source – Natural Law. Consequently, Aquinas affirms that any positive laws that are made derive from natural law as their foundation.[45]

In looking for a governance system for the cyberspace Locke's theory becomes crucial. His distinction between law and government is particularly pivotal. The absence of a political power-government does not mean that it is a lawless place. The cyberspace has a particular 'state of nature'. A state of nature here means that there is a particular way in which the cyberspace is ordered. The internet architecture layers principle and several protocols is system that arises due to the nature of how the internet was created just as the state of nature arises due to how beings have been created.[46]

Locke's state of Nature and the cyberspace's state of nature are similar in that despite not having a political power in the form of government, there is still some underlying 'law' that determines how things are ordered and coordinated. However a form of government is needed to regulate human behaviour within both environments. Failure to which it will become unstable and insecure for the people in it.[47] This is what justifies governments' involvement in the governance of the cyberspace. Some spheres believe that governments have no authority to make laws and policies within the cyberspace alleging that the internet can regulate itself and through some invisible hand[48] rectify any problems that arise.[49]

Both the cyberspace and the physical space are similar in that they can both be modified by human activity, there is however a striking difference in the cyberspace because its fundamental nature is shaped by engineering.[50] How the Internet runs or cyberspace operates is completely dependent

[44] See IEP http://www.iep.utm.edu/libertar/ on 6 December 2016.

[45] Aquinas T, *Summa Theologica Question 95*, Article 2.

[46] Solum L, 'The Layers Principle: Internet Architecture and the Law' 4 *Notre Dame Law review* 1, (2004), 815.

[47] Locke, *Second treatise of government* 1689, 7.

[48] Smith A, *The Wealth of Nations*, MetaLibri, Lausanne, 2007, 349.

[49] Barlow J, *A Declaration of the Independence of the Cyberspace,* 5. Cyber libertarianism purporting to lock any kind of government intervention is completely untenable. For the same reason that Locke gives that: It is unreasonable for men to be judges in their own cases.

[50] Solum L, 'The layers principle: Internet architecture and the law', 827.

on the code that implements it. As such any form of regulation by government should respect this or risk being ineffective.

Governments should not expect to achieve any worthwhile regulation by just imposing legislation that does not take into consideration these special conditions.

On its own the internet is built perfectly such that it would not need any external forms of regulation. It is the human interactions that take place in the cyberspace that make governments' intervention necessary.

Understanding the various principles underlying the internet's architecture, (layers Principle, and its corollary principles) together with legal, political and ideological theories that inform governance, should create a theory of Internet regulation policy.[51] This theory should inform any sort of legislation adopted by states. Such that even when new functionalities and innovations on the internet are developed, the underlying theory can be varied to capture any new 'regulatory gaps' that may arise.

2.2 The Extent of Legislative Power

The government and by extension state exists to provide the appropriate conditions for the individuals to define the good life for themselves just as long as they do not impede the ability of others to do the same.[52] As soon as any part of a person's conduct affects prejudicially the interests of others, the state has jurisdiction over it. The question that arises for discussion is whether the general welfare will or will not be promoted by interfering with it. However, when a person's conduct does not affect any persons interests other than his own, there is no room for such intervention.[53]

In exercising their legislative power governments should confine themselves to conduct that would be prejudicial to the society's safety, order, and morality.[54] As such any conduct within the

[51] Solum L, 'The layers principle: Internet architecture and the law' ,851

[52] Nozick R, *Anarchy, State and Utopia*, Blackwell publishers, 1974, 26, http://www.iep.utm.edu/noz-poli/ on 6 December 2016.

[53] Mill J, *On Liberty 1859,* Batoche Books (2001), 69.

[54] Article 50(9), 66(1), Constitution of Kenya 2010.

cyberspace that only affects the individual in his personal capacity should not be subject to political power. In as much as individuals relinquished some of their rights to a political power, it was so that they are able their lives, liberty and fortunes. Any departure from this is an affront to the purpose for which government is established. [55]

It is also important to be cognizant of the fact that enacting more laws and regulation may not offer answers or solution to all social or economic problems.[56] This is true both in the physical world as well as in the cyberspace, however within the cyberspace the complexities are even more since the underlying system of how things operate is established by engineering.[57] As such, there may be something to gain by reducing the scope of law[58] and allowing all the stakeholders to come up with solutions to various problems arising in the cyberspace.[59]

Internet governance, if taken as an as the investigation of the regulation of all activities when they took place on (or were significantly affected by) the Internet, then 'Internet governance' would be more or less equivalent to 'law and politics'. This approach is too broad and ill-defined to be useful. As such it is important to distinguish internet governance from two perspectives.[60] The first is internet governance as ordering of whatever technical systems enable the operation of the global network of networks as a platform for applications. It is regulation of Internet infrastructure, its current operation, and the processes by which it develops and changes over time. This is done by various international agencies; Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), Internet Telecommunication Union, (ITU), Internet

[55] Locke J, *Second Treatise on Government* 1689, 44. This is especially clear in media law as regards classification of film. Where the classification board role is to categorize forms of broadcasts. However recently it has gone on to stretch its mandate; acting as a content regulator and moral police by banning certain broadcasts. While its role is to guide citizens on which material is suitable for them, they cannot then make that decision for them.

[56] Epstein R, *Simple rules for a complex world*, Havard University Press, 1995, 17

[57] Solum L, 'The Layers Principle: Internet architecture and the law', 815.

[58] Epstein R, https://www.commentarymagazine.com/articles/simple-rules-for-a-complex-world-by-richard-a-epstein/ on 6 December 2016.

[59] Reidenberg J, 'Governing networks and rule-making in *cyberspace*' 45 *Emory Law Journal* (1996), 912.

[60] Solum L, 'Models of internet governance' *Social Science Research Network* (2008), 50-51.

Governance Forum (IGF) etc.[61] This regulation is well established and matters most only to network engineers. What matters then is the regulation of human activities and behaviour within the cyberspace. As such formulation of any regulatory policies needs to focus on the relationship between the technical infrastructure, internet architecture and broad policy considerations.[62]

This Chapter has discussed the relation between law and government. That law precedes government and government exists to preserve liberty. This discussion therefore sets the stage for the discourse on how to achieve good governance through sound regulatory policies on the internet. This entails examining the existing legal framework of regulation in light of these foundational premises.

[61] Internet Engineering Task Force, 'About Us' https://www.ietf.org/ Internet Engineering Taskforce, https://www.icann.org/ Internet Corporation for Assigned Names and Numbers, http://www.itu.int/en/about/Pages/default.aspx Internet Telecommunication Union, http://www.intgovforum.org/multilingual/ Internet Governance Forum on 16 December 2016.

[62] Solum L, 'Models of Internet Governance', 52.

CHAPTER THREE

The Challenge of Legislating Civil and Moral Wrongs in the Cyberspace

3.0 Introduction

The problem this paper seeks to address is governance of the cyberspace. The challenge of control and enforcement of civil and moral wrongs within the cyberspace stems from the very nature of the global information infrastructure.[63] Cyberspace and Global Information Infrastructure ("GII") shall be used simultaneously in this paper to refer to the non-physical complex environment resulting from the interaction of people, software and services over the internet by the means of technology devices and networks.[64] Contrary to popular belief the Global Information Infrastructure is not a lawless place; there are protocols and systems embedded in the networks and devices that control and determine how people interact with each other in the cyberspace.[65] For example network and device logins, network protocols, code, etc.[66](Refer to chapter 2 above) These determine who can access certain material, what you can and cannot do with your device, code in the Youtube application for example has enabled policing of copyright infringement.

The global network environment defies traditional regulatory theories and policymaking practices. This is evidenced by disintegrating concepts of territory and sovereignty, ambiguous substantive borders, powerful network communities[67] and visible network boundaries (these will be discussed below). Yet most attempts at developing new rules for the cyberspace fail to take into account these essential features.[68] This poses a fundamental challenge for effective leadership and governance. Due to the fact that laws and regulation can and do affect infrastructure development,

[63] Reidenberg J, 'Governing networks and rule-making in cyberspace' 45 *Emory Law Journal*, (1996) 912.

[64] Serianu, *Rethinking cyber security- An integrated approach: process, intelligence and monitoring,* (2014), Kenya Cyber Security Report, 9.

[65] Lessig L, *Code 2.0* (2006), 5.

[66] Lessig L, *Modalities of regulation*, 1999, 1- Code is Law.

[67] Johnson D, Post D, 'Law and borders, The rise of law in cyberspace', *Stanford Law Review* (1996), 4.

[68] Reidenberg J, 'Governing Networks and Rule-Making in Cyberspace' 45 *Emory Law Journal*, (1996) 912.

innovation and behaviour of GII participants, it is crucial to get it right so that the societal values are respected and adhered to.[69]

3.1 Features of the Cyberspace/ Global Information Infrastructure.

The features of the cyberspace that pose a challenge to governance stem from the disintegration of traditional sovereignty paradigms and emergence of network sovereignty.[70] Legal rules are generally made to govern distinct subject areas for defined territories.[71] These substantive areas and territorial sovereignty are what justify the regulatory authority and policymaking for states. Criminal law, administrative law belongs to the realm of public law, intellectual property rights protect certain aspects of information and its economic value. These laws are enforced by the relevant regulatory agencies in corresponding territories. The GII is designed so that persons from different geographical locations are able to interact under one roof, without the physical inhibitions of space and time these interactions range from contract, social media, publishing content, ecommerce etc.[72] Such interactions touch and sometimes blur various substantive areas of the law.[73]

3.2 Disintegration of Traditional National Borders

3.2.1 Permeable National Borders

The cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location.[74] Regulatory powers have always been defined by national

[69] Lessig L, *Code 2.0* (2006), 5.

[70] Reidenberg J, 'Governing networks and rule-making in cyberspace', 913, 917.

[71] *American Banana Company v United Fruit Company* (1909) 213US page 347and 357. (Holding that as a general rule of construction, any statute is presumed to be intended to operate within the territorial limits of the sovereign).

[72]Johnson D, Post D, 'Law and borders, The rise of law in cyberspace', 1.

[73] Reidenberg J, 'Multimedia as a new challenge and opportunity in privacy: The examples of sound and image processing', 22 *Materialien zum Datenschutz* 9, (1995) 9.

[74] Johnson D, Post D, 'Law and borders, The rise of law in cyberspace' 2.

borders, however transnational information flows on the GII undermine the capacity of national governments to exercise control of legally significant transactions.

This can be illustrated by the following scenario; a website with DNS registered territorially (.ke, .za, .uk) or one that can be anywhere in the world (.com) maliciously orchestrates a scheme to solicit confidential information from citizens by scripting/hijacking[75] a legitimate government site and using that information to defraud unsuspecting citizens, it would be nearly impossible to hold any person accountable.

First, a website registered in a particular country is bound by the particular laws of that regardless of the fact that the domain name may be used and accessed by different individuals in different geographical reaches. This is especially complicated by the fact that web hosting servers maybe in yet another country. Therefore even after justifying to the registering country why you should hold the owner of that domain name responsible, you would still have to go to yet another country to get evidence from the web hosting servers and most countries are not hospitable to such requests as it would expose them to potential cyber risks latent in such access.

Secondly, even if the offending device was to be found within the territorial limits of that state, it would be difficult to show that the person who was found with it was the perpetrator. This is because one can simply argue that they did not do; as multiple persons may have had access and in order to get proof of that enforcement agencies have to get warrants to get information from service providers raising issues of privacy and data protection[76] which providers are not willing to disclose and courts are uncertain about ruling on them.[77]

Hence a situation in which prima facie involved fraud, other issues dealing with other substantive laws such as privacy, data protection and property become prominent and need to be addressed. The predominant question being whose law applies, which governmental agencies should prosecute the offender; the victim of the crime or the state in which the domain is registered and the perpetrator resides. Even if one was to solve these issues how are they to be enforced within

[75] Open Web Application Security Project: Cross-site Scripting https://www.owasp.org/index.php/Cross-site_Scripting_(XSS) on 17 November 2016.

[76] Cohen J, 'Examined lives: Informational privacy and the subject as object', 52 *Stanford Law Review* 1373 (2000), 571.

[77] *United States v Morris,* Court of Appeal, Judgement on 7 March 1991, 11.

the cyberspace where there already exists code and system of running things and network communities which have replaced the physical proximate ones.[78]

3.2.2 Ambiguous substantive borders

This has been alluded to in the previous paragraph whereby governance has historically relied on distinctions and borders in substantive law. Intellectual property has been distinct from privacy just a telecommunications law is distinct from financial services law. The GII blurs substantive borders and the corresponding rights get jumbled up. A classic example today is how network service providers such as Safaricom which is a telecommunication company provides financial services such as payment, savings and loans which traditionally are within banks purview and banks such as equity offering platforms similar to network service providers – Equitel. It is also evidenced in how cable companies such as Zuku offer voice communication over and above the cable services. All this has been enabled by packet-data switching. However, the effect has been to undercut the well-defined borders of communication law.

Processing instructions can, for example, be embedded in a semiconductor chip to benefit from sui generis legal protection, stored on a floppy disk to be covered under copyright, or incorporated in a device to obtain patent protection.[79] This substantive blurring of rights creates significant uncertainty; the degree and scope of protection become variable.[80]

Another effect of blurring of the substantive borders is that, objectives of one body of law such as privacy can be achieved by application of another field of law rules such as intellectual property.

3.3 Emergence of Network Sovereignty

The network's architecture together with network service providers establish rules of participation in the cyberspace. These rules create visible borders within the cyberspace and the network communities acquire certain sovereign powers.

[78] Reidenberg J, 'Governing networks and rule-making in cyberspace', 914.

[79] Ginsburg J, 'The cyberian captivity of copyright: Territoriality and authors' rights in a networked world' 15 *Santa Clara Computer and High Technology Law Journal* 347 (1999), 124.

[80] Reidenberg J, 'Governing networks and rule-making in cyberspace'915.

3.3.1 Visible network borders

The presence of various network providers within any geographical area establishes a kind of boundary such that if you belong in Safaricom your access and activities in the GII are through the Safaricom network- not Airtel, MTN, or Verizon. These different service providers avail to their users' particular services and pricing options. Before proliferation of mobile money Safaricom was the only provider offering financial services within its network, hence you could only use this service if you belonged to the Safaricom network. While doing this the providers essentially determines what you can do over the network. An example is that before you can access the network you have to register the line(simcard) using a national identity card, to access the payment service you have to activate the account and setup a password, withdrawal has to be done through certified agents and so on. Therefore these networks setup borders and rules of engagement and as a result are able to police activities over the network acquiring some sovereign powers.

Technical standards set default boundary rules in the network that tend to empower selected participants. Web applications are capable of storing history and cache temporarily. This enables one to easily access frequented sites and to keep track of sites visited on a site. This is especially important for child safety. Further still these applications such as Google, Instagram, Youtube and Facebook have found ways to leverage this information gathered from the users to companies for advertisement on their platforms essentially commercializing information volunteered by users.

Technical standards may be market driven or set by a standards body. An example of a market driven standard is the QWERTY keyboard. As soon as they became popular, it became a standard and all keyboards are manufactured this way[81]. Technical standards set by a standards body seek to identify and recommend technical specifications for particular network needs such as security.

3.3.2 Powerful Network Communities

In addition to the new "geography" of borders, networks may now even supplant substantive, national regulation with their own rules of citizenship and participation. Networks themselves take on political characteristics as self-governing entities. They determine the rules and conditions of

[81] International Standards, Conformity, Assessment, and U.S, Trade Policy Project Committee, *Standards Conformity Assesment, and Trade into the 21st Century*, National Academy Press, Washington D.C, 1995, 24

membership. Private contracts mediate the rights and responsibilities of participants. Service providers offer different terms of adherence.

Networks also determine the rules of participant behaviour. This characteristic can result in rules that reverse established territorial laws.[82] An example is when Google Books was starting up they went all round the big libraries in attempt to secure publications on their platform. This activity was seen as an infringement of copyright holders' rights to adapt, distribute and reproduce their work and receive benefits from it. [83]

Like nation-states, network communities have significant powers to enforce rules of participant conduct. Service providers may terminate access for offending participants, applications have instituted self-policing mechanisms whereby one can report offensive and inappropriate content from users (this is prevalent in social media sites).[84] The network can also be able to block spam and pop up advertisements which are unsolicited.

States are identified by territory, government, population and laws and enforcement institutions.[85] As discussed above the cyberspace contains certain parameters and one knows the moment they have entered it, there is a system of regulation through the architecture, code and technical standards, and the network communities are contrasted to governments since they have the power to make rules and policies & enforce them on their users. Therefore any new rules promulgated should acknowledge that there is already a system, infrastructure and order in the cyberspace and using traditional governance theories will be futile. Instead of foundering on old concepts, the GII requires a new paradigm for governance that recognises the complexity of networks, builds constructive relationships among the various participants (including governments, systems

[82] National Research Council, *Rights and responsibilities of participants in networked communities,* The National Academies Press, 1994, Chapter 2 http://iimk.ac.in/gsdl/cgi-bin/library?e=d-000-00---0ecomme--00-0-0--0prompt-10---4------0-1l--1-en-50---20-about---00031-001-1-0utfZz-8-00&a=d&cl=CL1&d=HASH01470e354abbaed6735e60f1.4 eBook on 27 January 2017.

[83] *Authors Guild v Google*, U.S. Court of Appeals for the Second Circuit, 2015.

[84] Australia Cybercrime Online Reporting Network (ACORN) https://www.acorn.gov.au/protect-and-prevent/social-media on 27 January 2017

[85] Article 1, Convention on the Rights and Duties of the State, (1933).

operators, information providers, and citizens), and promotes incentives for the attainment of various public policy objectives in the private sector.

3.4 Cyber Libertarianism and Cyber Paternalism/collectivism

The emergence of network sovereignty, has led to divergent schools of thought as regards governance of the GII, the most prominent schools being cyber libertarianism and paternalism.

The *Cyber Libertarianism* school posits that individuals acting in whatever capacity they choose (as citizens, consumers, companies, or collectives) should be at liberty to pursue their own tastes and interests online.[86] It rejects any form of control by established governments and maintains that network freedom is freedom from state action which reorders its affairs to supposedly make certain people or groups better off or to improve some amorphous "public interest"—an all-to convenient facade behind which unaccountable elites can impose their will on the rest of us.

John Perry Barlow, in his work *A Declaration of the Independence of the Cyberspace* most intelligibly expresses this position:

'We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.'[87]

Cyber Paternalism/collectivism on the other hand advances the notion that the cyberspace would be untenable if no form of regulation is observed. It suggests that governance should be undertaken collectively with the various stakeholders (users, private corporations, technical experts and the

[86] Techliberation https://techliberation.com/2009/08/12/cyber-libertarianism-the-case-for-real-internet-freedom/ accessed on 16th November 2016

[87] Barlow J*, A Declaration of Independence of the Cyberspace,* 1996, Electronic Frontier Foundation.

government) all of whom have an interest in ensuring that GII is able to facilitate their different goals.

States have direct interests in the development of an information society. The private sector has a crucial role in the creation of the GII. Technologists have a pivotal position for policy choices and the GII empowers citizens to establish rules of their own. Policymaking among these different interest centers is intertwined. For example, technological choices may frustrate or support state interests or citizen goals. Overlapping jurisdiction and the rapid evolution of information technology defy the traditional forms of state control.[88]

While states cannot take over the control of the cyberspace, what this school suggests is that they can influence rule making by the networks. States can provoke the creation of network standards this is evident in the Youtube example that was alluded to earlier whereby the application in its capacity as an intermediary has mechanisms to detect copyright infringement and must inform the offender and authorise takedown of such material. If it fails to do this it may be held liable for intellectual property violations by the real world's enforcement agencies.[89]

Larry Lessig one of the proponents of this position, critiques the perceived freedom that cyber libertarians identify with by comparing it to post-communist Russia. Where people hastened to usher in the new regime of free markets and freedom. But instead one system of tyranny by the state was replaced with another run by the Mafiosi.[90] Cyberspace libertarians, propound the view that the market-driven forces shall guide activities by some sort of invisible hand. which in post-communist Russia failed.

Lessig instead suggest Liberty in cyberspace will not come from the absence of the state. Liberty there, as anywhere, will come from a state of a certain kind. Liberty is built by setting society on a kind of constitution. By constitution he means an architecture and not just a legal text that structures and constrains social and legal power, to the end of protecting fundamental values. He compares it to the Bill of Rights that affirm the values that are held dear by society which are critical to ensuring that powers held by the state is checked to ensure all peoples well-being.

[88] Reidenberg J, 'Governing Networks and Rule-Making in Cyberspace' ,926.

[89] Article 14, Digital Millennium Copyright Act.

[90] Lessig L, *Code 2.0* (2006), 2.

This chapter outlines various challenges of cyber regulation. These range from disintegration of traditional borders both territorially and in the substance of laws, as well as emergence of network sovereignty- this refers to actors outside of government who control key aspects of the communication and information infrastructure which governments would ordinarily handle. It therefore follows that enactment of laws should be aimed at clarifying how these inherent challenges should be resolved and not compound them at the very least. The following chapters look at the legal framework for cyberspace regulation in order to determine their efficacy in deterring illicit behaviour in the cyberspace as well as facilitating enforcement.

CHAPTER FOUR

International Legal Framework

4.0 Introduction

It is curious, that regulation on cybercrime and security began at the international level.[91] The advent of the internet made interaction across the globe in real-time workable.[92] This interaction is at all spheres of life: social, economic and political. This shift presented a regulatory nightmare for states as their reach in many interactions was restricted due to the fact that they transcended their borders, touched on various substantive aspects of law and because the rules of engagement within the cyberspace differed significantly from those of the physical world.

The Council of Europe formulated the Budapest Convention on Cybercrime with the intention of harmonising international laws in order to pursue a common agenda to combat cybercrime.[93] However what has emerged is that states are taking the Convention as a guideline and tailoring their own statutes in accordance with their own goals and challenges they experience.

[91] Weber A, 'The Council of Europe's Convention on Cybercrime', 18 *Berkley Technology Law Journal* 1 (2003) 429.

[92] Murungi M, *Cyber Law in Kenya*, Kluwer Law International, The Hague 2011, 28.

[93] Preamble, Convention on Cybercrime.

It is important to note that inasmuch as the cybercrime phenomena is universally shared, it manifests itself differently and uniquely in states.[94] For example in Kenya data exfiltration was ranked as the top cyber security threat in 2015 – this is mainly by top employees and cybercriminals, this is followed by social engineering and database breaches. These threats are to the integrity and confidentiality of data.[95] As a result, the African Union, regulation- African Convention on Cyber security and Data Protection is alive to this reality and this is reflected in its provisions targeted to securing the cyberspace for the purposes of development in ecommerce.[96] Whereas in the western world ecommerce is well established and the threats they face are complex and more politically motivated such as the Sony Pictures Attack from North Korea as a retaliation for creating a movie depicting the assassination of the North Korea leader, the Bowman dam infrastructure attack where Iranian hackers reportedly gained control of this New York dam's sluice system in 2013.[97] More recently the Russian hack of the Democratic National Convention (DNC) and the effect it has on the integrity of the US 2016 elections.[98] The bottom-line here is that the nature of the cyberspace and interactions upon it necessitated an international approach to regulation. Seeing as it is impossible to regulate criminal behaviour without a means to ensure enforcement of sanctions, international cooperation remains central to facilitating such enforcement.[99]

The following two Chapters will discuss the legal framework at the international regional & national levels. It will seek to examine whether the challenges in chapter three to regulation have been adequately taken care of. It will also interrogate two aspects of regulation in an attempt to come up with an effective theory for internet regulatory policy. The first aspect is how to formulate effective cyber laws. This will be done by looking at various strategies undertaken by various

[94] Tagert A, 'Cyber Security Challenges in Developing Nations' Published Doctoral Thesis, Carnegie Mellon University Pittsburgh, December 2010, 2.

[95] Serianu, Kenya Cyber security Report 2015, Nairobi, 15.

[96] Preamble, Article 2, African Union Convention on Cyber Security and Data Protection.

[97]'Walters R: Cyber Attacks on US Companies in 2016' *The Heritage Foundation*, 2 December 2016 http://www.heritage.org/research/reports/2016/12/cyber-attacks-on-us-companies-in-2016 on 9 January 2017.

[98]Diamond J: Russian hacking and the US election; what you need to know' *CNN*, 16 December 2016 http://edition.cnn.com/2016/12/12/politics/russian-hack-donald-trump-2016-election/ on 9 January 2017.

[99] Weber A, 'The Council of Europe's Convention on Cybercrime', 18 *Berkley Technology Law Journal* 1 (2003) 429.

states both in the developing and developed world. The merits and demerits of both sides will be discussed with an aim of coming up with an effective guide for formulating cyber laws.

The second aspect is founded on the assertion that liberty in cyberspace will not come from the absence of the state. Liberty there, as anywhere, will come from a state of a certain kind. 'We build a world where freedom can flourish not by removing from society any self-conscious control, but by setting it in a place where a particular kind of self-conscious control survives.'[100] Liberty in the cyberspace shall therefore be achieved by setting the society on a certain *Constitution.* A constitution here means an architecture that structures and constrains social and legal power, to the end of protecting fundamental values. Just constitutions guarantee fundamental values in the form of bill of rights (speech, privacy, due process), there needs to be a constitution for the cyberspace that enshrines various values that ought to be protected. A commitment to these substantive values would remain despite the passing fancies of normal, or ordinary, government.[101] The challenge here is coming up/ choosing between a set of values such as:[102] Will cyberspace promise privacy or access? Will it enable a free culture or a permission culture? Will it preserve a space for free speech? Once a set of values is agreed upon then code can be used to implement since the architecture of the cyberspace is based upon it. We can build, architect, or code cyberspace to protect values that we believe are fundamental. Or we can build, architect, or code cyberspace to allow those values to disappear.

This chapter finally argues that effective cyber laws need to be complemented by *Constitution* – a set of values that underpin interactions on the cyberspace. It's only when both of these aspects are together that there'll be adequate regulation. After a *Constitution* is agreed upon then these values can be implemented in the cyberspace through code. The technical standard setting bodies are critical to this process. Just as they were able to endorse standards during the development of the internet they can then implement a *Constitution* through code. This would ensure that laws are complemented and better enforcement is affected.

[100] Lessig L*, Code 2.0,*2006, 4.

[101] Wendell H, 'The Path of the Law' 10 *Harvard Law Review* (1897), 457.

[102] Merritt S, Marx L, *Does Technology Drive History? The Dilemma of Technological Determinism,* Cambridge: MIT Press, 1994, 1-35.

4.1 Budapest Convention on Cybercrime

The Convention on Cybercrime was adopted in Budapest in 2001 and entered into force in 2004. Although the Convention originated from the Council of Europe, [103] it has been ratified by a number of non-member states (Australia, Mauritius, Dominican Republic, Israel, Panama, Sri Lanka) and observer states (Canada, Japan United States and South Africa).[104]

The Budapest Convention is a multilateral agreement geared at facilitating international cooperation in the prosecution of cyber criminals.[105] It is the first international treaty on crimes seeking to address internet and computer crime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations.[106] It contains provisions on infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.[107] Its main objective, set out in the preamble, is to pursue a common criminal

[103] The Council of Europe 'About us' http://www.coe.int/en/web/about-us/who-we-are on 9 January 2017. The Council of Europe is an international organization focused on promoting human rights, rule of law and democracy in Europe. It has 47 member States.

[104] Council of Europe, Chart of Signatures and Ratification of Treaty 185, Convention on Cybercrime as of 2 February 2017 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

[105] Weber A, 'The Council of Europe's Convention on Cybercrime', 18 *Berkley Technology Law Journal* 1 (2003), 427.

[106] Weber A, 'The Council of Europe's Convention on Cybercrime', 18 *Berkley Technology Law Journal* 1 (2003) 429.

[107] Council of Europe https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.[108]

The treaty consists of four chapters. Chapter I defines terms used by the treaty. Chapter II establishes a common cannon of computer-based and computer-related crimes, requiring a common set of procedural powers, and loosely establishes a set of rules by which parties can assert jurisdiction. Chapter III sets up a framework for cooperation in the use of those powers. Chapter IV includes miscellaneous provisions common to most Council of Europe treaties.[109]

4.2 Internet Bodies

These are the bodies that govern the internet's architecture, technical standards and working making possible all the interactions that subsist presently. These bodies' work is well established and uncontested.[110] However, because they are responsible for the internet's working and nature they are crucial in the regulatory framework.[111]

4.2.1 Internet Engineering Task Force (IETF)

This body develops and promotes voluntary internet standards in particular the standards that comprise the Internet protocol suite (TCP/IP). It is an open standards organisation, with no formal membership or membership requirements. All participants and managers are volunteers, though their work is usually funded by their employers or sponsors.[112]

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

[108] Preamble, Convention on Cybercrime ETS No. 185.

[109] Article 26 -32, Convention on Cybercrime ETS No.185.

[110] Interview with Quaynor N, on 15 December 2016, During the Coala Block Chain Workshop at Strathmore Business School. Professor Nii Quaynor is a scientist and engineer who has played an important role in the introduction and development of the internet in Africa. He is a member of the ITU Telecom Board, Chair of the OAU Internet Taskforce and President of the Internet Society of Ghana.

[111] Lessig L, *Code 2.0* (2006), 5.

[112] International Engineering Task Force 'About Us' https://www.ietf.org/about/ on 9 January 2017.

The actual technical work of the IETF is done in its working groups, which are organised by topic into several areas (e.g., routing, transport, security, etc.). Much of the work is handled via mailing lists. The IETF holds meetings three times per year.

The IETF working groups are grouped into areas, and managed by Area Directors, or ADs. The ADs are members of the Internet Engineering Steering Group (IESG). Providing architectural oversight is the Internet Architecture Board,(IAB). The IAB also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society (ISOC) for these purposes. The General Area Director also serves as the chair of the IESG and of the IETF, and is an ex-officio member of the IAB.[113]

4.2.2 Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN was formed in 1998. It is a not-for-profit partnership of people from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers.[114]

To reach another person on the Internet you have to type an address into your computer - a name or a number. That address has to be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination we wouldn't have one global Internet.

ICANN does not control content on the Internet. It cannot stop spam and does not deal with access to the Internet. But through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet.

4.2.3 Internet Governance Forum (IGF)

IGF is a multi-stakeholder forum for policy dialogue on issues of internet governance. It brings together all stakeholders in the Internet governance debate, whether they represent governments, the private sector or civil society, including the technical and academic community, on an equal basis and through an open and inclusive process.[115] The establishment of the IGF was formally

[113] International Engineering Task Force 'About us' https://www.ietf.org/about/ on 9 January 2017.

[114] International Corporation for Assigned Names and Numbers https://www.icann.org/resources/pages/what-2012-02-25-en on January 9 2017.

[115] Internet Governance Forum http://www.intgovforum.org/cms/aboutigf on 9 January 2017.

announced by the United Nations Secretary-General in July 2006. It was first convened in October–November 2006 and has held an annual meeting since then.

4.2.4 Internet Research Task Force (IRTF)

The IRTF promotes research of importance to the evolution of the Internet by creating focused, long-term research groups working on topics related to Internet protocols, applications, architecture and technology.

Research groups have the stable long term membership needed to promote the development of research collaboration and teamwork in exploring research issues. Participation is by individual contributors, rather than by representatives of organisations.[116]

4.3 Formulating Effective Cyber laws

Chapter Three discusses the challenges that regulating the cyberspace has faced. It is therefore a laudable effort on the part of Council of Europe for formulating the Convention on Cybercrime. It was a step in the right direction as it contains comprehensive provisions not only substantively but also procedurally stressing on cooperation, information sharing and the handling of digital evidence. It however falls short on the part of protecting privacy and enhancing innovation.[117] As such it infringes on certain liberties of persons in the cyberspace. The delicate part of regulation is balancing the interests of law enforcement whilst ensuring that certain liberties are protected. Lessig's idea on having *Constitution* that enshrines these values and provides instances where they may be limited becomes a prudent solution to this dilemma.[118]

It is also ironic that despite the central role the internet's architecture has on any pursuit of regulation, there has been no attempt to consult with the technical internet bodies who set standards that facilitate the working of the internet. The involvement of technical bodies would be particularly insightful if adequate regulation is to be affected particularly because they have

[116] International Research Task Force, https://irtf.org/ on 9 January 2017.

[117] Article 26, 29, 30, 31, Convention on Cybercrime. This provisions provide States with avenues to preserve, store and disclose data with each other without a safeguard for users. This situation is similar to Snowden leaks where by the government argued that the mass surveillance on people but never used the data. That it was instead stored and then when necessary a court order would be sought from the Foreign Intelligence Surveillance Act (FISA) courts.

[118] Lessig L, *Code 2.0*, 2006, 4.

experience in how it works and also because they can effect changes in the infrastructure in order to reflect the spirit of the law.

Laws on the cyberspace have been led by governments. Even the Council of Europe is conglomerate of European countries. It is more likely than not that the process will be politically motivated or the outcome is such that a large part of the international community is excluded. This is clearly evidenced by the fact that even though it is hailed as an international convention the parties are Council of Europe countries US, Canada, Japan, Australia, Israel, Mauritius, and Panama. A total of 50 countries. If cybercrime and security is a universal concern how come then only a quarter of the countries have agreed to come together to address it? Law-making therefore needs to go beyond just governments and seek input from all other stakeholders.

Since the cyberspace cuts across territories and covers all people in the world, it is not unreasonable to expect that there are common set values that all persons are expected upheld and protected. Therefore for there to be any truly international undertaking these values need to be well established and settled. This can be compared to certain disciplines such as international environmental law where there are generally agreed principles such as sustainable development, generational equity, prevention and precaution. This is the same approach that regulation in the cyberspace should take. These principle are not to come from government but from a combined effort from industry, academia, governmental organization and as well as the users. As was the case with Rio, Stockholm and Nairobi conventions.[119]

The following section discusses strategies undertaken by Canada to preserve and protect cyber security. This is in order to chart a path on how governments' should formulate policies in order to protect their communications and information infrastructure.

[119] Birnie P, Boyle A, *International Law and the Environment, Oxford University Press*, New York, 2009, 106.

CHAPTER FIVE

Regional and National Legal Framework

5.0 Introduction

The previous chapter discusses the importance of having an international system of laws for cyber regulation.[120]The current international system is the convention on cybercrime we however see that it is really not as international as it has been hailed with most parties being in Europe and other western countries several continents are not represented. South Africa is the only country in Africa that has signed the convention.

The existence of a parallel system of laws is also due to the fact that developed and developing countries face varied challenges as was discussed in Chapter Three. Developing countries are faced with challenges involving the integrity of data and fraud as regards electronic transactions. Hence the African Union legal framework in particular stresses on empowering people to engage in electronic transactions confidently and facilitating E-commerce. However, developed countries have mass surveillance systems for spying on each other and their own citizens, Hence they have more complex threats such as attacks on critical infrastructure as well as politically motivated attacks such as the Russian on the DNC and the effects it had on the integrity of the US 2016 elections. [121]

This chapter interrogates the efficacy of the upcoming regional and national legal frameworks for cyberspace regulation. These frameworks are fairly recent. The AU Convention 2014 and Kenya cyber security bill has yet to be passed. These divergent systems of laws present a potential challenge for law enforcement as they do not provide cooperation and information sharing or capacity building and training for both the enforcement agencies as well as the judiciary. This Chapter also discusses the experiences of South Africa in adjudicating cyber cases given its relatively longer experience compared to other African countries.[122]

[120] Clough J, ‘A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonization’ 40 *Monash University Law Review* 3 (2014), 700.

[121] Tagert A, ‘Cyber Security Challenges in Developing Nations’ unpublished Doctoral Thesis, Carnegie Mellon University Pittsburgh, December 2010, 2.

[122] The Electronic Communications and Transactions Act 25 of 2002.

5.1 African Union Convention on Cyber security and Data Protection

The Convention was first drafted in 2011 and was adopted on June 27, 2014 with the last signature on January 29, 2016.[123] The Convention covers a very wide range of online activities, including electronic commerce, data protection, and cybercrime, with a special focus on racism, xenophobia, child pornography, and national cyber security.[124] Following its passing, many African nations have begun the process of enacting personal data protection laws for the first time, upheld by new, independent public authorities. This move represents a huge boon to user control over private information. In addition, each state is required to develop a national cyber security strategy, pass cybercrime laws, and ensure that e-commerce is "exercised freely."[125]

The Convention establishes a legal framework for cyber-security and personal data protection embodying the existing commitments of African Union Member States at sub-regional, regional and international levels to build the Information Society.[126] It takes into account the requirements of respect for the rights of citizens, guaranteed under the fundamental texts of domestic law and protected by international human rights conventions and treaties, particularly the African Charter on Human and Peoples' Rights. This Convention seeks to establish an appropriate normative framework consistent with the African legal, cultural, economic and social environment.[127]

5.2 The Kenya Cyber security and Protection Bill

The Kenya Cyber Security and Protection Bill as at January 2017 is still in parliament. It is a Bill to provide for the enhancement of security in cyberspace; to provide for the prohibition, prevention, detection, response, investigation and prosecution of cybercrimes to establish the national cyber security response unit.[128] It mainly focusses on the establishment of a National Cyber Threat Response Unit that shall be a department within the Ministry responsible for matters

[123] Article 36, African Union Convention on Cyber security and Data Protection. The Convention entered into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification on 27 June 2014.

[124] Preamble, African Union Convention on Cyber Security and Data Protection.

[125] Article 26, African Union Convention on Cyber Security and Data Protection.

[126] United Nations Economic Commission for Africa, 'Tackling the challenges of cyber security in Africa,' Policy Brief, Issue number NTIS/002/2014.

[127] Preamble, African Union Convention on Cyber security and Data Protection.

[128] Section 2, Kenya Cyber Security and Protection Bill

relating to information and technology.[129] This is directly modelled from the African Union Convention on Cyber security and Data Protection. The functions of the Unit shall be to- (a) receive reports of interruptions, disruptions or interference with computer systems or networks; (b) investigate the interruption, disruption or any other unlawful interference with a computer system or network; (c) advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related matters among other things.[130]

The Bill also proposes that private entities may enter into information sharing agreements with public entities or with each other. It sets certain conditions for such agreements: to ensure cyber security; for the investigation and prosecution of crimes related to cyber security; for the protection of life or property of an individual; and to protect the national security of the country. This will potentially be scandalous as it give government a backdoor to communication infrastructure and could infringe on constitutionally protected privacy [131]rights.[132] There is no provision for who determines if a particular situation amounts to what is disclosed under Section 9(2) and for how long such information sharing should subsist. Part IV of the Bill goes into detail on offences and penalties: Unlawful access to a computer system, System interference, unlawful interceptions, interception of electronic messages or money transfers, wilful misdirection of electronic messages., forgery, fraud, unauthorised modification of data, cyber terrorism, phishing, cyber bullying, child pornography among others.[133]

5.3 Canada

Canada has been traditionally described as a fire-proof house based on its advantageous geographic situation, however the globalized nature of cyberspace is eroding this conventional wisdom. The Canadian government released a cyber-security strategy in 2010. This strategy is built on three pillars: securing government systems, partnering to secure vital cyber systems outside the federal

[129] Section 3(2), Cyber Security and Protection Bill.

[130] Section 4, Cyber Security and Protection Bill.

[131] Article 31, Constitution of Kenya 2010.

[132] Section 9, Cyber Security and Protection Bill.

[133] Part IV, Cyber security and Protection Bill.

government, and helping Canadians to be secure online. The policy outlines the goals of securing Canadian cyberspace as well as a number of specific initiatives.[134]

The strategy identifies two approaches to preventing cyber-attacks. The first initiative involves reducing the number of access points to government systems, as follows: "The Government will enhance the security of its cyber architecture. It will continue to reduce the number of Internet gateways into its computer systems, and take other measures to secure systems".[135] This measure shows that the government recognises the need to centralise access points to its systems so as to isolate threats, given the unpredictability and anonymity of an attack. The second measure recognises the critical linkages between the individual and the system. Acknowledging the important role of its employees, it cites actions like changing passwords regularly and raising cyber awareness. The strategy similarly identifies two ways of managing and responding in real time to cyber-attacks. Its primary goal is to set out clear federal roles and responsibilities.

The government is also taking steps to increase intelligence capacity and threat management capability: "Communications Security Establishment Canada will enhance its capacity to detect and discover threats, provide foreign intelligence and cyber security services, and respond to cyber threats and attacks against Government networks and information technology system. The final step and set of problems that plague government response to cyber threats have to do with law enforcement. This set of issues is clearly identified in the strategy paper as a priority. The strategy aims at equipping Canada's law enforcement agencies investigative powers and tools. Providing them with new legislative authorities and supporting financial resources". [136] This prioritization reflects a clear understanding on the part of policymakers to one of the central pitfalls of government response to the cyber threats. The three aspects of response (prevention, real-time response, and law enforcement) are underwritten by a need to partner with the private sector and civil society to create a comprehensive framework of response. This underlying cooperative imperative is also reflected in the strategy. "The Government will build on existing programs and

[134] Canada's cyber security strategy: For a stronger and more prosperous Canada- Public Safety Canada, Ottawa, 2010.

[135] Platt V, 'Still the fire-proof house? An analysis of Canada's cyber security strategy' 67 *International Journal* (2012), 163.

[136] Platt V, 'Still the fire-proof house? An analysis of Canada's cyber security strategy' 67 *International Journal* (2012), 164.

expertise, such as Defense Research and Development Canada's Public Security Technical Program to better support cyber security research and development activities. We will also collaborate with our private sector and academic partners to enhance information sharing activities."

Canada's cyber security strategy prioritises prevention and security first, especially for government systems.[137] This by a far a prudent approach as opposed to reacting to attacks and situation. Having a prevention and security system cushions and anticipates attacks is something that developing countries can incorporate into their legislation. While many developing countries such as Kenya are still in the process of building their government systems it is laudable if they incorporate these and learn from past experiences in order to avoid pitfalls. The Kenya Cyber Security bill alludes to this by having a provision for critical Infrastructure.[138] It outlines what is to be considered critical infrastructure and goes ahead to state that stakeholders of critical infrastructure need to keep abreast with security measures and update the respective government agency whenever there is an intrusion and the steps they have undertaken to resolve those issues.

States need to ensure that when formulating policies they also need to equip the law enforcement agencies. This ranges from constant training on emerging threats, collecting and presenting digital evidence and financially enabling them.

Canada's strategy aims at building on existing programs and expertise, such as Defense Research and Development Canada's Public Security Technical Program to better support cyber security research and development activities. This is something most developing countries are yet to emulate. Having programs and expertise from academia, labs and the military will help greatly in anticipating risk to the cyberspace and providing adequate responses.

5.4 South Africa

The South African government has taken the lead in introducing cyber legislation to address cyber-crime. The ineffectiveness of the South African common law to combat cybercrime, led to the promulgation of the Electronic Communications and Transactions Act 25 of 2002 (ECT).

[137] Canada's cyber security strategy: For a stronger and more prosperous Canada, Public Safety Canada, Ottawa, 2010, 12.

[138] Section 6, Kenya Cyber Security and Protection Bill.

Although South Africa has signed the Council of Europe's Convention on Cyber Crime No. 185 it has not ratified the treaty.

Ineffectiveness of the South African common law to combat cybercrime, led to the. Earlier case law also illustrated the need for specific legislation to address computer crime. The case of *S v Mashiyi and Another*[139] is a case in point where the question of admissibility of computer-generated documents arose. The court held that in terms of the 'prevailing law', it could not admit the disputed documents which contained information that has been processed and generated by a computer into evidence.

The main objective of the ECT is 'to provide for the facilitation and regulation of electronic communications and transactions in the public interest'. The ECT deals comprehensively with cybercrime in Chapter 13. The following offences are punishable offences under the ECT: sections 86(4) and 86(3) introduce new forms of crimes called anti-cracking (anti-thwarting) and hacking law which prohibit the selling, designing or producing of anti-security circumventing technology; e-mail bombing and spamming are addressed in sections 86(5) and 45 of the ECT respectively; whereas the crimes of extortion, fraud and forgery are addressed in section 87.[140]

The Act has also created 'cyber-inspectors' who are authorised to enter premises to obtain information regarding cybercrime (in terms of section 82(1)). Cyber inspectors are empowered in terms of the ECT to enter any premises and access information that may impact on an investigation into cybercrime. However, this provision may infringe sections 14 and 25 of the 1996 Constitution, which deal with the right to privacy and right to property respectively.

There is a dearth of jurisprudence from South African Courts as pertains to economic crimes. In *R v Douvenga* the question was whether an accused employee, Douvenga, was guilty of a contravention of section 86(1) of the ETC. The accused intentionally and without permission, gained entry to data which she knew was contained in confidential databases and contravened the provision by sending this data by e-mail to her fiancé. The accused was found guilty of contravening section 86(1) of the ETC. She was sentenced to a fine of R1 000 or imprisonment for

[139] *S v Mashiyi* and another 2002 (2) SACR 387.

[140] Snail S, 'Cybercrime in South Africa – hacking, cracking and other unlawful online activities' *Journal of Information Law and Technology* ,2009, 6.

a period of three months. This case illustrates that the crime of hacking is entrenched in section 86(1) of the ETC. Thus any unlawful access and interception of data is regarded as a criminal offence.[141]

The case of *S v Ndiki and Others* demonstrates that the South African courts are adopting a progressive approach. In this case, the state sought to introduce certain documentary evidence consisting of computer-generated print-outs, 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 used as a tool to create the relevant documentation.[142]Therefore, these documents constituted hearsay. Exhibits D5 to D9 had been created without human intervention and such evidence constituted real evidence. Therefore, the admissibility of this evidence depended on the reliability and accuracy of the computer and its operating systems. The state bore the onus of proving such accuracy and reliability. The court's progressive approach in regarding part of the computer-based evidence as real evidence has been lauded by certain academics.[143]

South Africa has signed the CECC but not ratified it. So far, it is the only African country to have done so. The treaty contains important provisions to assist law enforcement in its fight against trans-border cybercrime. Therefore, South Africa needs to ratify the cybercrime treaty to avoid becoming an easy target for international cybercrime. Although substantive obligations are in place, South Africa needs to revise some procedural provisions to comply with the treaty such as introducing a 24/7 contact center. The establishment of the Computer Security Incident Response Team (CSIRT) indicates that a move to tackle cybercrime is gathering.[144]

The establishment of organisations such SABRIC to combat cybercrime in the banking industry is a positive move.[145] SABRIC provides the banking industry with crime risk information

[141] District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2003 (unreported case).

[142] *S v Ndiki* 2008 2 SACR 252.

[143] Cassim F, 'Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players', *University of South Africa Institutional Repository*, (2011), 127.

[144] Council for Scientific and Industrial Research, https://www.csir.co.za/news/2009 on 9 January 2017.

[145] SABRIC was established in 2002 as a wholly owned subsidiary of the Banking Association. Its key stakeholders are the four major South African banks namely, Standard Bank, Nedbank, Absa and First National Bank. For further information, see https://www.sabric.co.za on 24 January 2017.

management services and facilitates inter-bank initiatives to reduce the risk of organised bank-related crime, through effective public private partnerships. The police are collaborating with banks and the IT industry via SABRIC to combat cybercrime and bring cyber criminals to book.[146] It is submitted that the private sector has a vested interest in addressing bank-related crime. Such public-private partnerships are necessary in the fight against cybercrime.

The regional and national framework for cyberspace regulation falls short of the essential aspect of cooperation and information sharing which is necessary for enforcement of laws.

The AU convention is only workable if the signatories enact their own cyber laws and activity which is largely government led. What is likely to happen is that states will have different cyber laws locally and ultimately it will be difficult to form concerted efforts under the umbrella of the AU Convention. As such investigations and enforcement are thwarted by the fact that there is no common undertaking to share information and collaborate.

It is peculiar that there are also no common institutions with a cyber-security agenda for the continent. The Kenya Cyber security bill proposes to create a National Cyber Threat Response Unit a department within the Ministry responsible for matters relating to information and technology. [147] The fact that there are no established institutions and the judiciary has yet to be properly inducted to the working of these new technologies in order to properly adjudicate cases that may come before them.

It therefore follows that new regulations should be accompanied by capacity building for all the agencies involved. This is both financial and through training. It ensures that laws are complemented by institutions that are capable of adequate enforcement.

[146] Moodley-Isaacs N, The Saturday Star Personal Finance ‘What banks are doing 1 May 2010.

[147] Section 3(2), Kenya Cyber Security Bill 2016.

CHAPTER SIX

Conclusion and Recommendations

6.0 Conclusion

Chapter one began by introducing the challenge of regulation in the cyberspace a thereby in present the research objective which is to come with a theory for internet regulatory policy. There was literature review of the major ideas of this paper justifying the study of cyber law as an independent discipline, the cyberspace as a unique nature and code as law. This Then proceeds to the discussion on the theoretical framework in Chapter 2.

Chapter two was an analysis of the origins of government and extent of legislative power by Locke and Nozick. This was contrasted with the nature of the cyberspace which though does not have government in the political sense still has some underlying law which could be then molded in accordance with the challenges that present themselves today. This chapter concludes by stating that cyber laws should respect the architecture of the cyberspace which then can be modified accordingly. That government cannot presume to take on every foreseeable action against persons and legislative authority has its limits.

Chapter three presents the challenges to formulating effective cyber laws. This chapter also analyses the different philosophies of regulation and their merits and demerits. It sets the stage for analyzing the existing legal framework and whether they are alive to these challenges to ensure effective enforcement.

Chapter four and five discuss the approaches to be taken towards regulation of the cyberspace. This is done by discussing approaches taken by both South Africa and Canada and setting out various key things that states need to incorporate in their laws and strategies. It also affirms the need of constitution to complement laws. Constitution embodying various settled values would go a long way in ensuring effective law enforcement. These two chapters discuss the international and regional legal frameworks the shortcomings and successes and the implications they have on the development of an internet regulatory policy.

Chapter Six does a summary of all the chapters and makes recommendations on the way forward for states as they formulate strategies for cyber regulation.

6.1 Recommendations

Even with the most effective legislation one thing remains immutable- the exponential rate of evolution in the cyber domain outpaces the speed of legal and judicial processes.[148] This is further evidenced by the fact that each new defense strategy leads to co -adaptation by a corresponding set of attacks.[149]

The approach generally taken by most countries is reactionary. This is the point at which law enforcement is involved and steps are taken to contain the situation.[150] A better strategy would be taking steps to prevent attacks by; securing government systems, partnering to secure vital cyber systems outside the government, and helping citizens to be secure online. This would be by far be more effective and less costly compared to restoring systems post attack.

Governments can enhance the security of its cyber architecture by reducing the number of access points to government systems. This measure shows that the government recognizes the need to centralize access points to its systems so as to isolate threats, given the unpredictability and anonymity of an attack. [151]

International cooperation remains a cornerstone for enforcement. The first proposition is that African countries need to ratify the Budapest Convention on cybercrime as it is the only instrument geared at facilitating investigation through cooperation among countries. The ability to carry out investigations affecting the territory of other states, so-called 'investigative jurisdiction' is addressed in Chapter III of the Convention. The Convention does not expressly provide for the

[148] Ghanea-Hercock R, 'Why cyber security is hard' *Georgetown Journal of International Affairs* (2012), 85.

[149] Ghanea-Hercock R, 'Why Cyber Security is Hard' 82. The nature of Complex Adaptive Systems (CAS) is such that there is no longer an 'off-switch', as dreamed of by many political commentators. The Internet is now the world's digital nervous system, and suffers from parasitic and predator-prey activity. We are therefore in a state of co - evolution, where each new defense strategy leads to co -adaptation by a corresponding set of attack.

[150] Platt V, 'Still the fire-proof house? An analysis of Canada's cyber security strategy' 67 *International Journal* (2012), 163.

[151] Platt V, 'Still the fire-proof house?' 164. The second measure recognizes the critical linkages between the individual and the system. Acknowledging the important role of its employees, it cites s actions like changing passwords regularly and raising cyber awareness.

principle of reciprocity,[152] but does state that parties are to cooperate with each other 'to the widest extent possible' in the investigation of cybercrimes and the collection of electronic evidence.[153] This includes the sharing of information without request where it would assist another party in its investigation or which it believes might assist the receiving party in the investigation of any offence that could lead to a mutual assistance request under the Budapest Convention.

Although the Convention tacitly permits some cross-border access to stored computer data without the need to request mutual assistance, [154] such investigations are only allowed when access to the data is publicly available (open source) or when the state conducting the search has obtained "the lawful and voluntary consent of the person who has the lawful authority to disclose the data..[155]The drafters of the Convention on Cybercrime explicitly deny that the treaty permits remote exterritorial searches.

States need to ensure that when formulating policies they also need to equip the law enforcement agencies. This ranges from constant training on emerging threats, collecting and presenting digital evidence and financially enabling them.

Canada's strategy aims at building on existing programs and expertise, such as Defense Research and Development Canada's Public Security Technical Program to better support cyber security research and development activities. This is something most developing countries are yet to emulate. Having programs and expertise from academia, labs and the military will help greatly in anticipating risk to the cyberspace and providing adequate responses.

Since the cyberspace cuts across territories and covers all people in the world, it is not unreasonable to expect that there are common set values that all persons are expected upheld and protected.[156]

[152] In contrast, the United Nations Convention against Transnational Organized Crime, opened for signature 12 December 2000, 2225 UNTS 209 (entered into force 29 September 2003) art 18(1) ('UNTOC') states that parties 'shall reciprocally extend to one another similar assistance' where there are reasonable grounds to suspect that the offence is transnational in nature.

[153] Article 23, Convention on Cybercrime.

[154] Article 32, Convention on Cybercrime.

[155] Explanatory Report to the Convention on Cybercrime, supra note 3, 293- 294.

[156]Perritt HH Jr, 'The Internet at 20: Evolution of a Constitution for Cyberspace', 20 *William & Mary Bill of Rights Journal*, 4 (2012), 117.

Therefore for there to be any truly international undertaking these values need to be well established and settled. This can be compared to certain disciplines such as International Environmental law where there are generally agreed principles such as Sustainable development, generational equity, prevention and precaution. This is the same approach that regulation in the cyberspace should take. These principle are not to come from government but from a combined effort from industry, academia, governmental organization and as well as the user. As was the case with Rio, Stockholm and Nairobi conventions.[157]

Given the central role the internet's architecture has on any pursuit of regulation, there has to be consultation with the technical internet bodies who set standards that facilitate the working of the internet. The involvement of technical bodies would be particularly insightful if adequate regulation is to be affected particularly because they have experience in how it works and also because they can effect changes in the infrastructure in order to reflect the spirit of the law.

Proper internet governance can only be achieved by cooperation by all the stakeholders.[158] From private entities, users, technical bodies and government. Only with the involvement of all these agencies can there be effective la enforcement. Government alone, cannot be held responsible for formulating solutions in the cyberspace it has to be combined effort.[159]

New technologies can also be used to actualize various regulatory goals. Block chain technology which emerged during the period of financial crisis in 2008 came about at the exact moment in time when people were losing trust in a centralised system of law and order. Block chain's decentralised, open & cryptographic nature allow people to trust each other and transact peer to peer, making the need for intermediaries obsolete. This also brings unprecedented security benefits.[160] Hacking attacks that commonly impact large centralized intermediaries like banks

[157] Birnie P, Boyle A, *International Law and the Environment, Oxford University Press*, New York, 2009, 106.

[158] Reidenberg J, 'Governing networks and rule-making in the Cyberspace' *Emory Law Journal* (1996), 912.

[159]Confrence Talk with Murungi M on 22nd November 2016, at The Legal Hackers and CIPIT Fireside Chat in Strathmore Business School. Michael Murungi is Google's East Africa Policy and Government Relations Manager. Before joining Google he was the CEO of the National Council for Law reporting. He has held several talks in Strathmore Law School on Internet Governance and policy emphasizing on the importance of stakeholder participation.

[160] Nakamoto S, Bitcoin: *A Peer-to-Peer Electronic Cash System*, 1.

would be virtually impossible to pull off on the block chain. For example—if someone wanted to hack into a particular block in a block chain, a hacker would not only need to hack into that specific block, but all of the proceeding blocks going back the entire history of that block chain. And they would need to do it on every ledger in the network, which could be millions, simultaneously.[161] Such technologies and innovation are only possible when stakeholders agree to make them standards and implement them in transaction.

[161] https://medium.com/the-intrepid-review/how-does-the-blockchain-work-for-dummies-explained-simply-9f94d386e093#.2p9d00juy on 23rd December 2016.

Bibliography

Books

Aquinas T, *Summa Theologica Question 95*,

Bellia P, Berman P, Post D, Cyber law Problems of Policy and Jurisprudence in The Information Age, West Group, St Paul, 2003.

Birnie P, Boyle A, *International Law and the Environment, Oxford University Press*, New York, 2009.

Epstein R, *Simple rules for a Complex World*, Havard University Press, 1995.

International Standards, Conformity, Assessment, and U.S, Trade Policy Project Committee, *Standards Conformity Assesment, and Trade into the 21st Century*, National Academy Press, Washington D.C, 1995.

Lessig L, *Code 2.0*, 2006.

Lessig L, *Modalities of Regulation*, 1999.

Locke, *Second Treatise of Government* 1689.

Maggs P, Soma J, Sprowl J*, Computer Law Cases, Comments, Questions*, West Publishing Company, St Paul, 1992.

Mambi A, *ICT Law Handbook*, 2ed Mkuki na Nyota Publishers, Dar es Salaam, 2010.

Mill J, *On Liberty 1859,* Batoche Books (2001),

Murungi M, *Cyber Law in Kenya*, Kluwer Law International, The Hague, 2011.

National Research Council, *Rights and responsibilities of participants in networked communities,* The National Academies Press, 1994, Chapter 2 http://iimk.ac.in/gsdl/cgi-bin/library?e=d-000-00---0ecomme--00-0-0--0prompt-10---4------0-11--1-en-50---20-about---00031-001-1-0utfZz-8-00&a=d&cl=CL1&d=HASH01470e354abbaed6735e60f1.4 eBook on 27 January 2017.

Raymond K, Farber M, Cockfield A, *Cyberspace Law Cases and Materials*, Aspen law and Business New York, 2002.

Smith A, *The wealth of nations*, MetaLibri, Lausanne, 2007.

Smith Merritt, Marx L, *Does technology drive history? The dilemma of technological determinism,* Cambridge: MIT Press, 1994.

Journal Articles

Cassim F, 'Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players', *University of South Africa Institutional Repository*, (2011).

Clough J, 'A World of difference: The Budapest Convention on Cybercrime and the challenges of harmonization' 40 *Monash University Law Review* 3 (2014).

Cohen J, 'Examined Lives: Informational privacy and the subject as object', 52 *Stanford Law Review* 1373 (2000).

Ghanea-Hercock R, 'Why Cyber Security is Hard' *Georgetown Journal of International Affairs* (2012).

Ginsburg J, 'The cyberian captivity of copyright: territoriality and authors' rights in a networked world' 15 *Santa Clara Computer and High Technology Law Journal* 347 (1999).

Henry H. Perritt Jr, 'The Internet at 20: Evolution of a Constitution for Cyberspace', 20 *William & Mary Bill of Rights Journal*, 4 (2012).

Holmes Wendell, 'The Path of the Law' 10 *Harvard Law Review* (1897).

Internet Encyclopedia of Philosophy, http://www.iep.utm.edu/locke/#SH4a on 7 December 2016,

Johnson D, Post D, 'Law and Borders, The Rise of Law in Cyberspace', *Stanford Law Review* (1996), 4.

Lessig L, 'The Law of the Horse: What Cyber law Might Teach', *Havard Literature Review* (1999).

Nakamoto S, Bitcoin: *A Peer-to-Peer Electronic Cash System*.

Orji Uchenna J, ‘A discourse on the perceived defects of the draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber security’ *Communications Law*, (2012).

Platt V, ‘Still the fire-proof house? An analysis of Canada's cyber security strategy’ 67 *International Journal* (2012).

Reidenberg J, ‘Governing networks and rule-making in the Cyberspace’ *Emory Law Journal* (1996).

Reidenberg J, ‘Multimedia as a New Challenge and Opportunity in Privacy: The Examples of Sound and Image Processing’, 22 *Materialien zum Datenschutz* 9, (1995).

Snail S, ‘Cybercrime in South Africa – hacking, cracking and other unlawful online activities’ *Journal of Information Law and Technology* (2009).

Solum L, ‘The Layers Principle: Internet Architecture and the Law’ 4 *Notre Dame Law review* 1, (2004).

Weber A, ‘The Council of Europe’s Convention on Cybercrime’, 18 *Berkley Technology Law Journal* 1 (2003).

Weisner P, ‘Internet Governance, Standard Setting, and Self-Regulation’ *Northern Kentucky Law Review* (2001).

Internet Sources

Australian Cybercrime Online Reporting Network, ACORN ‘ Attacks on Computer Systems’ https://www.acorn.gov.au/learn-about-cybercrime/attacks-computer-systems on 20 January 2017.

Council for Scientific and Industrial Research, https://www.csir.co.za/news/2009 on 9 January 2017.

Cyber Libertarianism https://techliberation.com/2009/08/12/cyber-libertarianism-the-case-for-real-internet-freedom/ on 16th November 2016

International Corporation for Assigned Names and Numbers https://www.icann.org/resources/pages/what-2012-02-25-en Accessed January 9 2017.

International Engineering Task Force 'About Us' https://www.ietf.org/about/ on 9 January 2017.

International Engineering Task Force 'About us' https://www.ietf.org/about/ on 9 January 2017.

International Governance Forum http://www.intgovforum.org/cms/aboutigf accessed 9 January 2017

International Research Task Force, https://irtf.org/ accessed 9 January 2017.

Internet Engineering Task Force, 'About Us' https://www.ietf.org/ Internet Engineering Taskforce, https://www.icann.org/ Internet Corporation for Assigned Names and Numbers, http://www.itu.int/en/about/Pages/default.aspx Internet Telecommunication Union, http://www.intgovforum.org/multilingual/ Internet Governance Forum on 16 December 2016.

Internet Society, 'Brief History of the Internet' http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet on 20 January 2017.

News

Jeremy Diamond: Russian hacking and the US election; what you need to know' *CNN*, 16 December 2016 http://edition.cnn.com/2016/12/12/politics/russian-hack-donald-trump-2016-election/ on 9 January 2017.

Moodley-Isaacs N, The Saturday Star Personal Finance 'What banks are doing' 1 May 2010

Open Web Application Security Project: Cross-site Scripting https://www.owasp.org/index.php/Cross-site_Scripting_(XSS) on 17 November 2016.

Radware, 'Morris Worm' https://security.radware.com/ddos-knowledge-center/ddospedia/morris-worm/ on 20 January 2017.

Richard Epstein Simple rules for a Complex World. https://www.commentarymagazine.com/articles/simple-rules-for-a-complex-world-by-richard-a-epstein/ on 6 December 2016.

Riley Walters: Cyber Attacks on US Companies in 2016' *The Heritage Foundation*, 2 December 2016 http://www.heritage.org/research/reports/2016/12/cyber-attacks-on-us-companies-in-20169 (on 9 January 2017).

Council of Europe ‘About us’ http://www.coe.int/en/web/about-us/who-we-are on (9 January 2017)

Council of Europe ‘About us’ http://www.coe.int/en/web/about-us/who-we-are on (9 January 2017).

Reports

"Canada's cyber security strategy: For a stronger and more prosperous Canada," Public Safety Canada, Ottawa, 2010

Serianu, Kenya Cyber Security Report 2015, Nairobi

Dissertation

Tagert A, ‘Cyber Security Challenges in Developing Nations’ Published Doctoral Thesis, Carnegie Mellon University Pittsburgh, December 2010.