Harmonization of Cybercrimes Legal Frameworks within the East African Community

Majamba, H.I and Mwiburi, A, J (Editors)
Harmonization of Cybercrimes Legal Frameworks within the East African Community

Majamba, H.I. and Mwiburi, A.J. (Editors)
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TABLE OF CONTENTS</td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>x</td>
</tr>
<tr>
<td>BIO DATA OF AUTHORS</td>
<td>xi</td>
</tr>
<tr>
<td>ABBREVIATIONS AND ACRONYMS</td>
<td>xiv</td>
</tr>
<tr>
<td>CHAPTER ONE</td>
<td>1</td>
</tr>
<tr>
<td>OVERVIEW AND METHODOLOGICAL APPROACH IN HARMONIZING CYBERCRIMES LAW IN EAST AFRICA</td>
<td>1</td>
</tr>
<tr>
<td>1.1 INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.2 EAC EFFORTS IN HARMONIZATION</td>
<td>2</td>
</tr>
<tr>
<td>1.3 EFFORTS TO HARMONIZE CYBERCRIMES LAWS AT THE EAC LEVEL</td>
<td>5</td>
</tr>
<tr>
<td>1.4 RATIONALE FOR HARMONIZATION OF CYBERCRIMES LAWS IN THE EAC</td>
<td>6</td>
</tr>
<tr>
<td>1.4.1 Increased Use of Internet without Border Restrictions</td>
<td>6</td>
</tr>
<tr>
<td>1.4.2 Need for Combined Efforts in Criminalization and Investigation of Cybercrimes</td>
<td>6</td>
</tr>
<tr>
<td>1.4.3 Lack of Adequate Resources to Combat Cybercrimes</td>
<td>7</td>
</tr>
<tr>
<td>1.4.4 Technological Advancement among EAC Member States</td>
<td>7</td>
</tr>
<tr>
<td>1.4.5 Need for Regulation and Legal Framework</td>
<td>9</td>
</tr>
<tr>
<td>1.6 METHODOLOGY</td>
<td>10</td>
</tr>
<tr>
<td>CHAPTER TWO</td>
<td>13</td>
</tr>
<tr>
<td>HARMONIZATION OF THE CYBERCRIMES LEGAL FRAMEWORK IN BURUNDI</td>
<td>13</td>
</tr>
<tr>
<td>2.1 INTRODUCTION</td>
<td>13</td>
</tr>
<tr>
<td>2.2 BURUNDI IN THE EAC</td>
<td>14</td>
</tr>
<tr>
<td>2.3 OVERVIEW OF THE ICT INFRASTRUCTURE</td>
<td>15</td>
</tr>
<tr>
<td>2.4 POLICY, LEGISLATIVE AND INSTITUTIONAL FRAMEWORK FOR ICT</td>
<td>15</td>
</tr>
<tr>
<td>2.4.1 Status of Cyberlaws in Burundi</td>
<td>19</td>
</tr>
<tr>
<td>2.4.2 Regulatory Authorities/Institutions</td>
<td>20</td>
</tr>
<tr>
<td>2.5 OBSERVATIONS ON ICT THE INFRASTRUCTURE, POLICY, LEGISLATIVE AND INSTITUTIONAL FRAMEWORK</td>
<td>21</td>
</tr>
<tr>
<td>2.6 FINDINGS FROM THE FIELD</td>
<td>22</td>
</tr>
<tr>
<td>2.6.1 Challenges in Addressing Cybercrimes in Burundi</td>
<td>22</td>
</tr>
<tr>
<td>2.6.1.1 Legal Challenges</td>
<td>22</td>
</tr>
<tr>
<td>2.6.1.2 Policy Challenges</td>
<td>23</td>
</tr>
<tr>
<td>2.6.1.3 Institutional Challenges</td>
<td>23</td>
</tr>
<tr>
<td>2.6.2 Impact of Challenges on Day-to Day Work</td>
<td>24</td>
</tr>
<tr>
<td>2.6.3 Attempts to Address Challenges</td>
<td>25</td>
</tr>
<tr>
<td>2.6.4 Addressing Cybercrimes Challenges at Institutional Level</td>
<td>25</td>
</tr>
<tr>
<td>2.6.5 Internal Interventions to Address Challenges</td>
<td>27</td>
</tr>
<tr>
<td>2.7 IMPACT OF EAC STATES BY INTERVENTION PROGRAMMES</td>
<td>27</td>
</tr>
<tr>
<td>2.7.1 Impact of Measures adopted by Institutions to Address Challenges</td>
<td>28</td>
</tr>
</tbody>
</table>

iii
2.7.2 Relationship between Challenges and Attaining EAC Objectives ........................................ 28
2.7.3. Initiatives at the EAC level to address Cybercrimes ......................................................... 28
2.7.4 Reasons for Lack of Implementation of the EAC Initiative to Harmonize Laws .......................... 29
2.7.5 Suggestions on Addressing Challenges .................................................................................... 29
2.8 GENERAL SUGGESTIONS ........................................................................................................ 31
2.9 CONCLUSION .......................................................................................................................... 31

CHAPTER THREE .......................................................................................................................... 33

HARMONIZATION OF THE CYBERCRIMES LEGAL FRAMEWORK IN KENYA .......... 33

3.1 INTRODUCTION ......................................................................................................................... 33
3.2 POLICY, LEGISLATIVE AND INSTITUTIONAL FRAMEWORK FOR ICT ........................................... 33
3.3 STATUS OF CYBERLAWS IN KENYA ....................................................................................... 35
3.4 REGULATORY AUTHORITIES/INSTITUTIONS .......................................................................... 37
3.5 FIELD FINDINGS AND ANALYSIS ........................................................................................... 38
  3.5.1 Field Findings ....................................................................................................................... 38
   3.5.1.1 Office of the Director of Public Prosecutions ................................................................. 39
   3.5.1.2 Kenya Taskforce on Data Protection ............................................................................ 42
   3.5.1.3 Cyber-Security and Forensic Association ..................................................................... 46
   3.5.1.4 The Law Society of Kenya ............................................................................................ 47
3.6 ANALYZED OBSERVATION OF FIELD RESEARCH ................................................................... 49
  3.6.1 Legal Challenges ................................................................................................................. 49
  3.6.2 Policy and Statutes Challenges ............................................................................................ 52
  3.6.3 Initiatives undertaken at National Level in Addressing the Challenges .............................. 52
  3.6.4 Initiatives at the EAC Level in Addressing the Challenges ................................................ 53
3.7 CONCLUSION .......................................................................................................................... 53

CHAPTER FOUR ............................................................................................................................. 55

HARMONIZATION OF THE CYBERCRIMES LEGAL FRAMEWORK IN RWANDA .... 55

4.1 INTRODUCTION ......................................................................................................................... 55
4.2 DATA COLLECTION ................................................................................................................... 56
4.3 BACKGROUND TO INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY, LEGAL AND INSTITUTIONAL FRAMEWORK IN RWANDA ................................................................. 57
4.4 CYBER POLICY, LEGISLATIVE AND INSTITUTIONAL FRAMEWORK ........................................... 58
  4.4.1 Policy Framework ................................................................................................................ 58
  4.4.2 Legal Framework ................................................................................................................ 59
    4.4.2.1 Law Governing Information and Communication Technologies .................................. 59
    4.4.2.2 Law Regulating Media .................................................................................................. 60
    4.2.2.3 Law Establishing the National Cyber Security Authority and Determining its Mission, Organization and Functioning ......................................................... 60
    4.2.2.4 Law Establishing Rwanda Information Society Authority and Determining its Mission, Organization and Functioning ......................................................... 61
    4.2.2.5 Law Relating to Electronic Messages, Electronic Signatures and Electronic Transactions ............................................................. 61
  4.4.3 Institutional Framework ....................................................................................................... 61
    4.4.3.1 Rwanda Information Society Authority (RISA) .......................................................... 61
    4.4.3.2 The National Cyber Security Authority (NCSA) ......................................................... 62
    4.4.3.3 Rwanda Utilities Regulatory Authority (RURA) ........................................................ 63
7.1 General Conclusion .................................................. 133
7.2 Initiatives to Harmonize Cybercrimes Legislation in East Africa ........................................ 134
7.3 Areas of Convergence and Divergence on Cybercrime among the EAC Partner States .......... 135
    7.3.1 Areas of Convergence ........................................ 135
    7.3.2 Areas of Divergences ......................................... 136

CHAPTER SEVEN.................................................................. 133

OVERALL CONCLUSIONS AND RECOMMENDATIONS ..................................................... 133

6.4 Data Collection .................................................................. 98
6.5 Policy, Legal, and Institutional Framework ................................................................. 98

6.5.1 National Strategies and Plans ............................................................................. 99
  6.5.1.1 First National Development Plan (NDPII) 2010/11-2013/14 .................................. 99
  6.5.1.2 The Second National Development Plan (NDPII) 2015/16 – 2019/20 .............. 100
  6.5.1.3 ICT Sector Strategy and Investment Plan 2015/16- 2019/20 ............................... 101
  6.5.1.4 NITA-Uganda Strategic Plan 2012/13 – 2017/18 ............................................. 101
  6.5.1.5 National Information Security Strategy (NISS) .................................................. 102
  6.5.1.6 National Broadband Strategy (2016-2020) ...................................................... 102

6.5.2 ICT Policies .................................................................. 103
  6.5.2.1 National Information and Communications Technology Policy .................. 103
  6.5.2.2 National Information Security Policy (NISP) .................................................. 105
  6.5.2.3 National Broadband Policy (NBDP) ............................................................... 106

6.5.3 Legal Framework/Status of Cyberlaws ................................................................. 107
  6.5.3.1 The Computer Misuse Act, 2011 (Act No. 2 of 2011) ................................... 108
  6.5.3.2 The Electronic Transaction Act, 2011 (Act No. 8 of 2011) ............................. 108
  6.5.3.3 The Electronic Signatures Act, 2011 (Act No. 2 of 2011) .............................. 109
  6.5.3.4 The National Information Technology Authority, Uganda Act, 2009 (Act No. 4 of 2011) .................................................. 110
  6.5.3.5 The Regulation of Interception of Communications Act, 2010 (Act No. 18 of 2010) .................................................. 110
  6.5.3.6 The Uganda Communications Act, 2013 (Act No. 1 of 2013) ................... 111
  6.5.3.7 The Anti-Pornography Act, 2014 (Act No. 1 of 2014) .................................. 112
  6.5.3.8 The Data Protection and Privacy Act, 2019 .................................................. 113

6.5.4 Institutional Framework ............................................................................... 114
  6.5.4.1 Ministry of Information, Communications Technology and National Guidance (MoICT& NG) .................................................. 115
  6.5.4.2 National Information Technology Authority, Uganda (NITA-U) .................... 119
  6.5.4.3 National Computer Emergency Response Team Uganda/ Coordination Center (CERT.UG/CC) .................................................. 125

6.6 Challenges .......................................................................... 128
  6.6.1 Inadequate Computers and other Digital Equipment .......................................... 128
  6.6.2 Limited Public and Institutional Awareness ......................................................... 129

6.7 Conclusion ........................................................................... 131

6.8 Recommendations .................................................................. 131
  6.8.1 Addressing the Existing Legal Gaps ................................................................. 132
  6.8.2 Capacity and Resource Building .................................................................... 132
  6.8.3 Strengthening Law Enforcement Institutions .................................................. 132

CHAPTER SEVEN.................................................................. 133

OVERALL CONCLUSIONS AND RECOMMENDATIONS ..................................................... 133
7.4 Challenges Facing the EAC in Harmonizing Cybercrimes Laws

7.4.1 Civil and Common Law Systems in the EAC

7.4.2 Lack of Resources and Capacity for Technological Advancements

7.4.3. Slow Progress in Passing Laws and Implementation

7.4.4 Lack of Political Commitment

7.4.5 Territoriality

7.4.6 Budgetary Constraints and Balancing of Interests

7.4.7 Underdeveloped ICT Infrastructures

7.4.8 Lack of Basic Legal Regimes in Individual Partner States

7.4.9 Absence of a Body Mandated to Harmonize Cyberlaws in East Africa

7.4.10 Cybercrime and Restraint of Human Rights

7.4.11 Addressing the Challenges

7.4.12 Continuous Training of EAC Officials from Judiciary to EALA

7.4.13 Enactment of Soft Law on Harmonization of Cybercrime

7.4.14 Soliciting for Partnerships and Working Relationships with other Jurisdictions

7.4.15 Use of National and Regional Courts of Law

7.4.16 Ratifying Regional and International Instruments

7.4.17 Cooperation with International Bodies

7.4.18 ICT and Cyber-Security Education

7.4.19 Engagement of Key Stakeholders

BIBLIOGRAPHY
The development of a harmonized legislative framework in as far as regional integration is concerned is fundamental in order to maximize the benefits and potential of generating economic development gains for Members States. The study that led to this publication was prompted by, among others issues, the fact that despite initiatives and directives of the relevant organs of the East Africa Community (EAC), Member States have continued to experience challenges in harmonizing their legislative frameworks in order to combat cybercrimes in their jurisdictions.

The study focused on select countries in the EAC: Tanzania, Uganda, Kenya, Burundi and Rwanda. The bias in this selection was primarily based on logistical issues and the fact that the select States have diverse legal histories and legal frameworks. The other factor was the availability of research assistants who were capable and easily identifiable due to logistical challenges and difficulties in accessing literature, policies, laws and other documents in the other jurisdictions. The study probed on the extent to which these States have harmonized their legal, policy and institutional frameworks on cybercrimes as required by the Treaty Establishing the EAC. Factors that have made it difficult for the States to harmonize their legislative framework in line with the EAC call were also analyzed.

Literature review, analysis of legislation and policies and documents related to the theme of the study of the targeted EAC States was undertaken. Data was collected through fieldwork where the research assistants conducted interviews with personnel in charge with implementation of cyber-related policies and laws in the select States. The study findings reveal that States are at different levels in terms of harmonizing the cybercrime related laws to reflect the EAC directive. It has also been observed that although some States have made concerted efforts in this regard, different challenges still abound. Common ones relate to lack of funds and existence of a multitude of
uncoordinated institutions dealing with cybercrimes. Conflicting and duplication of mandates and lack of clear understanding by personnel charged with enforcement of cybercrimes in the select States have also been noted.

Efforts being made to address the challenges are admittedly laudable, but this must be backed up with political will by governments.
ACKNOWLEDGEMENTS

Members of the research Team would like to extend their gratitude to all who have in one way or another made the completion of this publication a reality. We certainly cannot mention all of them here. However, we would like to thank the University of Dar-es-Salaam for the initiative of coming up with the Research Project and allocating funds for the study. This was made possible through the Office of the Deputy Vice Chancellor, Research.

Ms. Cecilia Ngaiza very ably organized the process of identifying the research assistants and oversaw all logistical and administrative arrangements in ensuring the research assistants delivered their output within strict deadlines. She also summarized the raw field reports and therefore enabled researchers to easily compile draft reports. We are extremely grateful to the research assistants in the select EAC States for your commitment and industry in collecting data from the field: Nzabonimana, Symphorien Jean Jacques (Rwanda, Kigali) Alphonce Omondi Owucha, (Nairobi, Kenya), Ntahompagaze Arnaud, (Bujumbura, Burundi) and Violla Nabawanda, (Kampala, Uganda) - we thank you all so much!

Ms. Sophia Mwawengo and Aloyce Suleiman played critical roles of ensuring the financial aspects of the study were in compliance with relevant regulations and guidelines. Ms. Mariam Akukweti, the Office Management Secretary at the School of Law provided the much-needed secretarial assistance. Staff of the School of Law also played a critical role in supporting the team members prior to and in the course undertaking the study.

We would also like to thank all the respondents who agreed to provide critical and very useful information and insights that have greatly benefited the study and ultimately this publication.
BIO DATA OF AUTHORS

Abel Juma Mwiburi is a Lecturer at the Department of Private Law of the University of Dar es Salaam School of Law. He joined the University in 2009 after his stint as a Tax Consultant with PricewaterhouseCoopers. He holds a Bachelor of Laws degree (LL.B. 2008) and Master of Laws degree (LL.M. 2011) from the University of Dar es Salaam; Postgraduate Diploma in Legal Practice (2013), Law School of Tanzania; and Doctor of Laws (LL.D. 2018), University of Bayreuth, Germany. Dr. Mwiburi’s areas of specialization include Cyberlaw, Family Law, Jurisprudence, Law of Business Associations, Tax Law and Law of Negotiable Instruments. Dr. Mwiburi is also a consultant in ICT/Cyberlaws and Corporate Law. He is a member of Tanganyika Law Society and the East African Law Society, Bar Associations for Tanzania Mainland and East African countries, respectively.

Baraka Francisco Kanyabuhinya is a Lecturer at the School of Law in the Department of Private Law. He is a holder of a Bachelor of Laws degree, LL.B. (Hons.) Upper Second-Class (2003); Master of Laws (LL.M.) in Intellectual Property, Commerce and Technology, the University of New Hampshire (then called Franklin Pierce Law Centre-USA) (2005); and Doctor of Philosophy (Economic Law), University of Dar es Salaam (2014). Dr. Kanyabuhinya specializes in Competition Law, Intellectual Property, Consumer Protection, Commercial transactions and Entities, Technology, Data Protection, EAC Law, International Trade and Family Law. His other areas of interests include Land Law, Alternative Disputes Resolution (ADR), Labour Relations and WTO Law.

Boniphace Luhende is a Lecturer and Head of the Department of Public Law. Dr. Luhende joined the School in 2009. He had previously worked with PricewaterhouseCoopers as Tax Consultant. Dr. Luhende holds a Bachelor of Laws Degree (LL.B. 2008), Master of Laws degree (LL.M. 2011), University of Dar es Salaam; Postgraduate Diploma in
Legal Practice (2013), Law School of Tanzania; and Doctor of Philosophy degree (Ph.D. 2017), University of Cape Town. Dr. Luhende specializes in Mining Law, Oil and Gas Law, Tax Law, Law of Contract, and Corporate Law. Currently, Dr. Luhende coordinates the Taught LL.M. Program in Oil and Gas Law. He is also a member of Tanganyika Law Society, the Bar Association for Tanzania Mainland.

**Hamudi Ismail Majamba** is an Associate Professor of Law and Dean of the University of Dar es Salaam School of Law. A member of the Department of Private Law, he holds an LL.B. from the University of Dar-es-Salaam; an LL.M. from Queen's University, Canada; and a Ph.D. from Northeastern University, USA. He is an Advocate of the High Court of Tanzania. Prof. Majamba has been a member of the Panel on Gas and Oil (an Advisory Organ to the Government of the United Republic of Tanzania on the Natural Resources Charter) and has been engaged as a Consultant by the Government (and NGOs) to draft legislation and provide advice on legislative enactments with a bearing on the natural resources sector. He has also served as a member in the Government of Tanzania’s Negotiation Team (GNT) on Oil and Gas Contracts. He specializes in Environmental and Natural Resources Management Laws.

**Laurean Laurent Mussa** is a Lecturer in the Department of Private Law. He joined the University in 2008. Dr. Mussa holds a Bachelor of Laws degree (LL.B. 2007), Master of Laws degree (LL.M. 2009) and Doctor of Philosophy in Law (Ph.D. 2016) from the University of Dar es Salaam. He is an Advocate of the High Court of Tanzania and a member of Tanganyika Law Society and East Africa Law Society, Bar Associations for Tanzania Mainland and East African countries, respectively. Dr. Mussa is also a member of the World Commission on Environmental Law since 2016. His areas of specialty include Land Law and Environmental Law.

**Theodora Mwenegohha** is a Lecturer at the Department of Private Law. She holds a Bachelor of Laws degree (2003), a Master of Laws
degree (2005) from University of Dar es Salaam and a Doctor of Philosophy (2015) from Bond University, Australia. Dr. Mwenegoha specializes in cyber laws, commercial laws, intellectual property laws, competition and consumer protection laws and research. Dr. Mwenegoha is an Advocate of the High Court of Tanzania. She has served on boards of charitable and civil society organizations and was a member of Bond University Research Ethics Committee. Dr. Mwenegoha has served as the Vice Chairperson of the Institute of Judicial Administration Council. She is also a member University of Dar es Salaam College of Social Sciences Board and the Fair Competition Tribunal (FCT).
<table>
<thead>
<tr>
<th>ABBREVIATIONS AND ACRONYMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>APA</td>
</tr>
<tr>
<td>ARCT</td>
</tr>
<tr>
<td>CAK</td>
</tr>
<tr>
<td>CERT.UG/CC</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>CERTS</td>
</tr>
<tr>
<td>CI</td>
</tr>
<tr>
<td>CII</td>
</tr>
<tr>
<td>CIP</td>
</tr>
<tr>
<td>CIRC</td>
</tr>
<tr>
<td>CMA</td>
</tr>
<tr>
<td>CNC</td>
</tr>
<tr>
<td>CSIRT</td>
</tr>
<tr>
<td>DNS</td>
</tr>
<tr>
<td>EAC</td>
</tr>
<tr>
<td>EACO</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>ETA</td>
</tr>
<tr>
<td>FIRST</td>
</tr>
<tr>
<td>GDPR</td>
</tr>
<tr>
<td>GITS</td>
</tr>
<tr>
<td>ICANN</td>
</tr>
<tr>
<td>Acronym</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>ICTA</td>
</tr>
<tr>
<td>ICTs</td>
</tr>
<tr>
<td>INTERPOL</td>
</tr>
<tr>
<td>IT</td>
</tr>
<tr>
<td>ITU</td>
</tr>
<tr>
<td>KENIC</td>
</tr>
<tr>
<td>LSK</td>
</tr>
<tr>
<td>LTE</td>
</tr>
<tr>
<td>MINICT</td>
</tr>
<tr>
<td>MoICT&amp; NG</td>
</tr>
<tr>
<td>MPs</td>
</tr>
<tr>
<td>NBDP</td>
</tr>
<tr>
<td>NBI</td>
</tr>
<tr>
<td>NBS</td>
</tr>
<tr>
<td>NCIP</td>
</tr>
<tr>
<td>NCSA</td>
</tr>
<tr>
<td>NDPI</td>
</tr>
<tr>
<td>NDPII</td>
</tr>
<tr>
<td>NICI</td>
</tr>
<tr>
<td>NICTP</td>
</tr>
<tr>
<td>NISP</td>
</tr>
<tr>
<td>NISR</td>
</tr>
<tr>
<td>NISS</td>
</tr>
<tr>
<td>Acronym</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>NITA-U</td>
</tr>
<tr>
<td>No.</td>
</tr>
<tr>
<td>NPPB</td>
</tr>
<tr>
<td>NRD</td>
</tr>
<tr>
<td>P.</td>
</tr>
<tr>
<td>PP.</td>
</tr>
<tr>
<td>RANU</td>
</tr>
<tr>
<td>RDB</td>
</tr>
<tr>
<td>RIB</td>
</tr>
<tr>
<td>RICA</td>
</tr>
<tr>
<td>RISA</td>
</tr>
<tr>
<td>RLRC</td>
</tr>
<tr>
<td>RPF</td>
</tr>
<tr>
<td>RURA</td>
</tr>
<tr>
<td>TCRA</td>
</tr>
<tr>
<td>TGCL</td>
</tr>
<tr>
<td>UBC</td>
</tr>
<tr>
<td>UCA</td>
</tr>
<tr>
<td>UCC</td>
</tr>
<tr>
<td>UICT</td>
</tr>
<tr>
<td>UMC</td>
</tr>
<tr>
<td>UNCTAD</td>
</tr>
<tr>
<td>Acronym</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>UNESCO</td>
</tr>
<tr>
<td>WSIS</td>
</tr>
</tbody>
</table>
CHAPTER ONE

OVERVIEW AND METHODOLOGICAL APPROACH IN HARMONIZING CYBERCRIMES LAW IN EAST AFRICA

Abel Juma Mwiburi and Hamudi Ismail Majamba

1.1 Introduction

As result of technological advancement, cyber-security concerns are not only a concern of one nation, but a cross border issue with several complex dimensions. Consequently, addressing and enhancing cyber-security and protection has become not only a matter of national concern but also international involvement. Cyber security concerns have indeed become a new international political agenda and have played a major role in global politics. It is in this regard that, enhancing cyber-security and ensuring that a nation and its citizens are safe while operating both on the online and while offline world have become a new service that every government needs to offer to its people.

As cyber challenges have international dimension, limiting efforts in combating such challenges only at the national level is not effective. Cyber criminals tend to operate from countries with weak regulations in attacking even strong cyber regulated ones. It has also been noted that efforts to curb this vice has not been effective. For example, the offline mutual legal assistance agreements that have been entered by some States have not been successful due to the speed of

---

3 Marco, G. (Ed), op.cit p. 2.
4 Ibid.
developments in online platforms that require innovative measures to reflect its complexity.\footnote{Ibid., 78.}

Consequently, there is a need for global and regional harmonisation of legal efforts addressing cyber-issues, especially in cybercrimes and cyber-security. To ensure the strengthening of the regional integration and addressing the welfare of its citizens, the East African Community (EAC) needs to address cyber-security concerns at the national level and address harmonisation of cyberlaws so as to address the international aspect of these challenges.

\subsection*{1.2 EAC Efforts in Harmonization}

Efforts in harmonizing cyberlaws among the EAC States began in 2006 with support from the United Nations Conference on Trade and Development (UNCTAD). A special Task Force was formed and charged with the task of conducting a comprehensive research, review examine the reality and challenges facing the Member States. It was required to come up with measures that will not only address problems common to all but that would also address challenges brought due to the differences in their legal systems. Among the major finding of this Task Force in relation to cyberlaw legislation in EAC was that the laws in the States forming the EAC are ‘not harmonized and provide divergences in national approaches to cybercrime acts.’\footnote{See UNCTAD (2013), Harmonizing Cyber Laws and Regulations: The Experience of the East African Community, United Nations, New York, p. 6, available at: https://unctad.org/en/PublicationsLibrary/dtistict2012d4_en.pdf.}

In an attempt to address this challenge the Task Force developed and proposed the implementation of the EAC Draft Framework in Cyber Law. The first phase of the implementation of the Framework covered electronic transactions, electronic signatures and authentication, cybercrime, data protection and privacy. The second phase addressed
issues relating to intellectual property, e-taxation and information security.\textsuperscript{7}

Since the EAC has become a global village through advancement of technology and its Member States share the same challenges that very same technology advancement brings, it is critical to address the challenges jointly. This requires the EAC Member States to put in place legal mechanisms that will not only address the challenges arising in an individual States, but also address issues which may occur in other Member States. This requires harmonization of the cyber-legal frameworks. In achieving this harmonization, the EAC has taken the initiative to develop legal, policy and institutional frameworks as well as strategic plans to promote the development and implementation of information technology in the region.

It is critical to point out here that the Task Force recommended that the harmonization process of cyberlaws within the region coordinated at regional level and benchmarked against international best practices. It also recommended that a comparative review of the already existing laws and pending Bills in Partner States be undertaken as a basis for the development of a harmonized regional cyber-legal framework.\textsuperscript{8}

It is also notable that in 2013, the EAC organized the first Cyber Defence East Africa Conference together with the Norway Registers Development AS (NRD)\textsuperscript{9} and ISACA Tanzania Chapter.\textsuperscript{10} IT specialists attended the Conference from Uganda, Kenya and Tanzania. One of

\textsuperscript{7}Ibid.
\textsuperscript{9} Norway Registers Development AS (NRD) is a cybersecurity technology consulting, incident response and applied research company established in 1995, with its headquarters situated in Norway. It specializes in governance and economic digital infrastructure development. Its mission is to create a secure digital environment for states, governments, corporations and citizens in Central and Eastern Europe, Sub-Saharan Africa, South Asia and other regions. p. 17, available at: http://www.cybersecurity.ug/about/cdea/2018/, accessed on 14\textsuperscript{th} April, 2019.
\textsuperscript{10} The Conference that took place on the 28\textsuperscript{th} – 30\textsuperscript{th} of August in Morogoro.
the major objectives of the Conference was to assist organizations in the EAC region to create a secure digital environment through speeding up information security and create a community of IT security professionals who are ready to protect their networks and handle security incidents. The aim to ensure a conducive secure IT environment is mandatory in this instance so as to maintain the region’s development.\textsuperscript{11}

The harmonization of cyberlaws within the Community is an ongoing process in the region. In its approach, the EAC Task Force initiated the harmonization process to be in two phases. The First Phase comprised of Electronic Transactions, Electronic Signatures and Authentications, Data Protection and Privacy, Consumer Protection and Computer Crime. The Second Phase entailed taking on Intellectual Property Rights, Domain Names, Taxation and Freedom of Information. It was estimated that these should be in force by 2010. However, it has taken a slow pace in terms of legislation and implementation.\textsuperscript{12}

Other commendable efforts aimed at addressing cyber challenges among the EAC States have been taken. These include the adoption of the EAC Regional e-Government Programme in 2006, which aimed at improving and enhancing public service delivery through the use of Information and Communication Technologies (ICTs) in public administration and the adoption of the EAC Draft Legal Framework for Cyber Laws. At country level, Member States are at different stages in responding to cyber challenges and adopting EAC efforts of harmonizing cyberlaws and developing measures to address challenges.


1.3 Efforts to Harmonize Cybercrimes Laws at the EAC Level

There are various initiatives taken by EAC’s Partner States to harmonize their cyberlaws legislation. Recognizing the need for an enabling environment, in 2006, the EAC Council of Ministers approved that the EAC Framework for Cyberlaws be developed. The well-documented initiative is titled Draft EAC legal Framework for Cyberlaws (“Framework”) was prepared by the EAC Task Force on Cyberlaws. The Task Force comprises of representatives from the Partner States and the EAC Secretariat, with the support of UNCTAD.

The Framework contains a series of recommendations made to the governments of the Partner States about reforming national laws to facilitate electronic commerce; to facilitate the use of data security mechanisms; to deter conduct designed to undermine the confidentiality, integrity and availability of information and communication technologies; to protect consumers in an online environment, and to protect individual privacy. The recommendations are designed to harmonize the law reform process between the EAC Partner States, as well as reflecting international best practice.

---

16 Ibid.
17 Ibid.
1.4 Rationale for Harmonization of Cybercrimes Laws in the EAC

As noted above, cybercrimes are international crimes that affect various countries. This, therefore, makes harmonization of national laws in the region relevant in combating cybercrimes. In this regard, enhanced international and inter-regional co-operation against cybercrimes should be prioritized. The rationale for harmonization of cybercrimes laws include the following as discussed below:

1.4.1 Increased Use of Internet without Border Restrictions

The boundless possibilities of using information technologies facilitate committing criminal activity without any border restrictions or detection. This is because a cyberspace is a digital environment enabling the creation, process and exchange of information; formed by information systems, electronic communication on services and networks. Since cybercrimes are undetected and operated in a cyberspace, this may lead to cyber-criminals to commit crimes in other jurisdictions while in fact they are in another jurisdiction. Curbing crimes that are cross-border in nature may prove extremely difficult and often most go undetected. This, therefore, calls for EAC Partner States to harmonize their laws in order to combat cybercrimes to ensure detection and cooperation when investigating and prosecuting the cybercrimes.

1.4.2 Need for Combined Efforts in Criminalization and Investigation of Cybercrimes

Criminalization differences introduce challenges for effective inter-regional cooperation in criminal matters involving cybercrime in

particular, as regards the principle of dual criminality.\textsuperscript{19} While Uganda, Kenya and Tanzania provide for criminalization of cybercrimes, the sentences vary from country to country. Moreover the Law Nº 60/2018 of 22/8/2018 on Prevention and Punishment of Cyber Crimes of Rwanda does not state the specific punishment for commission of the cybercrimes. There are criminalization gaps in some countries such as South Sudan, which does not have any law on cybercrimes. These divergences are likely to cause havens for cybercriminals to affect the EAC. This, therefore, calls for concerted efforts for harmonization of cybercrimes in East Africa.

\textbf{1.4.3 Lack of Adequate Resources to Combat Cybercrimes}

It may be extremely difficult for a single country to combat cybercrimes. Cyber-criminals usually get away with cybercrimes because they are relatively new, and many law enforcement authorities are unskilled in dealing with cybercrimes. The investigations are usually very sophisticated and require a lot of resources and expertise, which many countries may not have, leading to a continuous cycle of cybercrimes. While on the one hand the victims of the cybercrimes are more hesitant to report such crimes, the criminals on the other hand become more confident because of a lack of cooperation between the victims and the authorities and global cooperation. Therefore, a concerted effort through harmonization is a better way to combat cybercrimes.

\textbf{1.4.4 Technological Advancement among EAC Member States}

Over the years there has been increased online investment, e-trade and e-services by the EAC citizens and non-EAC Members. This includes services such as e-transactions, online banking, e-investment, e-migration services among others. The nature of this online business

\textsuperscript{19}Ibid., p. 77.
is that it may easily be manipulated by cyber-criminals. This, therefore, calls for countries to harmonize laws to combat cybercrimes. Digital technology used for governments’ e-services also has also raised the rates of threats to national security, economies of countries and business entities in the EAC. Cyber-security, therefore, requires the protection of “computers, networks, software, data and other related digital technologies” from cybercrimes. This includes adopting an appropriate and harmonized legal and policy framework to curb cybercrimes in the EAC.

Individual EAC Member States have various ICT systems that are vulnerable to cyber-attacks, which include mobile money transfers such as *Mpesa*. Over the years the EAC countries have embraced several technological advancements for instance ICT systems developed to facilitate e-trade and the Customs Union all of which are prone to cyber-attacks. These include use of electronic filing of customs documents, which has improved speed and transparency. The United Republic of Tanzania and the Republic of Kenya have established the Single Window System; Rwanda and Uganda are still using (Automated Systems for Customs Data) ASYCUDA World while Burundi is still using ASYCUDA++.” This calls for concerted efforts for protection of new technologies, e-services, e-investments and online businesses through harmonization of laws, policies and practices.

---


22In Tanzania the Single Window System Replaced the ASYCUDA++, See Chimilila, C., et al., p. 4.

23Ibid., pp. 4 and 5.
1.4.5 Need for Regulation and Legal Framework

In order to have functional e-government services and strategies, there is a need to have harmonized legislation as a step to implementation of the e-government strategies. The Regional E-Government Framework Stakeholders’ meeting held in Nairobi 2005, identified cyberlaws and e-justice as a priority for curbing cybercrimes. The subsequent workshops on cybercrimes and e-justice and information security held in Kampala in 2016, provided recommendations for harmonization and involved a plan for the same based on national and regional legal frameworks on cyberlaws.  

1.5 Scope of Study

This study that led to this publication sought to address concerns from a number of stakeholders that a number of challenges were still being experienced in the process of harmonizing cybercrimes law in EAC States despite initiatives and directives of the relevant organs of the EAC. The study undertook an analysis of select EAC States focusing on the cyber related policy, legislative and institutional frameworks and specified law enforcement organ(s) in each of the identified States. It has probed into factors that have made it difficult to meet for the States set targets and makes recommendations. It is envisaged that the recommendations of the study will provide input into the efforts being made by the EAC Partner States to ensure obligations of the States in implementing the EAC directive related to harmonizing cyber laws are met.

The research Team comprised of members of the academic staff of the University of Dar-es-Salaam School of Law: Prof. Majamba (Principal Investigator), Dr. Mwenegoha, Dr. Luhende, Dr. Mussa, Dr. Kanyabuhinya, Dr. Mwiburi (Co-Principal Investigators). Research assistants comprising of Alumni of the School stationed in the select EAC States provided the necessary support.

---

24 UNCTAD, (2013), supra p. 5.
This publication is divided into six Chapters. Chapter One sets out the overall introduction, providing for the background to the study, the methodology employed in undertaking it and overall literature and documentary review. Chapter Six provides for the study’s overall conclusions and recommendations, the specific conclusions and recommendations having been addressed in each specific Chapter: that is Chapters Two to Five. Each case study of the EAC Member States that have been the focus of the study has been assigned a chapter comprising of a total of the four remaining chapters.

1.6 Methodology

The main methods that were applied in the course of undertaking the study leading to this publication were literature and documentary review and field work.

1.6.1 Literature Review

The study was preceded by review of literature comprising of articles, reports and studies that cover the subject of cybercrime in general and those that focus on the EAC in particular. Literature providing for the history of the States that have been selected from the EAC as a case study in the context of regional integration was perused to set the foundation of each particular State’s perspective.

Reports providing for the data and documentation of the ICT infrastructure that have been put in place, the regulatory agencies and the enabling institutional framework of each of the States were critically reviewed in each chapter outlining the state of affairs in each of the selected EAC Partner states.

The reviews were undertaken with a view to ensuring there is detailed coverage of the institutional, policy and legislative framework that the governments of the targeted States have put in place to regulate cybercrimes in their respective jurisdictions. Successes and challenges that the respective States have made or grappled with in their efforts
to harmonize their cybercrime related legislation in line with the EAC framework were critically discussed.

Finally, gaps in the literature and documents reviewed were identified and these formed part of the agenda for collecting field data in the respective jurisdictions.

Websites also provided important information and data on the state of affairs and developments on institutions charged with regulating cybercrimes in general, and harmonization of cybercrimes laws in the identified EAC Member States, in particular. Meetings among the investigators were conducted to chart out the direction of the research Project throughout the study. This enabled all researchers to have and maintain a common understanding in the course of undertaking the study.

1.6.2 Field Work

Research assistants were engaged to conduct fieldwork in the select EAC States. These were drawn from a database of LL.M. alumni of the University of Dar-es-Salaam School of Law maintained by School. The assistants are former Tanzania-Germany Center for Postgraduate Studies in Law (TGCL) students who are stationed in countries in which they were contracted to collect data from: Kenya, Uganda, Rwanda and Burundi. The Principal Investigator prepared terms of reference to enable research assistants earmarked and contracted to collect information from identified stakeholders in Uganda, Rwanda and Burundi (see Annexure B). This was after updating the research assistants on the background and objectives of the study. Interview guides were also prepared to assist them to collect the data (see Annexure A) for the sample of the Interview Guide).

The research assistants also made observations in the institutions they visited to collect data. No fieldwork was conducted in Tanzania due to constraints of time and logistics, as the dates for submission of the final report were brought forward in a relatively short period of time
to permit meaningful data collection. The literature and documentary review for identifying data and information from Tanzania was reinforced as a result of this unexpected event.
CHAPTER TWO

HARMONIZATION OF THE CYBERCRIMES LEGAL FRAMEWORK IN BURUNDI

Hamudi Ismail Majamba

2.1 Introduction

Burundi is one of the smallest countries in Africa. It had a population of 11 million in 2016. It is a landlocked country, being bordered by Rwanda to the North, the Democratic Republic of Congo to the West and Tanzania, to the East and South. Burundi covers an area of approximately 28,000 square kilometers and is one of the most densely populated countries in the world, with an average of nearly 250 people per square kilometer. Burundi’s economy is predominately agriculture based with the main exports being coffee and tea which account for a huge share of its foreign exchange earnings.25

Burundi has a checkered history. Prior to colonial rule, it was initially organized as a Kingdom comprising of three main tribes – the Batwa, Hutus and Tutsis. It was colonized by the Germans at the beginning of the 20th century and later placed under the mandate of Belgium by the League of Nations after the defeat of Germany in the First World War. Upon attaining independence in 1962, the government adopted a constitutional monarchy but in 1966 it turned into a Republic with a one Party State before plunging into serious tribal tensions. This set the path for a series of inter-ethnic conflicts in 1972, 1988, and 1992 which led to a large scale massacre of its people. In 1993, elections were held giving rise to the present State structure consisting of an Executive, Judiciary and a National Assembly. Despite the elections, there has been continued political unrest in the country. Attempts by

regional leaders to reconcile parties through a negotiation process have encountered all sorts of challenges promoting calls for intervention by the EAC.\textsuperscript{26}

Burundi’s National Assembly makes law but the President is also vested with power to make Decrees after consulting the Constitutional Court. The judicial system of this country comprises of civil law, following the influence of Belgium although rudiments of customary law are still found. In terms of sources of law, the fundamental law of Burundi is the Constitution of 2005. It empowers the National Assembly to enact organic laws as well as statutory laws. The Constitutional Court and other judicial organs also make decisions which guide in interpreting the law. International legal agreements also form part of the sources of law in Burundi.\textsuperscript{27}

\subsection*{2.2 Burundi in the EAC}

Burundi is one of the Member States of the EAC, having joined it in 2007. Developments to improve the use of ICT in the EAC region have been made possible with the installation of under the sea Fiber Optic Cable Network (SEACOM) in the region. This has admittedly led to increased use and in some cases abuse of the ICT systems and information insecurity in the region in general, and in Burundi in particular. Attempts to address some of the insecurity challenges have also been made in the region, with emphasis on the need to harmonize legislative and policy initiatives. Being a Member of the EAC, Burundi is also bound by Article 216(2)(b) of the Treaty establishing the EAC which requires Party States to take measures to align their legislative


\textsuperscript{27} Bizimana, S.,(2017), The Burundi Legal System and Research, available at: http://www.nyulawglobal.org/globalex/Burundi.html#_3._Legal_system, accessed on 20\textsuperscript{th} November 2019.
and policy frameworks with a view to harmonizing them. This is re-
echoed by Article 47 of the Common Market Protocol.

2.3 Overview of the ICT Infrastructure

Burundi is connected to undersea Fiber Optic Cables that run along the East African coast. The Burundi Backbone System is run under a public-private partnership comprising Burundian telecom companies and the government, with support from the World Bank. The Government has also encouraged other private businesses to invest in the ICT sector offering a range of services and has put in place a National ICT Policy Plan for 2010-2025. This Policy seeks to address the challenges in the country’s ICT framework.28

Some of the notable challenges that the government of Burundi has faced in terms of ICT range from lack of a comprehensive policy and legislative framework and inadequacy of local expertise on cyber-security. As a result of this, the confidence of businesses engaged in electronic related transactions is eroded. These challenges coupled with political instability makes the country vulnerable to attacks by criminals.29 In some cases, the Government has been charged with using undemocratic means to address some of the challenges in the course of regulating the sector to ensure security.30

2.4 Policy, Legislative and Institutional Framework for ICT

A Report of the United Nations Conference on Trade and Development (UNCTAD (2013), provides an important backdrop on the development

28 See: Kalemera, A., et al., op.cit. pp. 3-5
30 Kalemera, A., et al., op.cit. p. 5
of the policy and legislative framework and related ICT infrastructure in Burundi.\textsuperscript{31}

As noted above, the Government of Burundi has in place a National ICT Development Plan for the period 2011-2015. This Plan was preceded by the government’s effort to comply with its commitment to the 2005 World Summit on Information Society (WSIS). In 2006, the Government put in place a Strategy to cover the period between 2006 and 2010. The National ICT Development Plan is articulated through ten pillars. One of these Pillars is related to ensuring an appropriate legal and regulatory environment.

The UNCTAD Report notes that the government’s effort in facilitating the development of a dynamic information society led to the establishment of the Communications Infrastructure Project (CIP), which falls under the National Policy on ICTs and the National Information and Communication Infrastructure Plan (NICI). Accordingly, the efforts of the CIP are concentrated on identifying those elements that result in a reduction in the cost of connectivity; an extension of national coverage in telecommunication networks and the sustainability of national and international broadband infrastructure. The UNCTAD Report also noted that the legal and regulatory framework in existence then did not provide a secure environment for the creation of a climate of confidence without which e-commerce would take off.

This challenge led to the Government drafting a single legislative instrument (‘draft Bill’) to create a framework within which the information society could evolve and grow. The reforms targeted were to be in line with the ICT National Policy and the National Strategic Plan on ICT. In 2013, the framework focused mainly on telecommunications infrastructure development and services. Since 1997, when the telecommunications law was enacted, the Burundi

\textsuperscript{31} UNCTAD (2013), Harmonizing Cyber Laws and Regulations: The Experience of the East African Community, United Nations.
telecommunications sector had noted significant development rendered possible by its liberalization. However, the level of growth did not compare well with other EAC Partner States partly due to lower purchasing power. It may have also reflected the fact that the framework did not fully reflect international best practice in terms of openness and transparency, predictability, neutrality and objectivity, which may have had a negative impact on foreign investment in the sector during that time.

The UCTAD Report provides some guidance on the laws governing ICT in Burundi. It is accordingly noted that in 2013, the non-telecommunications legal framework comprised of the following pieces of primary legislation, some of which addressed cyberlaw concerns:

- Central Bank Act n°1/34 of December 2008;
- Competition Act n°1/06 of March 2010;
- Customs Code Act n°1/02 of January 2007;
- Industrial Property Act n°1/13 of July 2009;
- Penal Code Act n°1/95 of 22 April 2009;
- Press Act n°025/01 of November 2003;
- Private and Public Companies Act n°1/09 of May 2011;
- Protection of Right of Author and its related Act n°1/06 of December 2005;
- Trade Code Act n°1/07 of April 2010; and
- Value Added Taxation Act n°1/02 of February 2009.

These laws constituted the backbone of commercial activities in general, but without emphasis on e-commerce and it is noted that the same provided a good starting point for this study in tracing the recent developments in this area. Other important milestones in the reform of ICT law that have been documented by the UNCTAD Report are as follows:

- The Press Act n°025/01 of 27 November 2003 which refers explicitly to the concept of information published on the Internet. The text also makes reference to news on web agencies subject to
prior declaration to the National Council of Communication and the public prosecutor who requires information on their identity, including where the site is hosted;

- Industrial Property Act n°1/13 of July 2009, and the Protection of Right of Author and its related Act n°1/06 of December 2005, both include the protection of software and other electronic or digital formats;

- Penal Code Act n°1/95 of 22 April, 2009 contains some articles on cybercrime, including provisions related to computer-related forger; 32 computer-related fraud; 33 unauthorized access devices;34 and system interference;35

- The Telecommunications Act n°1/11 of 4 September 1997 includes the following provisions that reference ICT-related offences:

  Article 10 prohibits the unauthorized interception of communications not intended for use by the general public and the unauthorized disclosure, content publication or use of any communications not intended for use by the general public. Article 24 grants the regulator the ability to authorize such conduct.
  Article 23 requires network and service providers to ensure confidentiality, data protection and secrecy.

Records indicate that Burundi had adopted a National ICT development Policy in February 2007 as an update to the National ICT Strategy that was adopted in 2004. It is not clear whether this has since been implemented due to among others, the government’s focus on the post-war cease-fire issues and lack of funding. The 2007 National ICT development Policy had envisaged six strategic objectives:

32 See: article 473.
33 See: article 474.
34 See: article 475.
35 See: article 476.
• Capacity-building
• Enhancement of a legal and regulatory environment
• Promotion of a base infrastructure
• Promotion of good governance
• Promotion and encouragement of private investment
• Promotion of the development of content and applications

A follow-up by this study to ascertain the current status, developments and implementation of the 2007 Policy, especially in relation to the legal and regulatory framework for ICT in general and cybercrime in particular was found to be essential. This was done through field work where data from Bujumbura was collected as discussed below.

Another critical document that sets out the direction of Burundi in the development of ICT is Vision Burundi, 2025. Chapter 5 of this Vision sets out its Pillars, which among other things, seeks to enable citizens to access modern techniques of data processing and telecommunication, to develop the services sector and ensure the formation of national expertise. It also advocates for the installation of regional and international co-operation in the context of major investments with respect to telecommunications and the installation of underwater optical fibers, which is also an EAC initiative.36

2.4.1 Status of Cyberlaws in Burundi

The status of cyberlaw in Burundi has also been documented. The UNCTAD Report notes that the government of Burundi commenced efforts to implement recommendations of the EAC after an EAC Task Force meeting in 2011 by drafting a Bill which provided for mechanisms of self-regulation of electronic exchanges. The Bill sought to enact the basic principles applicable to electronic communications,

including aspects related to e-contracts and administration of e-signature and evidentiary issues.

Other developments in laws that have a bearing on cyberlaws captured by the draft Bill included provisions on the legal conditions necessary for the security of the digital economy. It also addressed the usage, transfer, import and export of cryptographic products, accreditation of certification service providers and their liability. The Bill also put in place the principle of electronic communication freedom and its limits. The draft Bill also required Internet access providers to store the needed data for the identification of illegal content publishers. Other critical areas covered by the draft Bill included Internet and mobile payment systems and e-taxation.\(^{37}\) It is obvious that the information documented in the UNCTAD Report requires follow-up to capture the current state of affairs in the Country that have a bearing on our study. Indeed, the Report provides critical information that provided a foundation for the study to commence from.

### 2.4.2 Regulatory Authorities/Institutions

The institutional framework governing cyberlaw in Burundi has also been documented. It is on record that there are two main regulatory authorities in place. One for the Telecommunications sector, the *Agence de Régulation et de Contrôle des Télécommunications* (ARCT) and one in charge of the media - the *Conseil National de la Communication* (CNC). These two institutions are implementation authorities and are not responsible for regulatory reforms. Reform is the responsibility of the Ministry in charge of ICT in general and, in particular, by the SETIC whose mission, among others, is the promotion of the National ICT Policy and the implementation of the National Information and Communication Infrastructures Plan (NICI Plan). The ARCT is in charge of the telecommunications sector. Its mission includes, among others, the settling of disputes between users

or subscribers and the operators on the one hand and between the associated services providers on the other.

ARCT deals with spectrum management, tariffs and interconnection control. It also delivers concessions and licenses for the establishment and management of radio networks. The regulatory authorities are not independent of the Government, but the draft Bill had proposed greater independence for the ARCT, in order to create an enabling business environment for the ICT sector.

2.5 Observations on ICT the Infrastructure, Policy, Legislative and Institutional Framework

A critical review of the existing literature and documents on the state of the ICT infrastructure and related institutional, legal and policy framework of Burundi is in place. Some literature has also discussed the efforts that have been made by the government of Burundi in re-aligning its laws and policies to conform to the directives of the EAC Treaty. It has been suggested by some literature that these efforts, however, have not been successful as the country still lags behind in harmonizing its legislative and policy framework with the EAC framework.

It is clear that the available literature on the state of affairs of the efforts made by the Government of Burundi is relatively old and has predominately focused on desk work with comparatively less focus on field work. Also, a systematic review of the available literature and documents that underscore the state of affairs in regard to ICT and related legal and institutional framework reveals that the coverage and scope in general is scanty, fragmented and does not capture the most recent developments. The review of the laws and policies in relation to the country’s commitment at the international and regional levels, including the EAC, has also not been adequately, critically and comprehensively examined in the light of contemporary developments.
It is in the light of the gaps identified above that this study brings to the fore more recent developments in the country with a critical focus by conducting field work where views and opinions of main stakeholders in the ICT sector in Burundi were interviewed. Observations were also made and more recent developments in the country’s legislative and policy reform process captured.

2.6 Findings from the Field

Data collection in terms of field research in Burundi was conducted at the Burundi Telecommunications Regulations and Control Agency (Agence de Régulation et de Contrôle des Télécommunications - ARCT), the Burundi Ministry of Justice and at the Ministry of East African Community.38

2.6.1 Challenges in Addressing Cybercrimes in Burundi

2.6.1.1 Legal Challenges

Interviews with the respondents revealed that the following are the main legal challenges facing Burundi in its effort to combat cybercrimes:

i) The lack of a comprehensive legal framework regulating the Burundian cyberspace. It was noted that Burundi is still lagging behind in enacting Regulations for operation of cyberspace since there is no specific law on cyberspace/cybercrimes in Burundi.

ii) The absence of a legal framework to regulate cybercrimes makes it difficult to address the emerging crimes related to cyberspace and consequently join the regional efforts to harmonise cyberlaws in EAC.39

38 See: Annexure “A” List of Respondents Interviewed.
39 Interview with Mr. HAKIZIMANA, Constaque, Technical Director of ARCT-Burundi, at the ARCT Burundi, Bujumbura on 17th April, 2019.
iii) Cybercrimes related offences are addressed by using the Burundian Penal Code which does not address all challenges that have resulted in cybercrimes.  40

iv) Burundi is still at the drafting stage of the framework law which has lagged for a while. At the time of writing, there was a draft Bill on cyber issues that had, however, not yet been approved by the competent bodies. 41

2.6.1.2 Policy Challenges

The absence of a framework law to address cybercrimes in Burundi is to a great extent been attributed to a lack of a clear Policy on the subject. Respondents attributed vacuum to the lack of a clear national vision and strategy on cyber-security by the responsible ministry (ies).  42 It was also noted that such situation necessitates very low awareness by the general public and the decision makers in particular on cyber-security and the cybercrimes situation in the country. Therefore, the initiatives to contain cybercrimes in the country have been rendered ineffective as the population sought to be protected lack knowledge on the government’s approach. This makes it difficult for citizens to cooperate with the Government in identifying and reporting breach of cyber-security.  43

2.6.1.3 Institutional Challenges

The study revealed that there are weaknesses in some of the institutions charged with the prevention of cybercrimes in Burundi,

40 Mr. Hakizimana, ibid, note 1.
41 Interview with Germain Ntawuvyamara, Adviser at the Cabinet of the Ministry of Justice of Burundi at the Ministry of Justice of Burundi, Bujumbura on 10th April, 2019.
42 Ibid.
43 Mr. Hakizimana, Supra.
despite the efforts to put in place a relatively vibrant institutional framework.\textsuperscript{44}

One of the challenges is that some institutions are not adequately equipped.\textsuperscript{45} For example, one of the respondents at the ARCT revealed that there was no specific legal framework on cybercrimes to refer to and there was shortage of regular training on cyber-welfare to staff to equip them with knowledge to fight cybercrimes in the country.\textsuperscript{46} The other challenge relates to limitation in control and regulation of Burundian cyberspace. This was attributed to lack of a specific legislation on cyberspace.\textsuperscript{47} Non-coordination and lack of sharing of experience among institutions within the cybercrime sector was noted to be another challenge. This was also contributed to the difficulties in coming up with a comprehensive legal framework on cybercrimes.\textsuperscript{48}

\textbf{2.6.2 Impact of Challenges on Day-to Day Work}

Information obtained from the field from a respondent at the Ministry of EAC suggests that the problems addressed by the Community concern the Community in general. There are no specific challenges which affect the day to day rights of workers in the Ministry.

At the Ministry of Justice, the respondent explained that there are no problems related to cyber issues affecting the daily rights of workers in the Ministry. He explained that the exchanges made by the Ministry on the internet do not cause any incitement to hatred, insults or privacy breach.

\textsuperscript{44} Mr. Ntawuvyamara, \textit{Supra}.
\textsuperscript{45} Hélène NIMBONA, Adviser at Department of infrastructure (Ministry of EAC-Burundi), interview by the researcher, at Ministry of EAC-Burundi, Bujumbura on 9\textsuperscript{th} April, 2019.
\textsuperscript{46} \textit{Ibid}, note 3.
\textsuperscript{47} \textit{Ibid}.
\textsuperscript{48} Mr. Ntawuvyamara, \textit{Supra}, Note 2.
2.6.3 Attempts to Address Challenges

Field findings reveal that the country has made efforts to seek solutions to the identified challenges as follows:

- An Awareness-raising Workshop on Security and Cybercrime for Senior Executives from various institutions organized by COMESA 24th November, 2016 in Lusaka.  

- A Workshop Launching the activities of the Computer Incident Response Centre (CIRC) held between 25th and 27th February, 2019 in Bujumbura.

- Attending the EAC Regional meeting held in June 2018, which had the objectives of exchanging experiences on identifying, analysing challenges and opportunities to advance programs related to cyber-security, capacity building. The focus was in key areas such as: strategies, legal and regulatory frameworks, protection of the strategic infrastructures of cyber-security, the establishment of cyber-security structures and centres of excellence in the cyber-sector. Issues related to the development of a regional approach to better and effectively address relevant cyber-security challenges were also addressed.

2.6.4 Addressing Cybercrimes Challenges at Institutional Level

The government has put in place a system that seeks to address identified challenges and those that arise at the level of institutions in the country.

---

49 Mr. Hakizimana, Supra.
50 Ibid.
51 Ms. Nimbona, Supra, Note 6.
For example, at the ARCT it was noted that despite the challenges faced by the ARCT in containing cyberspace in Burundi, the ARCT has put in place mechanisms to:

- Sensitize responsible institutions to create cyber-incident prevention centres;
- Create an information exchange network between the cyber-incident prevention centres; and
- Report cyber-incidents to the Burundi Computer Incident Response Centre (CIRC) for control purposes.

Also, the Ministry of Justice has put in place mechanism such as:

- Reviewing of relevant laws and returning them to relevant institutions on time. It was noted that this intervention has proved to be relatively effective; and
- Providing technical assistance in analysis of the laws and giving legal opinions in time.

On the part of the Ministry of EAC in addressing the problem of cybercrimes in Burundi, the study revealed that it has done the following:

- Reminding the department in charge of security to organize awareness sessions which aim at informing the public on the existence of cybercrimes; and
- Assisting other relevant the Ministries in setting up laws, which aim at preventing and punishing cybercrimes, committed at national level in line with the regional arrangement.
2.6.5 Internal Interventions to Address Challenges

The ACTR has put in place internal programs to address identified challenges. These include:

- Establishment of the Computer Incident Response Team (CIRT) that handles computers’ security breaches and contain possible cybercrimes; and

- Organization of staff training on the technical and regulatory issues of cyber security conducted in January 2019.

At the Burundi Ministry of Justice, the respondent insisted that the Ministry is mainly in charge of coordinating technical institutions like the (ARCT) in charge of implementing specific programs related to cybercrimes.

At the Ministry of EAC, the main strategy adopted by such Ministry in addressing challenges associated with cyber space in the country is to promptly inform ministries and technical institutions in charge of cybercrimes about the decisions and directives taken in this area at regional level.

2.7 Impact of EAC States by Intervention Programmes

A respondent at the EAC Ministry noted that the programmes adopted at the EAC level are excellent but they must be evaluated by all Partner States periodically to issue specific recommendations by stakeholders of cybercrimes. In his view, by doing so, the activities designed to address the challenges of cybercrimes will be shared by all stakeholders in time and there will be uniformity in the actions taken to address them.

Findings reveal that efforts to address the challenges at the Ministry of Justice are not sufficient but progressive. The draft of the Burundian cyberlaw was noted to be a step towards addressing the problem of cybercrimes in the country.
2.7.1 Impact of Measures adopted by Institutions to Address Challenges

At the Ministry of EAC, the respondent was of the view that, the main work of the Ministry of EAC in Burundi was to coordinate all the activities of the EAC and to monitor the implementation of the decisions and directives taken by EAC Partner States. The respondent observed that the Ministry was doing its best to keep track of the implementation of laws which govern cybercrimes with the Ministry of Public Safety. It was noted further that this coordination would help to deter criminals and facilitate law enforcement officers in their day to day work towards prevention and punishment of cybercrimes.

2.7.2 Relationship between Challenges and Attaining EAC Objectives

Information obtained from a respondent at the Ministry of the EAC reveal that institutions responsible for monitoring the process of harmonizing cyber-legislation respect the objectives and goals set up by the EAC for the common development of Partner States.

2.7.3. Initiatives at the EAC level to address Cybercrimes

Regarding the initiatives at the EAC level to address the cybercrimes problem, the respondents had different knowledge on the issue. The key informant from the ARCT made it clear that he was not aware of any initiative at the EAC level to address the problem of cybercrimes nor any intervention programmes adopted by the EAC States to address the said problem.

At the Ministry of Justice, it was revealed that the Ministry was aware of the initiative taken by the EAC to address cybercrimes. It was elaborated that the EAC has organized meetings of experts to set up a community legal framework on e-Commerce, including organization of a forum on e-Government and cyber legislation.
From the Ministry of the EAC the respondent was of the view that a number of initiatives were being taken at the EAC level to address challenges related to cybercrimes. She mentioned the development of the security protocol, which covers cyber-security sector, and organization of trainings at the regional level targeting all the EAC Partner States as a case in point.

2.7.4 Reasons for Lack of Implementation of the EAC Initiative to Harmonize Laws

There were no clear answers as to the reason behind lack of implementation of the EAC initiative to harmonise cyberlaws in Burundi from the Ministry of Justice. It was explained by the Ministry of Justice that lack of implementation can only be known by the institutions of the EAC. However, the respondent proposed that there must a common cyberlaw in all EAC Partner states of which the Partner States will be seeking to harmonise. Unfortunately, he added, Burundi is yet to have a specific cyberlaw as a starting point to harmonise cyberlaws in the EAC.

From the Ministry of EAC the respondent was of the opinion that the main reason for the lack of implementation of the EAC initiative to harmonize cybercrime laws and policies in Burundi is the fact that the concept of cybercrime is still new and the law which governs the same is still at the drafting stage.

2.7.5 Suggestions on Addressing Challenges

At the Institutional level:

Recommendations by ARCT:

- Regularly auditing of the operation of the network;
- Setting up utilities to protect against cyber incidents (antivirus, firewall);
• Implementation of a strategy for the protection of infrastructures (material and human); and

• Sensitization of staff in the protection of infrastructures and data as well as reporting of the cyber-incidents.

Recommendation by the Ministry of EAC:

• The respondent in this Ministry recommended that there should be prompt information to the stakeholders about changes in the field of cybernetics, to ensure that everyone feels concerned about the issue and equip the relevant services to be aware of the matter of scams on the internet, blackmail, hacking email addresses, paedophiles, etc.

At the EAC level:

It was recommended by the Ministry of Justice that;

• The EAC secretariat should plan for awareness raising programs on cyberlaws in each Partner State; and

• The EAC Secretariat should oversee that several mechanisms are devised for each Partner State to comply with the laws enacted and indicate the deadline for implementation by each State.

Recommendations by the Ministry of the East African Community:

• There should be harmonization of laws in the cyber sector at regional level;

• Development of the relevant technical expertise to deal with cybercrimes at regional level; and

• Development of a regional strategy for combating cybercrimes.
2.8 General Suggestions

It was generally suggested by the ACRT that there should be:

- Setting up of a legal and regulatory framework regulating the Burundian cyberspace;
- Awareness raising to the general public and decision-makers on cyber-security and cybercrime in particular;
- Building human resources capacity in cyber-security and cybercrimes to all relevant institutions.

It was generally suggested by the Ministry of Justice that:

- There should be collective technical meetings between the experts in cyberspace and users of the services offered for knowledge exchange on how to combat cybercrimes in Burundi.
- Sensitization of all decision-makers (Executive, Legislature) on the importance of putting in place a regulation on cyber security and cybercrimes in Burundi; and
- Initiation of cyber incident prevention centres within different relevant institutions.

General suggestion from the Ministry of East Africa was:

- Adoption of an effective law on cybercrimes in Burundi; and
- Organizing capacity building trainings for stakeholders within the cybercrime sector to deal with new cybernetics challenges.

2.9 Conclusion

The field research in Burundi has revealed that efforts to combat cybercrimes in Burundi are highly being impaired by lack specific legal framework touching on cyberspace. However, it has been revealed
that, such legislation is on the pipeline. It is presumed that the coming into effect of the law addressing cyberspace in Burundi will also contain the current challenges and problems related to cybercrimes and provide for more coordinated institutional framework and functioning to combat cybercrimes.
CHAPTER THREE

HARMONIZATION OF THE CYBERCRIMES LEGAL FRAMEWORK IN KENYA

Theodora Mwenegoha

3.1 Introduction

Officially known as the Republic of Kenya, Kenya is comprised of 580,367 square kilometres (224,081 square miles). It has a population of slightly above 50 million and is considered as the world's 48th largest country by total area ranking it as the 27th most populous country in the world. The country is bordered by South Sudan to the North West, Ethiopia to the North, Somalia to the East, Uganda to the West, Tanzania to the South and the Indian Ocean to the South-East.52

In terms of economic development, Kenya is considered a lower-middle-income economy being the largest in Eastern and Central Africa. Its capital City, Nairobi, serves as a major regional commercial hub. Agriculture is the largest sector; tea and coffee are traditional cash crops, while fresh flowers are a fast-growing export. The service industry is also a major economic driver, particularly tourism. Kenya is a member of the East African Community trade bloc, though some international trade organizations categorize it as part of the Greater Horn of Africa. Africa is Kenya's largest export market, followed by the European Union.

3.2 Policy, Legislative and Institutional Framework for ICT

The ICT sector in Kenya has experienced tremendous growth as a result of Government improvements in the area, including the

installation of four fibre-optic sea cables between 2009 and 2016. Consequently, the Government of Kenya reviewed its ICT Policy with a view to take into consideration the new technological developments in the Sector. This resulted into the Kenya National ICT Policy of June, 2016.

The aim of the 2016 Policy is to provide a ‘proactive policy and regulatory framework that is not only in synch with contemporary technological realities and dynamics,’ but which is also expected to guide the orderly development of the ICT sector in order to ensure maximum developmental impact for the benefit of all Kenyans.

Along with the Policy, there are other laws and regulations in the ICT sector in Kenya. These include the Kenya Communications Act (KCA) of 1998; the Science and Technology Act (Cap. 250) of 1977; and the Kenya Broadcasting Corporation (KBC) Act of 1988.

The several regulations in the ICT area include the Kenya Information and Communications (Dispute Resolution) Regulations, 2010, the Kenya Information and Communications (Tariff) Regulations, 2010, the Kenya Information and Communications (Compliance Monitoring, Inspections, and Enforcement) Regulations, 2010, the Kenya Information and Communications (Fair Competition and Equality of Treatment) Regulations, 2010, the Kenya Information and Communications (Interconnection and Provision of Fixed Links, Access and Facilities) Regulations, 2010, the Kenya Information and Communications (Universal Access and Service) Regulations, 2010, the Kenya Information and Communications (Consumer Protection) Regulations, 2010, the Kenya Information and Communications (Radio Communications and Frequency) Regulations, 2010, the Kenya Information and Communications (Numbering) Regulations, 2010, the Kenya Information and Communications (Licensing and Quality of

---

54 Kenya National ICT Policy, June 2016.
Service) Regulations, 2010, the Kenya Information and Communications (Importation, Type approval, and Distribution of Communications Equipment) Regulations, 2010 and the Kenya Information and Communications (Electronic Certification and Domain Name Administration) Regulations, 2010.

These laws and regulations provide for provisions which address diverse matters of ICT in Kenya including dispute resolution between consumers and service providers, determination of tariffs and tariff structures, regulating issues of compliance, including monitoring and enforcement of installations and maintenance of communication infrastructure, addressing interconnections issues, consumer protection and regulating and promoting of fair competition in the ICT sector.

There are several bodies overseeing these laws. The main ones include the Ministry of Information and Communications Technology, the Postal Corporation and the Communications Commission, the Kenya ICT Board and the ICT Authority.

3.3 Status of Cyberlaws in Kenya

The development of cyberlaws in many of the East African countries is attributed to the efforts established by the United Nations Conference on Trade and Development (UNCTAD). These efforts resulted into the establishment of special cyberlaw task force under the EAC to come up with legal framework for cyberlaws. Consequently, East African countries began adopting frameworks at their national levels. Whereas the UNCTAD efforts began in 2007 it was a year later that Kenya has enacted its cyberlaw legislation known as the Computer Misuse and Cyber Crimes Act, 2018.

---

However, the efforts towards this legislation can be traced way back to the Kenya e-Government Strategy issued in 2004 and Kenya National ICT Policy which was reviewed in 2016\(^{56}\) with both reflecting initiatives for the development of cyberlaws of the country.

The Computer Misuse and Cybercrime Act, 2018 of Kenya contains several cybercrimes provisions embodied in Part III of the Act including computer access crimes such as computer espionage, internet crimes, unauthorized access, access with intent to commit further offence, unauthorized interference, unauthorized interception, illegal devices and access codes, unauthorized disclosure of password and access code.

The Act also provides for Internet and content related crimes including cyber-espionage, false publications, child pornography, computer forgery and fraud, cyber-harassment, cybersquatting, identity theft and impersonation and phishing. The Act addresses cyber-terrorism and data protection as well.

Apart from the specific provisions, the Act in general has provisions with the aim of combating cybercrimes and addressing cyber issues emerging in the country. Also, matters pertaining to detection, investigation and prosecution of cybercrimes are addressed in the Act. Part IV of the Act has specific provisions on procedures to be followed in investigation of cybercrimes.

The Act further provides for provisions regulating International Cooperation, mutual assistance and handling of cybercrime issues in its Part V. Jurisdiction matters are addressed under Part VI of the Act.

The Development of the cyber legislation in 2018 in Kenya is also attributed to the Kenya Information and Communication Act (KICA), Chapter 411A of the Laws of Kenya\(^{57}\) which not only regulates improper


\(^{57}\) This Act has been amended from time to time.
use of the telecommunication system (see section 29), establishes general offences relating to telecommunication services (Part III of the Act), but also has provisions on cyberlaw and security.

The Information and Communication Act has provisions relating to telecommunication services such as regulating modification of messages, interception and disclosure and tampering with telecommunication plants (sections 31 – 32 of the Act). Part VIA of the Act has specific provisions on electronic transactions and cyber-security where provisions on electronic records to provisions enhancing e-government are presented.

Other Acts, which have a bearing on cybercrime in the country, include the Penal Code, Cap. 63, and the Trademark Act No. 3 of 2003, the Copyright Act, No. 12 of 2001 and the Industrial Property Act Cap. 509.

3.4 Regulatory Authorities/Institutions

There are Authorities in Kenya vested with task of regulating ICT in the country. These include the Communications Authority of Kenya (CAK)\textsuperscript{58}, which is the regulatory body for the communications sector in Kenya. The Authority is vested with a task of facilitating the development of the Information and Communications sectors including: broadcasting, multimedia, telecommunications, electronic commerce, postal and courier services. The Authority attains its mandate from sections of both the Computer Misuse and Communication Act (see section 1) and Kenya Information and Communication Act (Cap. 411A).

There is also the Information and Communication Technology Authority (ICTA) which is tasked with ‘rationalising and streamlining the management of all the Information and communication

\textsuperscript{58} Communications Authority of Kenya, Official Website, available at: https://ca.go.ke, accessed on 12\textsuperscript{th} October 2019.
Technology (ICT) functions of the Government of Kenya’ The ICTA has a broad mandate that entails enforcing ICT standards in the Government and enhancing the supervision of its electronic communication. The authority also promotes ICT literacy, capacity, innovation and enterprise in line with the Kenya National ICT Master plan 2017.

The ICTA is a consolidation of three previously separate government agencies; the Information and Communication Technology Board of Kenya (ICT Board), the e-Government Directorate and the Government Information and Technology Services (GITS).

3.5 Field Findings and Analysis

The above discussion highlights the current situation and the state of the ICT infrastructure and related institutional, legal and policy framework of Kenya. Whereas the above discussion has revealed that Kenya has advanced in its ICT, it also highlights the gaps that still remain in such development and in ensuring that not only ICT issues in Kenya, but also those in the EAC are addressed. These gaps are further revealed and reflected in the field research results where the study shows that there is a need of further efforts to be taken in order to address cyber concerns in Kenya and also in relation to harmonizing the EAC ICT and cyber framework.

3.5.1 Field Findings

Several institutions were contacted for data collection where respondents were asked questions in relation to several related themes of the research including cybercrime related challenges, challenges on legislation, policies and institutional framework and measures taken or to be taken at national and international (EAC) levels. These findings

59 Ibid.
60 Ibid.
61 Ibid.
emanate from a field research conducted in terms of interviews among the officers in the Office of the Director of Public Prosecution, Kenya Task Force on Data Protection, IP Committee of the Law Society of Kenya, the Law Society of Kenya, and the Kenya Cyber Security and Forensic Association. The findings are grouped based on the responses obtained from each office.

### 3.5.1.1 Office of the Director of Public Prosecutions

#### (a) Cybercrime Challenges

The study identified a number of challenges in combating cybercrimes in the country. Some of the main challenges include the fact that cybercrimes by their very nature are crimes that can be easily committed and are often committed by people who are not necessarily within the jurisdiction of the Kenyan courts.

Secondly, the process of collection, preservation and presentation of evidence of cyber-related offences is not easy. This mainly because the evidence is often volatile and at times is not within the country but lies in machines and servers outside the jurisdiction of law enforcement agencies.

Thirdly, the legal framework for combating cybercrimes is playing catch up with the offences. This implies that perpetrators of cyber offences are constantly developing new and ingenious ways of committing these offences. The law on cybercrime is also inhibited by constitutional standards. For example, the right to privacy precludes a police officer from searching the contents of a mobile phone without a search warrant, yet if the police officer were to go before a judge to obtain the warrant it is very possible that the digital footprints will be erased or destroyed by the time the officer returns to the scene of the crime.

---

62 Interview with Duncan Ondimu, Principal Prosecution Counsel, Office of the Director of Public Prosecutions.
(b) Legal, Policy and Institutional Challenges in Combating Cybercrimes

Interviewees noted that the legal, policy and institutional frameworks of the country have specific challenges. It was noted that the legal framework of the country is under review in response to the new and ingenious ways that cybercrimes are being committed. Currently, the legal framework cannot be said to be fully combative of cybercrimes.

The second problem is that the cybercrime laws are strewn in very many different statutes. This makes it difficult for the relevant institutions to implement. Furthermore it was observed that the statutes create different institutions with the same mandate of curbing cybercrimes. The duplication of roles makes it difficult to effectively address cybercrimes.

As to whether these challenges have been discussed in various forums at national or sectoral levels, the findings were that the Kenyan legal framework has recently been reviewed with the intent of addressing cybercrimes. The Constitution of Kenya 2010 acknowledges and provides the foundation of using and admitting into evidence digital material. Article 260 of the Constitution of Kenya defines the term document in contemplation of both physical and virtual environments. Furthermore, pursuant to this Constitution underpinning, the Evidence Act of Kenya was amended to permit the admissibility of electronic evidence in Kenya. (Sections 106B and 78A).

The Kenya ICT policy is currently being reviewed by different state and non-state agencies. The intention of the policy is to lay a basis for the adoption of digital evidence and a national ICT Master plan.

It was also noted that the Parliament is one of the key players in the discussions for enhancing the legal framework for curbing cybercrime. At the Office of the Director of Public Prosecutions there have been initiated training programs for police officers and other enforcement agencies. Also, there are training programs for the members of the
public. It was also confirmed that the DPP’s Office was not aware of any initiatives at the EAC level to address the cybercrime related challenges.

This study further found that the office of the DPP is tasked with the responsibility to prosecute people who breach the law. However, it was observed that prosecuting cybercrime is the most frustrating activity because the offenders may be out of the jurisdiction of the courts. Also, it was admitted that matters become more complicated when there is no collaboration framework between Kenya and other States for the extradition and punishment of perpetrators of cybercrime.

Despite the Office of the DPP being unaware of any initiatives to deal with cybercrime at the EAC level, it was the opinion of the Office that the interests of the EAC are better served when there is minimal criminal activity, especially in the cyberspace. Also, in terms of the reasons behind the lack of implementing the EAC initiatives relating to cybercrimes in Kenya, it was noted that the differences in approaches taken by Member States in defining and conceiving cybercrimes renders the exercise difficult. Since cybercrimes are like any other criminal offences, differences in defining and punishing the same among the Member States of the EAC are the main challenge. This means that, what is a cybercrime in Kenya may not be necessarily a crime in Rwanda or Burundi.

It was also found that the office of the DPP has a special department dealing with the prosecution of cybercrimes. The DPP cooperates with the special investigation agencies of the police in investigating and prosecuting these offences. The respondent from the DPP’s Office was of the opinion that the strategies (Rules and Regulations) adopted in the country are very relevant in addressing the identified challenges. Since cybercrimes are unique, they require skilled officers to investigate and successfully prosecute the same. However, it was commented that more should be done towards establishing effective cooperation channels with other countries. The institutions tasked with
the research, investigation and prosecution of these offences should also work with greater synergy.

It was further found that the law as it currently stands is not adequate to deal with cybercrimes. There are other Bills still pending in Parliament such as the Data Protection Bill that are very important in securing personal information of individuals. The need to increase resources and personnel to improve investigations and prosecution of cybercrimes was also realized. The Data Protection law will go along with preventing the commission of these crimes because it will impose an obligation on the part of those who handle personal data to ensure that the information remains secure.

(c) Measures at National and International Levels

The respondent at the Office of the DPP being one of the key stakeholders in the institution addressing cybercrimes in Kenya noted that the best way to deal with the problem of cybercrime is to make law reforms to provide for the authentication and certification of digital evidence. He noted that this was being done in the UK and makes the prosecution of cybercrimes relatively easier. Also, it was observed that the starting point at the EAC level should be for the Partner States to agree on the definitions of cybercrimes. It will also be important that an agreement is reached providing the framework for cooperation between State agencies in terms of real time information sharing. The agreement should also make cybercrimes extraditable offences within the region.

3.5.1.2 Kenya Taskforce on Data Protection

At this institution, two separate interviews were held. The focus of the interviews was to collect information on three different aspects of cybercrime as documented below.

---

63 One Interview was held with John Walubengo, an academic staff at the Kenya National Taskforce on Data Protection (first respondent) and another interview was held with
(a) Cybercrime Challenges

The first respondent observed that the main challenge in combating cybercrimes is the lack of coordination between different investigation agencies within the State. There is also a shortage of skilled personnel with the knowledge of handling and preserving evidence in this area. Also, the second respondent noted that cybercrimes are crimes committed in the cyberspace. Some of these offenders are often far from the reach of our courts. The perpetrators of these offences are high skilled individuals. They are capable of committing these offences and quickly erasing whatever evidence there may be.

It was further noted by the first respondent that at the moment there is no national policy in place, although a draft policy is under review. The law is yet to fully define all cyber-related offences. The institutions tasked with research, investigation and prosecution of cybercrimes also have an acute shortage of skilled officers. The second respondent was of the view that the issue of cybercrimes has only recently received the full attention of the government after various financial institutions reported losses as a result of cybercrimes. It is no wonder that Kenya is in the process of formulating a national ICT policy now. Also, the institutions tasked with investigation and prosecutions of these offences do not have sufficient skilled manpower. For instance, very many police officers do not even know what cybercrimes are and the process of collecting evidence.

On whether these challenges been discussed in different forums at national and sectoral levels, the first respondent stated that he had the benefit of attending various multi-agency forums where the reform agenda of this sector of law was the main issue being discussed. The second respondent confirmed that a lot of stakeholder meetings are being carried out by the taskforce in collaboration with other

---

Gatuyu Thuranira, Law Society of Kenya (LSK) Member to the Kenya National Taskforce on Data Protection (second respondent).
institutions with a view of developing an appropriate legal framework. However, on awareness of any initiatives at the EAC level to address the challenges, both respondents confirmed that they were not aware of any such initiatives. It was, therefore, noted that apart from the provisions of the EAC Treaty calling for collaboration in matters of security, the Partner States do not appear to be very keen on addressing the issue of cybercrimes or generally crimes for that matter jointly.

Furthermore, it was noted that the national taskforce has the responsibility of undertaking a comprehensive audit of the existing legislation, regulation, policies, administrative procedures, sessional papers, Government guidelines and circulars relating to privacy and data protection frameworks in Kenya. It is also within the mandate of the taskforce to identify any gaps or inconsistencies in the existing frameworks and proposes specific review requirements. The taskforce is further supposed to propose any new policy, legal and institutional framework that may be required to implement the policy and regulatory framework for privacy and protection. It was noted that these tasks were enormous.

As to whether the cybercrime challenges interfere with the process of attaining the EAC objectives and goals, the second respondent opined that when the Partner States integrate, the first point of contact for most market participants is the cyberspace. Unless there is a robust legal framework at the regional level to deal with cybercrime within the region, the process of integration stands imperiled. The barriers behind lack of implementing the EAC initiative was said to be different approaches taken by the States on what amounts to a criminal offence. Harmonizing criminal law generally and cybercrime law specifically suffers the same fate.

Regarding the role of the task force in addressing cybercrime challenges, the respondents observed that the task force has a very important role to play. The task force’s work is very important in
informing the reform agenda in this area of law. Furthermore, it was confirmed that the task force has a number of specific programs in where it works together with all the stakeholders in this sector including private organizations. The task force undertakes awareness raising programs and public training sessions.

On the relevance and effectiveness of the strategies adopted, the respondents noted that most of the strategies adopted are very relevant. For example, training members of the public creates awareness that in turn results with the members of the public handling their personal information with greater care. The task force is constantly engaged in stakeholder conferences where views of both public and private sector entities are collected. This is useful to the task of proposing a streamline to the legal framework for the prevention and prosecution of cybercrimes. Despite the above, it was further noted that there is a need for more collaboration with internal state actors and other regional and international institutions. More strategies need to be developed and engage at a wider level with the public and the institutions involved in curbing cybercrime. Unfortunately, budgetary constraints were also seen as a challenge towards developing and implementing more strategies.

(b) Challenges on Legislation, Policies and Institutional Framework

On this aspect, it was further observed that the main function of the taskforce is to collate all the laws in this area with a view of proposing a comprehensive legal framework. Cyberlaws in Kenya are generally spread across a multitude of statutes, which creates a discord and inhibits the fight against cybercrimes. It was also observed from the respondents that there are still a lot of internal conflicts within the texts of the law that need to be amended and harmonized. A specific aspect of the law identified for amendment included, among others, in relation to the presentation of digital evidence in court so that the same is in touch with the very character of cybercrimes.
The most appropriate way of dealing with cybercrime as recommended by the respondents is through the creation of a single state agency with the duties of researching, training and investigating cybercrimes. This state agency should be staffed with highly skilled personnel and granted sufficient resources to carry out the task of detecting, preventing and collaborating with the DPP in the prosecution of cybercrimes. Also, it was proposed by the respondents that there should be in place a robust legal framework clearly providing for the various cybercrimes. The institutions dealing with the cybercrimes should be equipped with up to date equipment for detecting cybercrime and analyzing digital forensic material.

(c) Measures at National and International Levels

As per the interviews it was noted that the National Taskforce on Data Protection is at the forefront of reviewing the law on cybercrimes. The mandate of the institution is to propose the legal framework that effectively deals with the issue of cybercrimes. Regarding the anti-cybercrime interventions at the EAC level, the respondents demanded for harmonization of the EAC cyberlaws. The EAC Partner States should agree on definition of these crimes and should endeavor to create a legal framework for cooperation in the investigation, prosecution of these crimes and information sharing.

3.5.1.3 Cyber-Security and Forensic Association

The responses received from this institution indicate that the main challenge in combating cybercrimes is the skill gap with the government agencies tasked with the role of combating cybercrime. To this institution the law is not a problem at all when it comes to fighting cybercrime. It was the opinion of the institution that there are enough legal provisions dealing with the issues of cybercrime. Also, it was alleged that the institutions that are mandated to investigate and prosecute cybercrimes do have the same set of skills as the criminals engaging in these crimes.
Officers from the association have been invited in various stakeholder conferences organized by public and private entities. The challenge of lack of skills within the investigatory arms of the Government has been cited as one of the biggest challenge in combating cybercrimes. Also, the shortage of cyber security experts has been cited as among the factors making it difficult for organizations to develop cyber-resilience. A lot of institutions have lost substantial sums of money due to vulnerability to cyber-attacks. Furthermore, in terms of the roles and relevance of the association, the cyber-security and forensics association of Kenya offers training to its members on developing technology. This is considered to be very important because of the dynamic nature of cybercrimes. The Association offers public training on individual data management and strategies and skills in managing corporate data. The association shares its views at stakeholder forums on some of the strategies being employed by cybercriminals.

Further to the above, the cyber-security and forensics association’s main objective is to educate the public and our clients on techniques for establishing systems that are resilient to cyber-attacks. It is believed that training and imparting of these skills is a critical component of combating cybercrime. Also, more collaboration between the state agencies and private entities was insisted. Having special divisions with the necessary training and skills to detect and prevent cybercrime in the law enforcement agencies was recommended. The association was not aware of any EAC level intervention in dealing with cybercrime.

3.5.1.4 The Law Society of Kenya

The details documented in this part are based on the interview conducted with the Law Society of Kenya (the LSK).\textsuperscript{64} It was observed that there are a lot of challenges in combating cybercrime. The greatest challenge is that these are crimes that are committed by

\textsuperscript{64} Interview with Maria Mbeneka, Council Member & Convener of the ICT/IP Committee of the Law Society of Kenya.
persons who are highly skilled and who may be anywhere on earth. It was further noted that, firstly, there are legal and institutional shortfalls in the fight against cybercrimes in Kenya. The present legislation does not adequately address the problem of cybercrimes. There are inconsistencies in the definition of essential terms relating to cybercrimes. Secondly, handling and presenting digital evidence is still a challenge for both the prosecutors and the court. Furthermore, traditional human rights such as the right to privacy makes it difficult for investigating agencies to carry out investigations.

As to whether these cyber challenges have been part of the debates and discussions, it was observed that the LSK through the Committee on ICT/IP has and continues to engage with stakeholders in different fora at different levels of the Government. Also, at the LSK level, lawyers have reported to the Society the need for training in cyber security. The law society provides training packages for lawyers to enhance the security of the data that comes into their possession on the basis of confidentiality.

In terms of the role of the LSK in addressing the cybercrime problem, it was noted that the LSK being the premier bar association of Kenya, is mandated with the professional wellbeing of lawyers in Kenya. The Society closely keeps a look on the development of the law on cybercrime and the potential effect of the legislation on the practice of law by advocates in Kenya. Also, the Society is engaged in public awareness programs, public training sessions and continuous professional development programs for advocates. The respondents further stated that the relevance of the LSK in the war against from cybercrime is derived from the core mandate of the LSK, which is to ensure the professional wellbeing of Advocates. Advocate-Client confidential is a legal and ethical obligation on the part of advocates. Cyber security trainings enable advocates to maintain these confidentiality and therefore maintain high standards in terms of their legal and ethical obligations. It was further noted that there is
definitely the need of creating greater awareness among members of the public and training data handlers on cyber security measures.

Regarding the adequacy of legislation, policies and institutional framework which seek to address cybercrimes, it was observed by the respondents from the LSK that there is a remarkable improvement in the legal framework on cybercrime in the past decade. However, as earlier indicated there are still gaps within the law and institutional deficiencies that need to be addressed. It was argued that the most effective way of dealing with cybercrimes is through collaboration among state agencies, other states and relevant international institutions.

3.6 Analyzed Observation of Field Research

3.6.1 Legal Challenges

The field research revealed several challenges that the Kenyan Government faces in combating cybercrimes. Among the major challenges that have been identified by majority of participants interviewed in the research is the cross border nature of cybercrimes. It is evident from the interviews that several cybercrimes happening in Kenya are not committed under its jurisdiction, rather from other jurisdictions. This raises challenges in dealing with such crimes, not only in operational point of view, but also in legal sense. It is possible that criminal acts offending in Kenya are not action of criminal nature from originating jurisdictions. These challenges may easily be addressed in offline initiatives. However, the cyber nature of the crimes raises complexity, which cannot be addressed by Kenya alone. Due to the nature of technology, a cybercrime can be committed from several jurisdictions at the same time; or to several jurisdictions at the same time. Clearly, Kenya needs to work with other jurisdictions in cyber-policing in order to effectively curb cybercrimes.
It is also evident from the field research that harmonization of cybercrimes among EAC is crucial so as to have common definition and understanding of cybercrimes and common efforts in combating cybercrimes within EAC Member States. Similar efforts may be needed between EAC Member States and other Regional and International communities to overcome cybercrime-fighting challenges the individual countries such as Kenya face.

Moreover, the research has revealed that prosecuting cybercrimes is complicated and challenging as far as evidence collection, preservation and presentation are concerned. This is due to the volatile and fast changing nature of the cyber-world. Evidence at hand can vanish within seconds and tracing it down cannot easily be achieved without collaboration with other involved jurisdictions. These emphases further the importance of combined efforts among EAC Member States against cybercriminals. Tracking down cyber-criminals and tracing them online can be much easier task if collaborated among Member States. Moreover, these combined efforts are also needed in enforcement level where all EAC Member States need to have common enforcement mechanism.

It was revealed from the study that Kenya does not have comprehensive measures at hand in dealing with cyber challenges and little is being done at EAC level. Among other concerns expressed is the fact that there are insufficient legal responses as far as cyber-regulation is concerned. As expressed with one respondent during the interview, there is a view that the legal framework for combating cybercrime ‘is playing catch up with the offences’. The consequence of this is that the cyber-criminals are always ahead of the law, developing new and ingenious ways of committing cybercrimes.

It is certain that cyber-world is growing every day and it is hard for governments and lawmakers to foresee new challenges that are likely to arise with new technologies. However, this does not give a reason for lawmakers and cyber-security enforcers to drag behind the cyber-
criminals. Rather, quick measures are needed for new cyber challenges and stable measures should always be in place for the old ones. In order for the Kenyan Government to achieve this, it needs to work in close collaboration with other EAC Member States to ensure that it is ahead of technology and that is able to address new tricks invented by cyber-criminals. This emphasizes the need to harmonize cyberlaws and efforts in the Community.

The research has also revealed that legal initiatives in combating cybercrimes are inhibited by constitutional standards. Several legal provisions in cybercrime legislation are contradictory to Constitutional provisions. An example given on this scenario is the right to privacy, which precludes a police officer from searching the contents of a mobile phone without a search warrant; however, such warrant takes a long time to obtain allowing erasing of evidence from a suspect.

Adherence to the rule of laws is very important at this age of technology development. It is essential that the Government and its institutions adheres to the constitution and laws of their countries and administer them fairly and justly. Such adherence does not exempt cybercrimes or the enforcement of its law. The Government should come up with measures to address possible challenges arising from cyber-world. Such measures are bound to be successful and effective if efforts of different nations are pulled together to fight one course. The Kenyan Government and other EAC Member States should draw lessons from other regional integration such as EU in harmonizing efforts combating cybercrimes. Moreover, swift actions need to be implemented by each EAC Member States in order for such efforts to be effective. The ongoing concerns from the field research results from Kenya are evident that more is still to be done in order to reach a satisfactory state in combating cybercrimes, both at national and regional level.
3.6.2 Policy and Statutes Challenges

The study has revealed that the current legal framework of Kenya is not comprehensive and does not address all offences occurring in the online world, hence it does not fully combat cybercrimes. Moreover, cybercrime laws are scattered in different statutes. This makes the implementation of such laws to be difficult and uncertain. This also creates confusion as the scattered laws create different institutions with the same mandate of curbing cybercrimes. To complicate the matter even further, the study has revealed that there is lack of coordination between different investigation agencies within the country in combating cybercrimes. This makes it difficult to effectively address cybercrimes.

The challenges highlighted above can be addressed at national level through amendments and enacting a comprehensive law with clear provisions regarding its implementations. However, a single regional framework on cybercrime is a certain measure of eradicating unsatisfactory and scattered national laws by acting as a comprehensive cyber framework to be incorporated into each member state cyberlaw system.

3.6.3 Initiatives undertaken at National Level in Addressing the Challenges

The Kenyan Government has been working towards combating cybercrime. The study revealed that the country has done commendable efforts in the area and continues to do so. Among these efforts is reviewing of the Kenyan legal framework with the intent of addressing cybercrimes. Such review is noted in the Constitution of Kenya 2010, where it acknowledges and provides the foundation of using and admitting electronic and digital evidence. Article 260 of the Constitution of Kenya in defining the term document contemplates both physical and virtual environments.
As a result of this Constitutional reinforcement, the Evidence Act of Kenya was amended to permit the admissibility of electronic evidence in Kenya (sections 106B and 78A of the Act). Moreover, the Kenya ICT Policy is currently being reviewed by different State and non-state agencies so as to lay a foundation for the adoption of digital evidence and a National ICT Master Plan. Furthermore, there are several Bills pending to be passed as laws with cyber-regulating provisions. One such Bill is the Data Protection Bill.

In further efforts to ensure smooth operations in combating cybercrimes, the office of the Director of Public Prosecutions in Kenya has initiated training programs for police officers and other enforcement agencies. The office also offers training programs for the members of the public.

3.6.4 Initiatives at the EAC Level in Addressing the Challenges

Whereas there are several commendable efforts carried out under the EAC in addressing cybercrimes concerns, there are no specific initiatives, which may link the Kenyan Government’s efforts to the EAC. Moreover, it was revealed during the study that there is no collaboration framework between Kenya and other states in combating cybercrimes, making efforts for extradition and punishment of perpetrators of cybercrime complex. This highlights the current state of inter-governmental efforts in combating cybercrimes and evidence that more needs to be done in harmonizing, combating and fighting cybercrimes at inter-governmental and regional level.

3.7 Conclusion

This study revealed that, despite major efforts undertaken by the country, there still remain major challenges, which still need to be

---

65 It is noted, however, that this is only a Draft Policy which was never in place; lack of such leaves a significant gap in efforts towards combating cybercrimes.
addressed. It is concluded that although there are some commendable efforts by the Kenyan government in combating cybercrimes and addressing cyber challenges, such as reviewing policies, Bills, enacting laws and establishing relevant institutions, there is still significant challenges. There is still a legal gap as not all cyber concerns are addressed. Furthermore, the country has not taken significant efforts in addressing harmonization of cyberlaws among EAC Member States.
CHAPTER FOUR

HARMONIZATION OF THE CYBERCRIMES LEGAL FRAMEWORK IN RWANDA

Laurean Laurent Mussa

4.1 Introduction

Rwanda is a landlocked sovereign State located in central Africa with a widely varied geography. It has one of the highest population densities in Africa (1060/square mile) with a young, mostly rural population. In 2019, the population was estimated at 12.63 million, an increase from 2013’s estimate of 11.8 million. The country has struggled with its legacy of ethnic tension associated with the traditionally unequal relationship between the Tutsi minority and the majority Hutus and currently trying to recover from the ethnic strife that culminated in government-sponsored genocide in the mid-1990s. The country’s population density is the highest in Africa and it is estimated to be 467 people per square kilometer.

Also known as ‘The Land of a Thousand Hills’, Rwanda has five volcanoes, 23 lakes and numerous rivers, some forming the source of the River Nile. The country lies 75 miles south of the equator in the Tropic of Capricorn, 880 miles ‘as the crow flies’ west of the 2 Indian Ocean and 1,250 miles east of the Atlantic Ocean-literally in the heart of Africa. Uganda to the North, Tanzania to the East, Burundi to the South and the Democratic Republic of Congo to the West border it. 66

According to UNESCO, 67 Rwanda was a centralized monarchy under Tutsi kings until 1899 when it became a German colony. In 1919, it was placed under Belgium in accordance with the Mandate System of

---

the League of Nations. From 1959 onwards, there were systemic massacres against the Tutsi; and this lead to the formation (by Rwandan refugees in exile) of the Rwandese Alliance for National Unity (RANU) in 1979; which became Rwandese Patriotic Front (RPF) in 1987. In 1990, RPF launched armed liberation struggle, which witnessed ousting of the dictatorship in 1994. In July 1994, Government of National Unity was formed; Major General Paul Kagame became the President in 2000 after the Parliament had voted out President Pasteur Bizimungu. In 2003, Paul Kagame was elected President for seven years and was re-elected in 2010 and 2017.

Rwanda joined the EAC in July 2009 and has since taken some steps in harmonizing her laws in line with the EAC framework. The steps include formulating policies and strategies, enacting various laws and establishing relevant institutions.68

4.2 Data Collection

Field data for Rwanda was collected between March and April, 2019. The respondent institutions visited include: Rwanda Law Reform Commission (RLRC), Rwanda Investigation Bureau (RIB), National Public Prosecution Bureau (NPPB) and the Ministry of Information, Communications Technology and Innovation (MINICT). These institutions are established by the Government of Rwanda to coordinate and regulate the ICT infrastructure, including issues related to cyber-security, at national and regional level.

Rwanda has made some developments as far as information and communication technology is concerned, especially in terms of policies, laws, plans and strategies. According to the National ICT Strategy and

68 Examples of laws include Law No. 4 of 2013 Relating to Access to Information, Law No. 24 of 2016 Governing Information and Communication Technologies, Law No. 2 of 2013 Regulating Media and Regulation No. 2 of 2018 on Cyber Security. Institutions include, for example, Ministry of ICT and Innovation, National Cyber-Security Authority, Rwanda Development Board, Rwanda Investigation Bureau and Rwanda Information Society Authority. Policies include, for example, National Cyber-Security Policy, National Data Revolution Policy, National Broadband Policy and National Digital Talent Policy.
Plan 2015, Rwanda has integrated ICT as a key driver in socio-economic development. The National Information and Communication Infrastructure Plan aims at achieving the following, among other strategies: (i) to transform Rwanda into an IT-literate nation; (ii) to promote and encourage utilization of ICT in society; (iii) to improve efficiency in public and civil service; (iv) to develop Rwanda’s information and communication infrastructure; (v) to make Rwanda a regional ICT hub; (vi) to transform the educational system by using ICT; and (vii) to develop ICT’s legal, institutional and infrastructure framework.

4.3 Background to Information and Communication Technology (ICT) Policy, Legal and Institutional Framework in Rwanda

The development of ICT policy, legal and institutional framework in Rwanda can be analyzed from the lens of the country’s Vision 2020 and the EAC Draft Legal Framework for Cyberlaws 2008.

The overall objective of Vision 2020 is to transform Rwanda into a middle-income country by 2020; and this will require achieving per capita income of USD 1240, poverty rate of 20% and average life expectancy of 66 years. Specific objectives include: (i) macroeconomic stability and wealth creation to reduce donor dependency; (ii) structural and economic transformation; and (iii) creating a productive middle class and fostering entrepreneurship. ICT is recognized as a cross-cutting issue and to that effect, the Government of Rwanda commits itself to continuing investing in developing adequate and highly skilled scientists and technicians.

---

71 Ibid., p. 6.
72 Ibid.
73 Ibid., pp. 6-7.
74 Ibid., p.8.
75 Ibid., p.17.
In the context of harmonization of cyberlaws, the Draft EAC Legal Framework is the most relevant as it provides for areas of harmonization. These include: (i) electronic transactions;  
(ii) electronic signatures; (iii) cybercrime; (iv) consumer protection; and (v) data protection and privacy. The next section looks at how far Rwanda has gone in putting in place relevant policies, laws and institutions in its endeavour to harmonize cyberlaws in line with the EAC framework and Vision 2020.

4.4 Cyber Policy, Legislative and Institutional Framework

4.4.1 Policy Framework

Rwanda has had a number of policies for purposes of boosting the ICT sector in general and cyber related issues in particular. According to the 2015 National ICT Strategy and Plan, emphasis is on five key areas, namely, skills development, private sector development, community development, E-Government and Cyber-Security. On cyber-security, the mission is to secure Rwanda’s cyberspace and information assets. Consequently, the Plan aims at achieving the following objectives: (i) to develop cyber-security awareness; (ii) to build cyber-security capabilities; (iii) to protect critical infrastructure and systems against cyber-attacks; (iv) to foster national and international cooperation in handling cybercrimes and threats; and (v) to improve legal and regulatory environment for purposes of supporting cyber-security.

77Ibid., pp. 13 -14.
78Ibid., pp. 14 – 16.
79Ibid., pp. 16 – 17.
80Ibid., pp. 17 – 18.
82Ibid., p. 7.
83Ibid., p. 25.
84Ibid.
85Ibid.
86Ibid.
87Ibid.
It has been established that there are other policies which are currently being developed. These include: (i) Draft E-Waste Policy 2012; (ii) Draft Postal Sector Policy 2013; (iii) Draft Open Data Policy; and (iv) Draft Data Revolution Policy.

4.4.2 Legal Framework

4.4.2.1 Law Governing Information and Communication Technologies\(^{88}\)

According to article 2, this law covers four sectors, namely electronic communications, information society, postal services and broadcasting. Each of these sectors is regulated in terms of licensing requirements, duty to observe conditions of licence, supervisory powers of regulatory authorities, offences and penalties. For example, as far as the telecommunications sector is concerned, there are three types of licence, namely, individual licences, standard licences and standard authorizations.\(^{89}\) In line with article 40, there are four categories of licensees or operators; these are network infrastructure licensees, network service licensees, application service licensees and content service licensees.

The Law provides principles of consumer protection in respect of electronic communications service providers. According to article 117, the principles are: (i) in case of doubt, the law must be interpreted in favour of consumers; (ii) agreements are binding only between parties thereto; and (iii) the electronic communication service licensee can only satisfy users. Other provisions relate to information society;\(^{90}\) broadcasting;\(^{91}\) and postal services.\(^{92}\)

\(^{88}\)Law No. 24 of 2016.
\(^{89}\)Ibid., article 39.
\(^{90}\)Ibid., articles 129 – 223.
\(^{91}\)Ibid., articles 224 – 264.
\(^{92}\)Ibid., articles 235 – 264.
4.4.2.2 Law Regulating Media\textsuperscript{93}

The purpose and scope of the Law is to determine rights, obligations, organization and functioning of the media in Rwanda.\textsuperscript{94} Article 2(10) defines the term media to include the internet, hence the relationship between this law and cyberspace issues. Moreover, the law has provisions relating to the internet based media. According to article 19, every person has the right to receive, disseminate or send information through internet. This right extends to creating websites and dissemination of information through the internet does not require the sender to be a professional journalist.

4.2.2.3 Law Establishing the National Cyber Security Authority and Determining its Mission, Organization and Functioning\textsuperscript{95}

This law establishes the National Cyber Security Authority (NCSA) for purposes of securing cyber-security in the Republic of Rwanda. According to article 10, NCSA is given powers to, among others: (i) set guidelines and standards for cyberspace protection and ICT security in public and private institutions; (ii) carry out audits of critical information infrastructure, cyber-systems and networks; (iii) investigate any cyber-threat, take preventive actions and collaborate with other organs to fight cybercrime which poses a threat to national security; (iv) conduct cyber-security operations; and (v) put in place mechanisms for sharing information on cyber threats or cyber-attacks.

\textsuperscript{93} Law No. 2 of 2013.
\textsuperscript{94} Ibid., article 1.
\textsuperscript{95} Law No. 26 of 2017.
4.2.2.4 Law Establishing Rwanda Information Society Authority and Determining its Mission, Organization and Functioning

The purpose of this law is to establish Rwanda Information Society Authority (RISA) and vest it with mandate, responsibilities and functions. According to article 8, RISA is composed of two management organs, the Board of Directors and the Chief Executive. The Board is the overall policy and decision maker while the Executive oversees day to day management issues.

4.2.2.5 Law Relating to Electronic Messages, Electronic Signatures and Electronic Transactions

According to article 1, the Law governs electronic transactions, electronic messages and prevention of misuse of computers. It has detailed provisions regulating electronic messages; electronic signatures; consumer protection; electronic transactions; and cybercrime and computer misuse.

4.4.3 Institutional Framework

4.4.3.1 Rwanda Information Society Authority (RISA)

Law No. 2 of 2017 with the mandate to plan and coordinate the implementation of the National ICT for Development Agenda establishes RISA. The ultimate goal is to digitize government services

---

96 Law No. 2 of 2017.
97 On RISA’s functions, see paragraph 2.3.1 of the Report/Paper.
98 Law No. 18 of 2010.
99 Ibid., articles 3 – 7.
100 Ibid., articles 20 – 50.
101 Ibid., articles 51- 57.
102 Ibid., articles 72 – 77.
103 Ibid., articles 58 – 65.
and ensure easy access by citizens.\textsuperscript{104} The specific functions of RISA include:\textsuperscript{105}

- Implementation of ICT policies and programmes for purposes of fast-tracking socio-economic growth
- Implementation of strategies that increase access and affordability of ICT
- Accelerating community development through mainstreaming ICT in national socio-economic sectors
- Preparation and coordination of programmes that increase the required skills in ICT in order to achieve a knowledge-based economy
- Strengthening programmes on ICT innovation
- Coordination of implementation of projects which deliver ICT services and
- Cooperating and collaborating with regional and international institutions with similar functions

4.4.3.2 The National Cyber Security Authority (NCSA)

NCSA is established under article 3 of Law No. 26 of 2017 as a financially and administratively autonomous public institution.\textsuperscript{106} Among other responsibilities, NCSA is required to:

- Advise the President of Rwanda and other public and private institutions on strategies to defend Rwanda’s interests in cyberspace
- Conduct cyber intelligence and come up with relevant information
- Establish guidelines on ICT security principles
- Coordinate and implement the national ICT security policies and strategies
- Develop strategies to secure all electronic operations
- Monitor all national ICT security programmes

\textsuperscript{105} Ibid.
\textsuperscript{106} Law No. 26 of 2017, \textit{op cit.}, article 8.
• Prevent cyber attacks
• Develop national cyber security educational programmes and
• Cooperate and collaborate with regional and international institutions in charge of cyber security

4.4.3.3 Rwanda Utilities Regulatory Authority (RURA)

RURA is established under article 1 of the Law Establishing Rwanda Utilities Regulatory Authority and determining its mission, powers, organization and functioning.\textsuperscript{107} According to article 2 of the Law, relevant regulated public utilities include telecommunications, information technology, converging electronic technologies, audiovisual information and postal services. In line with article 6 of the Law, RURA has powers to:
• Carry out investigations at service delivery sites
• Impose administrative sanctions for non-compliance with the law
• Settle and facilitate settlement of disputes and
• Issue directives to regulated service providers

4.5 Field Findings and Analysis

Rwanda as one of the EAC Member States was subject to this research. The following institutions were targeted for the purpose of field research: Rwanda Law Reform Commission (RLRC), Rwanda Investigation Bureau (RIB) and the National Public Prosecution Authority (NPPA). During field visits, a necessity to expand the list of the targeted institutions emerged due to the fact that the link of mandates among the targeted institutions became inevitable. Therefore, the Ministry of ICT and Innovation (MINICT) was added to the list of the targeted institutions for the research.

\textsuperscript{107} Law No. 9 of 2013.
4.5.1 Challenges during Field Visits

Due to some challenges encountered in the field, some of the above-mentioned institutions could not be visited before lapse of the time limit prescribed in the terms of reference for the research assistants. Some challenges encountered were:

4.5.1.1 Bureaucracy in the Institutions

The targeted institutions reacted differently in accepting the request to conduct research in their premises. The Rwanda Law Reform Commission and the Ministry of ICT and Innovation reacted immediately and positively in the sense that having received the request to conduct a research therein, no conditions were imposed. The research assistant was directed to the right respondents who offered information needed.\(^{108}\) Differently, RIB and NPPA conditioned a research permit from the Ministry of Justice which directed the research assistant to the National Institute of Statistics of Rwanda (NISR) for the same permit. This prolonged procedure has negatively affected the researcher’s timeline. In this context, no data was obtained from the Rwanda Investigation Bureau and the National Public Prosecution Authority.

4.5.1.2 Suspension of Services in Public Offices

Between 07\(^{\text{th}}\) and 14\(^{\text{th}}\) April, 2019, the research assistant was circumstantially obliged to suspend his schedule and resume later after lapse of the period for commemoration of the 1994 genocide against Tutsi in Rwanda. During this period, all administrative offices visited

---

\(^{108}\) These were DUSHIMIMANA Lambert, Head of Legislative Drafting & Translation Department (Tel: (+250) 0788837063 Email: lambert.dishimimana@rlrc.gov.rw) and NGENZI Octave, Business Law Research & Reform specialist (Currently acting as Criminal Law Reform Specialist) - Tel: +25 0783347887 Email: octave.ngenzi@rlrc.gov.rw ) were interviewed at the Rwanda Law Reform Commission and MUKIZA Edwin, Legal Advisor, (Tel: +250781852091 Email: emukiza@minict.govrw) was interviewed from the Ministry of ICT and Innovation
were in focus of the commemoration activities. In view of this Chapter contains information from the RLRC and MINICT only.

4.5.2 Institutions Visited: An Overview

4.5.2.1 The Rwanda Law Reform Commission (RLRC)

As provided by article 1 of the Law No 35/2014, the overall and permanent mission of RLRC is to review Rwandan laws with a view to ensuring their development and reform. In particular, the RLRC is responsible for:

i) Analysing Rwandan laws and providing recommendations to relevant institutions for their improvement, updating and reform;

ii) Conducting studies designed to assess laws in force in the country in order to identifying those that are not implemented, suggesting the new ones that are necessary and advise relevant institutions accordingly;

iii) Identifying laws provided for under the Constitution that are not yet put in place and preparing related draft bills;

iv) Identifying national laws in force to be harmonized with principles that are provided for under international instruments ratified by Rwanda.

Considering the role played by the RLRC this institution was found relevant for this research in Rwanda.

4.5.2.2 The Ministry of ICT and Innovation (MINICT)

The Ministry of Information Communication Technology and Innovation in Rwanda, has a mission of addressing national priorities for economic growth and poverty reduction through development and coordination of national information technology, communication,

---

innovation policies and programs as well as citizen’s empowerment. The ICT programmes coordination is in the hands of the Ministry in partnership with the monitoring agencies including Rwanda Development Board (RDB); Rwanda Utility Regulatory Authority (RURA); the Postal Services; and the Rwanda Information Society Authority (RISA). The National Cyber Security Authority (NCSA) is also intended to be a partner in these efforts except that it is not yet in place. The Ministry’s coordinating and monitoring role in ICT development programs make it a critical stakeholder for this study.

4.5.3 Data Analysis

4.5.3.1 Main Challenges in Addressing Cybercrimes in Rwanda

From the Rwanda Law Reform Commission, the main challenges were identified to be inadequate information and technology infrastructures in the country and existence of the non-skilled personnel especially with regard to cyber-attacks prevention.

From the Ministry of ICT and Innovation, main challenges in relation to addressing cybercrimes in Rwanda were said to be:

(i) less experience in combating cyber-attacks and crimes by the designated officers;
(ii) Insufficient financial means to materialize the NCSA that is supposed to highly contribute to strengthening the safety of Cyber environment in Rwanda; and
(iii) High costs to hire skilled workers with knowledge on cyber security.

4.5.3.2 Specific Challenges Related to Laws, Policies and Institutions

It was addressed that Rwanda has made remarkable steps in terms of policy and legal framework on cyber-security. Different laws and
policies have been put in place with the purpose of regulating such sector. However, institutional challenges are highly manifested.\textsuperscript{110}

(a) Legal Framework

As far as the legal framework is concerned, the non-existence of the law on cybercrimes used to be a challenge in Rwanda. The Penal Code of 2012 does not extensively address issues related to cybercrimes, as such criminality was not revealing itself widely in the country. Following the revision of the Rwandan Constitution in 2015, mandate to have criminal and sanction provisions was given to laws other than the Penal Code. In that regard, the Law n° 60/2018 of 22/8/2018 on Prevention and Punishment of Cyber Crimes was enacted and responded to the said challenge as the rate of cybercrimes in Rwanda was mounting.\textsuperscript{111}

(b) Institutional Framework

As far as institutional framework is concerned, the following were identified to be the most pressing challenges:

(i) Non-Operation of the NSCA

The fact that the NCSA is not yet materialized remains a challenge in Rwanda. NCSA, an institution established by Law no 26/2017 of 31/05/2017 to mainly deal with cyber-intelligence on any national security threat on cyberspace; establishment of guidelines based on national, regional and international ICT security principles; implementation and monitoring of the national ICT security policy and strategy; prevention of cyber-attacks, in cooperation with regional and international organs in charge of cyber security has remained only in

\textsuperscript{110} Interview with NGENZI Octave, Business Law Research & Reform specialist (Currently acting as Criminal Law Reform Specialist) on 14\textsuperscript{th}March, 2019 at the Rwanda Law Reform Commission.

\textsuperscript{111} Ibid.
papers. This is quite an institutional setback in curbing cybercrimes in Rwanda as NCSA’s functions are on hold.\textsuperscript{112}

(ii) Shortage of Skilled Personnel

This was identified to be yet another institutional challenge. Reference was made to the failure to launch the NCSA. It was said that part of the reason for such failure is through shortage of enough skilled personnel to perform the work that has been mandated institution.\textsuperscript{113}

(iii) Lack of Sufficient Funding

Again, the NCSA, an institution, which was legally established in 2017 with mandate to enforce cyber-security measures, is still in papers due to the lack of financial means. This was said to be a loophole in terms of enforcement.\textsuperscript{114}

(c) Policy Framework

Policy framework in Rwanda has no remarkable challenge. There is sufficient policy on cybercrimes in the country as noted later below.\textsuperscript{115}

4.5.3.3 Challenges in Different Fora

It was argued by the Rwanda Law Reform Commission that the Ministry of ICT could better address issues of addressing challenges in different fora because, the RLRC’s duty is mainly to provide recommendations to relevant institutions for the improvement, updating and reform of laws of their concern. At the Ministry of ICT and Innovation, it was noted that at the national level, the fora of discussions between partner agencies (RDB, RURA, RISA, and the

\textsuperscript{112} Ibid, note 16.
\textsuperscript{113} Interview with MUKIZA Edwin, Legal Advisor, the Ministry of ICT and Innovation, 27\textsuperscript{th} March, 2019 at the Ministry of ICT and Innovation.
\textsuperscript{114} Ibid.
\textsuperscript{115} Mr. NGENZI Octave, Rwanda Law Reform Commission, Supra.
Postal Services) are always arranged. On the regional and international level, Rwanda usually participates in all arranged fora.

**4.5.4 Initiatives at EAC Level**

Respondents at the Rwanda Law Reform Commission elucidated that it does not in particular see any practical initiative at the Community level until today, apart from the regional vision of having a harmonized cyber-security framework. However, as an institution, the RLRC has an agent specifically in charge of EAC obligations compliance (focal person) internally.

The Ministry of ICT and Innovation commented that the EAC initiative to come up with a harmonized cyber-framework within the region is known to the Ministry. It was added that, this sounds as a good starting point and the Ministry has played a key role in performing Rwanda’s related obligation.

**4.5.5 Challenges and Workers’ Rights in Institutions**

It was expounded from the Rwanda Law Reform Commission that generally, all the partner agencies in the technology sector are aware of the said challenges in the country. As to the (RLRC), the recommendations are made basing on the researches’ findings especially with regard to legal framework. As to the workers, no workers’ rights are affected; rather the RLCR’s commitment is to see such workers grow in skills to fight cybercrimes in the country.

From the Ministry of ICT and Innovation, it was explained that the challenges are addressed by:

i) The Government of Rwanda hiring skilled workers to cover the cyberspace skills’ gap.
ii) The Government of Rwanda through the MINICT in cooperation with foreigner partners arranging trainings of its personnel with the purpose of to rising up their skills.

iii) The Government of Rwanda engaging in the process of ratifying the African Union Convention on Cyber Security and Personal Data Protection of June 2014. The Ministry in charge had already received the final report from the MINICT recommending such ratification at the time of writing. The ratification of this regional Convention is expected to connect Rwanda to the African cybersecurity framework.

iv) The General Data Protection Regulation (GDPR) is also being looked at by the MINICT to verify its applicability in Rwanda with purpose to welcoming foreign investment.

v) Initiatives relating to development of the National ICT Strategy and plan in Rwanda was outlined in a Phases approach to achieving Vision 2020 through ICT as follows:

- a) Phase I (2000-2005) focused on creation of an enabling institutional, legal and regulatory environment for ICT development;
- b) Phase II (NICT I-2010) concentrated on development of critical national ICT infrastructure;
- c) Phase III (2011-2015) is focused on leveraging the existing infrastructure and environment to improve service delivery to Rwandans.

### 4.5.6 Cybercrime Challenges and Attaining EAC Objectives and Goals

From the Rwanda Law Reform Commission, it was elucidated that, as long as each of the EAC Member keeps concentrating on its programs as individual States, it will take more time to overcome challenges and
it may even be impossible to achieve the needed security in the regional cyberspace. The respondent added that, it is good to note that the cyber insecurity is a big challenge to the financial projects. The high expenses to hire skilled workers and even to hire the information control centres from the developed countries have negative implications to the EAC Member countries’ budgets which are already insufficient. He concluded by posing the question: how can the Community reach its objectives if members are operating with deficit budgets?

4.5.7 Role of Visited Institutions

The respondent at the Rwanda Law Reform Commission responded that, for the problem to be addressed, it first of all has to be identified. Such identification involves issues of research. He noted that generally more of the RLRC workers (including himself) are vested with the mandate to conduct research especially targeting the need of enacting a certain law, compliance of the enacted law, impact of the existing laws as well as their amendment or repeal if need be. He explained that this is the role he plays in his institution as long as the mandate does not change.

From the Ministry of ICT and Innovation, the respondent explained his role in such institution as a legal advisor is to intervene in the context of laws. He added, it is good to note that the political situation is the one driving everything in the country; therefore, his role sometimes may be limited especially in the context of the EAC agenda.116

4.5.8 Specific Programs/Interventions

The RLRC elucidated that it has played a big role in programmes aimed at addressing identified challenges as follows:

116 Mr. MUKIZA Edwin, Supra, Note 96.
i) Contributing to the enactment of the Law nº 60/2018 of 22/8/2018 on Prevention and Punishment of Cyber Crimes; and that; after two (2) years in force, such institution shall conduct an impact assessment on cyber criminality.

ii) Participating in the draft of the Presidential Order determining mechanisms to protect Critical Information Infrastructures (CII Presidential Order) which is also in process in the RLRC.

As to the Ministry of the MINICT, it was disclosed that:

i) The Ministry has been in control of the challenge of low skilled personnel;

ii) It deals with establishment of equipped institutions;

iii) The Ministry has been working to ensure availability of the financial means to ICT initiatives that are being introduced;

iv) It establishes cooperation with various stakeholders to train personnel for example; at the time of the visit, some of members of MNICT team were in Japan for a four-months training in combating cyber-attacks in cyberspace;

v) It works to promoting the foreign investment in the technology sector; and

vi) It has joined regional arrangements to build a secured cyberspace in Rwanda.

4.5.9 Relevance and Effectiveness of the Strategies

RLRC explained that, the existing legal framework on cyber security in Rwanda is of relevance in regulating the institutional framework. The MINICT commented that; the strategy to ratify the African Convention on Cyber Security is relevant to fight cybercrimes in Rwanda. The Ministry believes that, Rwanda may be the first EAC country to ratify
such a Convention and may act as a role model to the rest of the EAC countries.

The RLRC mentioned that, it couldn't say satisfactorily that the legal, institutional and policy frameworks adopted in Rwanda are sufficient as the cybercrimes problem in the country is yet to be totally eliminated. The Commission suggests temporary solutions to the challenges like the ongoing hiring of the skilled personnel (foreign workers to train the Rwandese personnel on issues related to cyber security). However, the RLRC believes that the EAC regional commitment to address such challenge of low skills could work better and faster if adopted. This implies the exchange of medium skilled workers that some of the Member countries may have today; the exchange of information on cyber-related criminality through the regionally organized forums and even the commonly prepared trainings. Establishment of regional research centres was also suggested as a positive tool.

The MNICT had the view that one cannot say that the adopted measures are enough while the technology keeps developing. It was explained that one of the effective measure to be adopted by the MINICT with its Partner Agencies should be extensive and timely research on how well problems related to cyber security in the country may be tackled at the national or regional level. It is believed that in research is where the country can find most of the possible solutions to the problem.

4.5.10 Legislation, Policies and Institutional Framework

Respondents noted that the RLRC takes a big part in the preparation and drafting process of laws including those related to cyber-security. Also, the findings of the researches conducted by the RLRC are based in preparing various policies.
4.5.10.1 Legislation

It was explained the main pieces of legislation relating to cyber-security in Rwanda are:

i) Law n° 24/2016 of 18/06/2016 governing Information and Communication Technologies;

ii) Law n° 02/2013 of 08/02/2013 regulating Media;

iii) Law n° 04/2013 of 08/02/2013 relating to Access to Information;

iv) Law nº 60/2018 of 22/8/2018 on Prevention and Punishment of Cyber Crimes; and

v) Regulation no 02/2018 of 24/01/2018 on Cyber Security.

4.5.10.2 Policies

With regard to policy framework, the following were identified as the relevant policies on cyber-security so far developed in Rwanda:

i) The National Cyber Security Policy 2015;

ii) The National Data Revolution Policy 2017;

iii) The National Broadband Policy 2013; and


It was further hinted that other policies such as the e-waste policy and the Data protection policy are still under the drafting process.

4.5.10.3 Institutions

At the Ministry of ICT and Innovation, the interviewee mentioned a list of institutions dealing with cyber-security in Rwanda to be:

i) Ministry of ICT and Innovation
ii) National Bank of Rwanda/Central Bank
iii) National Cyber Security Authority
iv) National Institute of Statistics of Rwanda
v) National Public Procurement Authority
vi) Rwanda Development Board
vii) Rwanda Investigation Bureau
viii) Rwanda Information Society Authority
ix) Rwanda Law Reform Commission
x) Rwanda Utility Regulatory Authority

4.5.11 Adequacy of Measures

The RLRC was of the view that comparing to the situation in Rwanda in previous years, there is a remarkable development. Today, there are clear legal provisions and institutions of enforcement to curb cybercrimes in Rwanda. However, there is still a need for efficient equipment mostly in the relevant institutions with the skilled personnel to combat/prevent cyber-related attacks.

The Ministry of ICT and Innovation commented that the measures taken to overcome challenges related to cybercrimes in Rwanda are not well equipped to combat cybercrimes in Rwanda. It was argued that the human capital is still not skilled enough in the relevant institutions. Also, the NCSA, which only exist on paper, was expected to do much on cyber-security agenda in Rwanda. The legal framework also still needs some adjustments, update and reform to absolutely deal with the cybercrimes problem. This is explains why the laws and policies in Rwanda are continuously made and reviewed from time to time to enable the legal framework in Rwanda to fully address issues relating to cyber-security. It was pointed out that a data protection law
and the Presidential Order determining critical information infrastructures and modalities of their protection were in the pipeline, in the drafting process. Also, there is a national data centre established to collaborate with the RISA in Data protection.

4.5.12 Addressing Challenges

From the RLRC, the most appropriate way of addressing challenges was having a common initiative to exchange information, common cyber-related infrastructures and exchange of skilled workers at the EAC level. Most of all, harmonization of cyberlaws was pointed out to be one of the most appropriate way to address cyber-security challenges not only in Rwanda, but also in the EAC region at large.

The Ministry of ICT and Innovation had the opinion that finding immediate alternatives to the existing challenges can be the most appropriate way to solve cyber security challenges in Rwanda. For example, the country’s move to grant RISA temporary mandate to perform responsibilities of NCSA has been hailed as a commendable move to tackle problems associated with non-functioning of the NCSA on time. The RLRC also suggested continual training of personnel in the relevant institutions on cybercrimes issues, together with the increase of resources for conducting research.

The Ministry of ICT and Innovation was of the view that, the best way to deal with the problem is already applied by having a full package of policies and laws, as well as the capacity building strategies such as trainings and hiring skilled workers in the country.

4.5.13 Effectiveness of EAC Intervention Programmes

It was noted at the RLRC that intervention programmes adopted by the EAC States are currently not sufficient. It was recommended that there is a need for EAC to put in place regional research institutions and centres, arrangement of common forums to share knowledge on
challenges and to work on common solutions. It was further recommended that the Community should have serious implementing and monitoring organs.

At the Ministry of ICT and Innovation, it was hinted that the lack of political will in the EAC is still a dysfunctional factor for the organs of the EAC. The recommendation was therefore made that there be established a clear process to share views between enforcing institutions among Members of the Community with the intent to come up with the same image on the cyber-security on skills, infrastructures, and or legal/institutional frameworks. It was also recommended that there is a need to ratify African and other international instruments on cyber-security with purpose to globalize the efforts.

4.6 Conclusion

Based on the Draft East African Community Legal Framework for Cyberlaws, it is concluded that Rwanda has in place relevant cyberlaws covering almost all envisaged areas, namely, electronic transactions, electronic signatures, computer crime, consumer protection and data protection. These areas are covered either by standalone pieces of legislation or as part of laws dealing with other issues.

Field data indicate that the visited institutions believe that Rwanda has reached far in implementing its obligation vis-a-vis the EAC cyberlaws harmonization requirement. However, there are still challenges both to have a full and equipped legal and institutional framework, and to have such framework in line with other EAC Partner frameworks. Such challenges include: the inadequate information and technology infrastructures; the non-skilled personnel especially with regard to cyber-attacks prevention; and the non-operational of the NCSA, an institution established by the Law no 26/2017 of 31/05/2017 to deal with cyber-intelligence on any national security threat in cyberspace. Also, the reluctance and variable speed of EAC Members in the harmonization exercise poses a challenge.
4.7 Recommendations

Having made the above observations, the following recommendations are pertinent to Rwanda:

(i) Generally, there is a need of capacity building together with modern infrastructures of technology;

(ii) There is a need to increase research centres and institutions;

(iii) Sensitization of people to increase knowledge of society on the cyber-attacks and crimes as the information technology is developing fast;

(iv) Development of research on cyber security in the region can help to identify the shared challenges and develop collective ways of overcoming the same; and

(v) Timely update of the legal and institutional framework as the ICT world is evolving day by day.
CHAPTER FIVE

HARMONIZATION OF THE CYBERCRIMES LEGAL FRAMEWORK IN TANZANIA

Baraka Francisco Kanyabuhinya

5.1 Introduction

This Chapter makes an analysis of the state of affairs relating to cyber security in Tanzania Mainland. However, it is predominately based on literature review and provides a backdrop for the final Chapter by putting in place the underlying position in the EAC relating to critical issues on this subject.

The United Republic of Tanzania (hereinafter to be referred to as Tanzania) is a union formed by merging two sovereign States of Tanganyika and Zanzibar in 1964. The union is very unique in terms of its structure and sharing of powers between the two former States that form part of the unification.

Eight countries border Tanzania. It is surrounded by the Indian Ocean on the East while on the North she is bordered by Kenya and Uganda. On the West, she is bordered by Rwanda and Burundi, Democratic Republic of Congo (separated by Lake Tanganyika) and Zambia. On the South there are Mozambique and Malawi.

It is worth noting that although, the United Republic of Tanzania is recognized under international arena as one sovereign State, but legal matters are seldom shared. Under the Articles of the Union, legal matters are treated as non-union with few exceptions. Whereas some national portfolios like defense, finance and internal affairs are union matters, implying that the Government of the United Republic of Tanzania centrally handles them; cybercrimes legislation is not entirely applicable in Zanzibar. Save for the issue of compounding offences,
the law regulating cybercrimes is applicable to Mainland Tanzania as well as Tanzania Zanzibar.\textsuperscript{117}

Tanzania follows the Common Law legal system. This fact has a historical explanation as both Mainland Tanzania and Zanzibar got independence from the same colonial master (Great Britain), hence inherited her legal system.

The court system is also not considered to be part of the union matters. Mainland Tanzania has its own courts as Zanzibar also does. The only court that is seen as a creature of the statute is the Court of Appeal of Tanzania. It has the jurisdiction to hear appeals from the High Courts of both parts of the Union (Mainland Tanzania and Zanzibar).\textsuperscript{118}

Laws are enacted by the Legislatures of both parts of the union. The Parliament of the United Republic of Tanzania is responsible to legislate on union matters and non-union matters applicable in Mainland Tanzania.\textsuperscript{119} On the other hand, the House of Representatives of Zanzibar is charged with enacting laws that are applicable in Zanzibar.

The main notable disquiet concerning the Parliament of Tanzania when exercising her legislative powers is what appears now to be a custom; that is, passing legislation swiftly under the auspice of "certificate of urgency". The House with majority Members of Parliament (MPs) from the ruling part "Chama Cha Mapinduzi", has, in some sessions, passed laws, which are thereafter condemned to be draconic. The current Cybercrimes Act of 2015 is a typical example of such laws and it has received surmountable criticisms for violating individuals’ freedom of

\textsuperscript{117} Save for section 50, this Act shall apply to Mainland Tanzania as well as Tanzania Zanzibar (Section 2 of the Cybercrimes Act, 2015).

\textsuperscript{118} Article 116 of the Constitution of the United Republic of Tanzania (Cap. 2 RE. 20012).

expression, right to privacy and generally suppressing the due process of the law.

Furthermore, more critics are of the view that the provisions of the Act create a room for law enforcers to abuse their power during investigation. The law, for example, provides that where disclosure of data is required for purposes of criminal investigation or the prosecution of an offence, a police officer in charge of a police station or a law enforcement officer of a similar rank may issue an order to any person in possession of such data compelling him to disclose such data. At least, such order should have been made possible under an order of the Court.

5.2 Tanzania in the EAC

Tanzania is one of the founder Partner States in the establishment of the EAC. The Treaty for the Establishment of the EAC states, *inter alia*: “Contracting Parties” means the Republic of Uganda, the Republic of Kenya and the United Republic of Tanzania. Also, the Treaty defines “Partner States” as the Republic of Uganda, the Republic of Kenya and the United Republic of Tanzania and any other country granted membership to the Community under Article 3 of this Treaty. Thus, at a regional (EAC) juncture, it is worth noting that the United Republic of Tanzania is deemed as one sovereign State, consequently rendering Zanzibar not to feature as a Partner State in any regional integration fora.

As the EAC’s Partner State, Tanzania is duty-bound to observe article 126 (2) (b) and article 47 of the Common Market Protocol, both call for States to harmonize all their national laws appertaining to the

---

120 Section 32 of the Cybercrimes Act, 2015.
122 Article 1 of the Treaty for the Establishment the EAC.
Community. It is with this spirit that the Law Reform Commission of Tanzania has been participating in numerous East African Community meetings especially those aiming at approximation and harmonization, and meetings aimed to review EAC laws to be in line with the East African Community Agreements. As of now, Member States have already harmonized laws in the following areas: company laws, bankruptcy laws, immigration laws, contract laws and sale of goods laws. The EAC Competition Act has also been enacted and Member States are in the process of aligning their national competition laws to the Act. Moreover, laws, which do not comply with the East African Common Market Protocol, have been identified and Members have been required to harmonize them accordingly. Thus, Tanzania as the EAC’s Member State is obliged to undertake deliberate efforts in ensuring that the region has a harmonized legal regime in combating cybercrimes.

5.3 ICT Development and the Rate of Cybercrimes

Tanzania, like any other country found herself caught in the web of computers’ use and proliferating internet connections rendering to commission of new forms of offences, namely cybercrimes. Literature suggests that Internet availability and use has been in place since the 1990s. Surveys indicate that the usage of ICT has been slow and gradual due to a number of reasons, mainly due to inadequate power supply, especially in rural areas. In 2005, only 2 percent of Tanzanian households had a working computer with an Internet connection. These households were all located in urban areas.

---

125 Ibid.
126 Ibid.
128 Ibid.
129 Ibid.
Recent reports, however, indicate that internet users in Tanzania have risen by 16 percent at the end of 2017 to 23 million, with the majority of those using their handsets to go online.\textsuperscript{130} The Reuters report states further that mobile phone use has surged in Tanzania and other African countries over the past decade, helped by the launch of cheaper smart phones and data services.\textsuperscript{131}

Major mobile phone operators in Tanzania include Vodacom Tanzania, a unit of South Africa’s Vodacom; Tigo Tanzania, which is part of Sweden’s Millicom; Bharti Airtel Tanzania; and Halotel, owned by Vietnam-based telecoms operator Viettel.\textsuperscript{132} In a nutshell, Tanzania has liberalized the communications and broadcasting sector in order, among other things, to attract investment and increase competition.

While the use of ICT in Tanzania dates a way back in 1990s, it was until in 2015 that specific laws aimed at combating cybercrimes and related electronic transactions wrongs were enacted. This was in order to address the looming cyber-associated offences in particular: computer frauds, cyber-bullying, spam and other forms of cyber-attacks.\textsuperscript{133}

Incidences of cybercrimes occurring in Tanzania have rapidly increased. The Tanzania Cybercrimes Report 2016, has highlighted the following common cyber-attacks frequently occurring in Tanzania and the likely contributing factors: numerous attacks on mobile money through social engineering; use of malware and account personifications; numerous attacks through social engineering; use of malware and account impersonations; malware targeting critical mobile and internet banking infrastructure are on the rise; numerous counts of vulnerabilities and systems misconfigurations; lack of practical

\textsuperscript{130} Tanzania Internet users hit 23 million; 82 percent go online via phones: Regulator, Available at https://www.reuters.com/article/us-tanzania-telecoms/tanzania-internet-users-hit-23-million-82-percent-go-online-via-phones-regulator-idUSKCN1G715F, accessed on 5\textsuperscript{th} December 2018.

\textsuperscript{131} Ibid.

\textsuperscript{132} Ibid.

\textsuperscript{133} Ibid.
regulatory guidance from local industry regulators and government; and technical training of employees is not sufficient and that only 3% successful prosecution.\textsuperscript{134}

The report further states that despite the increase of cybercrimes, 91\% of cybercrime cases are not reported to the police.\textsuperscript{135} Out of 9\% cases that are reported to the police, only 3\% are successfully prosecuted.\textsuperscript{136} This factual finding glues the extent of cybercrimes in Tanzania and how regulatory mechanisms have not been able to curb the mischief. It was with the understanding that Tanzania should not turn into cyber-attackers haven, that the new cyberlaws were enacted in 2015 with the aim of fighting cybercrimes.

5.4 Policy, Legal and Institutional Frameworks for ICT

Tanzania has promulgated various policies, laws and established some regulatory institutions to deal with cybercrimes and ICT infrastructure. It is worth noting that issues of ICT fall under the Ministry of Works, Transport and Communication.

In 2016, the responsible Ministry enacted the National Information and Communications Technology Policy, which among other things reviews the National ICT Policy of 2003 (NICTP 2003) and provides a comprehensive framework for guiding the development and growth of the industry to ensure optimal benefits to the nation and its citizens.\textsuperscript{137}

Another policy in place is the National Postal Policy which acknowledges the need to take measures such as the use of electronic surveillance machines which are capable of monitoring theft, violation


\textsuperscript{135} Ibid.

\textsuperscript{136} Ibid.

\textsuperscript{137} See Preface of the National Information and Communications Technology Policy (Tanzania), available at: https://tanzict.files.wordpress.com/2016/05/national-ict-policy-proofed-final-nic-review-2.pdf, accessed on 5\textsuperscript{th} December, 2018.
of postal articles and detecting some dangerous and prohibited articles sent through the post.\textsuperscript{138}

Other policies which are relevant to ICT and cybercrimes are, \textit{inter alia}: the National Telecommunications Policy of 1997, the National Information and Broadcasting Policy, 2003; Tanzania Development Vision 2025 and the National Science and Technology Policy for Tanzania. A bird’s eye view of these policies, clearly indicate that they have one thing in common, that is, improvement of telecommunication systems and ICT development.

\textbf{5.4.1 ICT Related and Cybercrime Laws}

On the other hand, having realized an increase of cybercrimes and ICT misuse especially \textit{via} social media, Tanzania embarked on enacting new laws and regulations to regulate behavior of players in the cyberspace. A list of principal legislation is as follows:

\begin{itemize}
  \item The Tanzania Communication Regulatory Authority Act, No. 12 of 2003;
  \item The Universal Communications Service Access Fund Act, No. 11 of 2006;
  \item The Evidence Act, Cap. 11 [R.E. 2002] as amended by the Written Laws (Miscellaneous Amendments) Act, No. 15 of 2007;
  \item The Electronic and Postal Communications Act, No. 3 of 2010;
  \item The Electronic Transactions Act, No. 13 of 2015;
  \item The Cybercrimes Act, No. 14 of 2015;
  \item The Access to Information Act, No. 6 of 2016;
  \item The Whistle blowers and Witness Protection Act, 2015; and
  \item The Media Service Act, No. 12 of 2015.
\end{itemize}

The Cybercrimes Act which came into force in 2015 creates a number of offences, namely: illegal access, illegal remaining, illegal interception, illegal data interference, data espionage, illegal system

\textsuperscript{138} National Postal Policy 2003, para 2.7.
interference, illegal device, computer related forgery, computer related fraud, child pornography, pornography, identity related crimes, publication of false information, racist and xenophobic material, genocide and crimes against humanity, cyber bullying, unsolicited messages and violation of intellectual property rights - to mention a few.

The Electronic Transactions Act on the other hand, aims to provide for the legal recognition of electronic transactions, e-Government services, the use of Information and Communication Technologies in collection of evidence, admissibility of electronic evidence, to provide for the facilitation of use of secure electronic signatures; and to provide for other related matters.  

The Tanzania Communication Regulatory Authority Act establishes the Tanzania Communication Regulatory Authority (TCRA), which among other things regulates the communications sector, which includes telecommunication, broadcasting and postal services. It is also mandated to monitor the implementation of ICT applications and establishing standards of the regulated goods and services.

The Electronic and Postal Communications Act provides for the enactment of electronic and postal communications law with a view to keeping abreast with developments in the electronic communications industry; creating a comprehensive regulatory regime for electronic communications service providers and postal communications service providers; and to establish the Central Equipment Identification.

There was a move to enact the law to protect privacy and a proposed Bill on Data Protection Act was prepared, however, it was never tabled before the Parliament for debate.

Apart from principal legislation, there are several delegated legislations that are made under these laws. These are, *inter alia*:

---

139 Objective clause to the Electronic Transactions Act, No. 13 of 2015.
• The Electronic and Postal Communications (Value Added Services) Regulations, 2015;
• The Electronic and Postal Communications (Electronic Communications Equipment Standards) Regulations, 2014;
• The Electronic and Postal Communications (Telecommunications Traffic Monitoring System) Regulations, 2013;
• The Electronic and Postal Communications (Quality of Service) Regulations, 2011;
• The Electronic and Postal Communications (Central Equipment Identification Registers) Regulations, 2011;
• The Electronic and Postal Communications (Digital and Other Broadcasting Networks) Regulations, 2011;
• The Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2011;
• The Electronic and Postal Communications (Competition) Regulations, 2011;
• The Electronic and Postal Communications (Tariffs) Regulations, 2011;
• The Electronic and Postal Communications (Mobile Number Portability) Regulations, 2011;
• The Electronic and Postal Communications (Postal) Regulations, 2011;
• The Electronic and Postal Communications (Radio Communications and Frequency Spectrum) Regulations, 2011;
• The Electronic and Postal Communications (Interconnection) Regulations, 2011;
• The Electronic and Postal Communications (Accounting Separation) Regulations, 2011;
• The Electronic and Postal Communications (Consumer Protection) Regulations, 2011;
• The Electronic and Postal Communications (Electronic Communication Numbering and Addressing) Regulations, 2011;
• The Electronic and Postal Communications (Access, Co-Location and Infrastructure Sharing) Regulations, 2011;
The Electronic and Postal Communications (Licensing) Regulations, 2011; and
The Tanzania Broadcasting (Content) Regulations, 2005.

Despite the fact that the enforcement of these cyberlaws and regulations has curbed some forms of cybercrimes, they have been heavily criticized for being violating civil liberties, in particular the freedom of expression. They have also been condemned as a weapon deliberately set to target politicians from the opposition faction. Some activists have gone a step further to challenge the Cybercrime Act for being unconstitutional. It is reported that in December 2016, section 50 of the Cybercrimes Act was declared by the High Court to be unconstitutional, thus the Attorney General was subsequently ordered to initiate the process of amending the section within twelve months.¹⁴⁰

In some instances, some donor States have threatened to halt their aid in a bid to pressure Tanzania to amend the Act so that it meets international standards on protection of civil liberties.¹⁴¹ Notwithstanding of the criticisms, the cybercrimes provisions remains enforceable and unscathed.

**5.4.2 Institutional Framework**

Pursuant to widespread of Internet and ICT usage in Tanzania, the Government established a specific sector regulator, in order to standardize the rules of the game and to ensure that players on the cyberspace comply with the regulatory framework. Accordingly, TCRA was established as a quasi-independent Government body responsible for regulating the communications and broadcasting sectors in


Tanzania.\textsuperscript{142} It was established under the TCRA Act No. 12 of 2003 to regulate the electronic communications, and postal services, and management of the national frequency spectrum in the United Republic of Tanzania.\textsuperscript{143} The Authority became operational on 1\textsuperscript{st} November 2003 and effectively took over the functions of the now defunct Tanzania Communications Commission (TTC) and Tanzania Broadcasting Commission (TBC) respectively.\textsuperscript{144} The vision of TCRA reads: \textit{``To be a world-class Communications Regulator creating a level playing field among Communication Service Providers, and promoting environmentally friendly, accessible and affordable services to consumers''}, whereas the mission is to \textit{``develop an effective and efficient communications regulatory framework, promote efficiency among the Communications Services Providers, and protect consumer interests with an objective of contributing to socio-economic and technological development in the United Republic of Tanzania.''}\textsuperscript{145}

Apart from TCRA, E-Government Agency is another initiative that has been advocated by governments globally as a means to acquire efficiency, accountability, and transparency in governance.\textsuperscript{146} Sabo’s findings reveal that a major task of e-government projects is to collect and store data on various issues related to various censuses and economic data.\textsuperscript{147} Data collection exercises are initiated to collect relevant data from various locations around the country.\textsuperscript{148} The data is transferred online to the National Bureau of Statistics (NBS) headquarters for analysis and storage before dissemination.\textsuperscript{149}

\textsuperscript{142} See TCRA Profile, available at: https://www.tcra.go.tz/, accessed on 6\textsuperscript{th} December, 2018.
\textsuperscript{143} Ibid.
\textsuperscript{144} Ibid.
\textsuperscript{145} Ibid.
\textsuperscript{147} Ibid.
\textsuperscript{148} Ibid.
\textsuperscript{149} Ibid.
5.5 Challenges in Addressing Cybercrimes in Tanzania

Since the coming into force of the Cybercrimes Act in 2015, there are challenges that have blossomed that threaten achieving a harmonized EAC’s cybercrimes legislation. Most of these challenges touch the substance of the Act itself, the procedures of enforcement and the expedite process of its enactment.

5.5.1 Challenges Relating to the Substance

It has been noted that some provisions of the Cybercrimes Act appears to be violating the Constitution of the United Republic of Tanzania, in particular by limiting the freedom of expression. Breakthrough Attorneys have noted that the large percentage of the public and the opposition parties have been voicing their outcry against the enactment of the law, citing “limitation of freedom of information” as one possible vice of the impugned law.\(^{150}\)

In support of the above position, the provisions of section 16 attract much attention as most respondents expressed their view that it is widely formulated and capable of capturing anyone who posts any unverified information, in the exercise of freedom of speech. The provision reads \textit{inter alia}:

\begin{quote}
Any person who publishes information, data or facts presented in a picture, text, symbol or any other form in a computer system where such information, data or fact is false, deceptive, misleading or inaccurate commits an offence, and shall on conviction be liable to a fine not less than three million shillings or to imprisonment for a term not less than six months or to both.
\end{quote}

\(^{150}\) Breakthrough Attorneys, Cybercrimes Act 2015 Tanzania, the Challenges in the Hands of both Corporate and Individuals; available at: https://breakthroughattorneys.com/cybercrimes-act-2015-tanzania/, accessed on 26th June 2019.
The Human Rights Watch in 2019 has hinted that the 2015 Cybercrimes Act continues to impede free expression and privacy rights.\textsuperscript{151}

\section*{5.5.2. Challenges Relating to Procedure and Enforcement}

Bird’s eye view of the Act underlines the wider mandate vested with law enforcers (police officers) and the Director of Public Prosecution in enforcing the Cybercrimes Act. The Act gives wider and excessive powers to police officers when conducting search and seizure of computer system. Police officers are conferred with primary powers for implementing the wishes of the Act.\textsuperscript{152} Stakeholders on the contemplation for arbitral exercise of these powers have made critiques. The Cybercrimes Act, for instance, does not make it mandatory for the investigating police officer to seek judicial order while engaging in surveillance, and thus providing a leeway for the abuse of surveillance powers.\textsuperscript{153}

Furthermore, obtaining the data or device in custody of the law enforcement officer is in the discretion of the officer.\textsuperscript{154} The officer may agree or refuse a person access to one’s data or device that is in custody of the law enforcement officers under the Act.\textsuperscript{155}

Moreover the Act empowers the Director of Public Prosecutions to order a person to pay a sum of money specified by him but not exceeding the amount of fine prescribed for any of such offence.\textsuperscript{156}

\begin{flushright}
\textsuperscript{152} The Cybercrimes Act, 2015 sections 31-38.
\textsuperscript{153} Ibid., section 32(2).
\textsuperscript{154} Breakthrough Attorneys, Cybercrimes Act 2015 Tanzania, the Challenges in the Hands of both Corporate and Individuals; available at:\url{https://breakthroughattorneys.com/cybercrimes-act-2015-tanzania/}, accessed on 26\textsuperscript{th} June 2019.
\textsuperscript{155} Ibid.
\textsuperscript{156} The Cybercrimes Act, section 50. Activist has challenged this provision successfully in court and the High Court has advised the Government to amend the same. For more details about the case, see: \textit{Jebra Kambole vs. Attorney General}, \textit{Miscellaneous Civil Cause No. 32 of 2015, High Court of Tanzania (Main Registry) at Dar es Salaam (Unreported)}. \end{flushright}
DPP’s order in this regard is final and not appealable. This provision usurps the powers of sentencing, which is bestowed on courts of law. It also creates a room for corruption and defeats the due process principle of criminal justice.

**5.5.3 Institutional Challenges**

Some institutional challenges were noted in particular lack the institutional capacity to implement the Cybercrimes Act. Incapacity ranges from insufficient technology capabilities of the law enforcement personnel, inadequate tools for computer investigation, inadequate forensic computer investigative skills accompanied with less number of trained officers in ICT matters.

On the other end, computer crimes are difficult to investigate and establish admissible evidence before courts of law. Respondents reported that in some cases with social media such as WHATSAPP, the servers are located out of our jurisdiction, thus getting access to information through messengers of this nature needs consulting the servers hosts located in another jurisdiction.

**5.5.4 Multi-Enforcers Syndrome**

Most cybercrimes involving fraud and financial losses require inputs from various law enforcement agencies. A suspect is arrested by police force and taken into police custody for interviewing. A charge is prepared based on cooperation of various enforcement agencies such as those from Tanzania Communication Regulatory Authority (TCRA), financial crimes unit and the office of national prosecution. The multi-enforcers agencies’ trend has an effect of delaying justice as a suspect, in some instances may remain in police custody for more than two weeks.
5.6 Specific Interventions to Address the Challenges

There are different measures taken by the Government of Tanzania to curb cybercrimes. These measures includes: capacity building, public awareness creation, establishment of Cybercrime Unit in the Department of Police, international collaboration in controlling cybercrime, the use of CCTV camera around ATM locations, preparation of Cybercrime Act and find better software to detect intruders, investing in computer engineering skills along with forensic computer investigation and establishment of financial intelligence fraud plus property financial crime unit.\textsuperscript{157}

With regard to provisions that are considered as violating the freedom of speech and privacy, interventions by activists mostly challenging the same in court of law, has proved fruitful. There are some pending cases in the High Court testing the constitutionality of some provisions of the Cybercrimes Act.\textsuperscript{158}

5.7 Conclusion

Tanzania has undertaken deliberate efforts to streamline her legal framework on combating cybercrimes at a local level. Two pieces of legislation that were enacted in 2015, which are the Cybercrimes Act and the Electronic Transactions Act, mark a good start towards harmonization of cyberlaws at the EAC level.

The available literature and legislation are updated and signifies a positive move towards harmonization of the EAC cyberlaws. As noted, the cyberlaws of Tanzania, notably the Cybercrimes Act of 2015, has

\textsuperscript{157} The University of Dar es Salaam, School of Law is currently offering Cybercrimes Course for the Program of Bachelor of Arts in Law Enforcement (BALE) and as a postgraduate Course for those taking LL.M. in Corporate and Commercial Laws.

\textsuperscript{158} The High Court in \textit{Jebra Kambole vs. Attorney General} [Misc. Civil Cause No. 22 of 2018, High Court of Tanzania at Dar-es-Salaam] held for that Section 50 to be anomaly and ordered the AG within 12 Months to correct the anomaly. https://tanzlii.org/tz/judgment/high-court-tanzania/2019/6-0 (accessed: 29th November 2019)
been widely condemned for violating civil liberties. On that basis, this law is not commendable to serve as a model law in the process of approximation or harmonization. Well known regional cyberlaws such as the Budapest Convention on Cybercrimes, the first international treaty on crimes committed via the Internet and other computer networks and the SADC Model Law on Cybercrimes, should be the guiding documents in the process of harmonizing the EAC cybercrimes legislation.
CHAPTER SIX

HARMONIZATION OF THE CYBERCRIMES LEGAL FRAMEWORK IN UGANDA

Boniphace Luhende

6.1 Introduction

Uganda is a landlocked country across the equator in the Eastern Africa bordering Lake Victoria in South East. Uganda is bordered by South Sudan in North, Kenya in East, Democratic Republic of the Congo in West and by Rwanda and Tanzania in South. Uganda has an area of 241,038 square kilometers making it the third largest country in the EAC. It is estimated that as of July 2018, Uganda had a population of 40,000,000. Spoken Languages in Uganda include English (official language), Luganda (major language), Swahili and other native languages.¹⁵⁹ Uganda achieved her political independence from the British in 1962.

6.2 Uganda in the EAC

Uganda, like Tanzania and Kenya has a long history of co-operation under different regional integration arrangement during colonial and post-colonial era.¹⁶⁰ These arrangements include: the Customs Union between Kenya and Uganda in 1917, which the then Tanganyika (now Mainland Tanzania) later joined in 1927; the East African High Commission (1948-1961); the East African Common Services Organization (1961-1967); the EAC (1967-1977) and the East African Co-operation (1993-2000).¹⁶¹


After the dissolution the defunct EAC in 1977, the new EAC was revived through the signing of Treaty for the Establishment of the EAC in Arusha Tanzania on 30 November 1999. The Treaty entered into force on 7th July 2000 following the conclusion of the process of its ratification and deposit of the Instruments of Ratification with the Secretary-General by all the three original Partner States (Kenya, Tanzania and Uganda). Rwanda and Burundi acceded to the EAC Treaty on 18th June 2007 and became full Members with effect from 1st July 2007. South Sudan acceded to the EAC Treaty on 15th April 2016 and became a full Member on 15th August 2016.

As a Member of the EAC, Uganda is obliged to comply with Article 126(2)(b) of the Treaty for the Establishment of the East African Community which requires Member States to harmonize all their national laws appertaining to the EAC. The same obligation is amplified by article of 47 of the Protocol on the Establishment of the EAC Common Market 2009, which calls for approximation, and harmonization of policies, laws and systems with the Community.

As noted earlier, cyber-security has become an important aspect for the East African region due to its rapid growth in social and economic development. In this regard, the EAC Partner States, in the spirit of furthering regional growth and integration, are working towards having harmonized cyberlaws that would be relatively effective, efficient and uniform within the Community. Such harmonized and effective cyber-legal framework will enhance coordinated cyber-security and prosecution of cybercriminals regardless of where the crime has been committed in the region.162

6.3 Overview of ICT Infrastructure in Uganda

The Government of Uganda in ensuring a conducive ICT environment has built and strengthened its institutional framework for policy coordination, regulation and implementation of ICT priority programmes and projects in the country. ICT is one of the primary drivers of economic growth and a key strategy for improving efficiency of service delivery to the citizens. The agencies/institutions in place are the Ministry of ICT and National Guidance, Uganda Communications Commission (UCC), National Information Technology Authority, Uganda, Posta Uganda and the Uganda Institute for Information and Communication Technology (UICT).\footnote{NITA-U Strategic Plan 2012/12-2017/2018, available at: \url{http://www.nita.go.ug/publication/nita-u-strategic-plan-201213---201718}, accessed on 28\textsuperscript{th} March, 2019.}

The government has also adopted national development strategies such as Uganda Vision 2040, National Development Plans as well as strategies and policies to ensure an effective and efficient ICT environment. These have given mandate to various ICT institutions to provide avenues through creating awareness and sensitization of stakeholders in both public and private sector in the bid to combat cybercrime in Uganda.

In terms of developing a comprehensive ICT infrastructure, priority is in the extension of the NBI which will further consolidate e-Government services and applications for efficiency. That is construction of ICT incubation hubs/centres and ICT parks.\footnote{Ibid., p. XIII.} Currently, the first incubation hub is under construction and will be situated in Nakawa, Kampala. The Government anticipates constructing other centres in Mbarara, Gulu, Mbale and Arua.

With these tremendous efforts that are being undertaken in the protection of cyber-security, Uganda was ranked first in Africa in cyber-
security management. The Global National Cyber Security Index\textsuperscript{165} 2018 commended Uganda’s tremendous efforts in analyzing cyber-threats and information management, protecting digital services, education and professional development as well as combating cybercrime, among others. However, it also acknowledges that Uganda still faces immerse challenges in terms of addressing cyber-threats and security for a conducive cyber-environment.\textsuperscript{166}

6.4 Data Collection

Field data on harmonization of cyberlaws in Uganda was collected during the months of March and April, 2019. The key Institutions visited include the Ministry of Information, Communications Technology and National Guidance, and National Information Technology Authority, Uganda. These are duly established institutions by the Government of Uganda to coordinate and develop the ICT infrastructure at national and regional level. More so, data was collected in form of conducting structured interviews. These interviews were conducted on face to face with respondents within these institutions. Among the respondents were legal and information technology experts who were able to give Uganda’s performance in ensuring a conducive and effective cyber-security culture at both national and regional level.

6.5 Policy, Legal, and Institutional Framework

The information technology environment is very dynamic and grows a supersonic speed making it prone to threats, misuse and manipulation.

\textsuperscript{165} The National Cyber Security Index (NCSI) is a global index which measures the preparedness of countries to prevent the realization of fundamental cyber threats and readiness to manage cyber incidents, crimes and large scale cyber crises, available at: http://www.sbs.ox.ac.uk/cybersecurity-capacity/content/national-cyber-security-index/, accessed on 17\textsuperscript{th} March, 2019.

These cybercrimes and threats have become more complex and sophisticated. This is because the perpetrators keep on devising means on how to disrupt the information technology systems due to increased computer and internet accessibility and usage. Cybercrimes pose massive threats to individuals on a personal level as well as to the security of a nation(s). With these increased cybercrimes and threats, countries have and continue to cooperate and devise means on how to protect themselves against these perpetrators (cyber-criminals) at national, regional and international level. Uganda in that regard, has taken tremendous steps by putting in place a progressive policy, legal and institutional framework in fighting these cybercrimes. The next section analyses these policy, legal and institutional frameworks adopted by the Government of Uganda.

6.5.1 National Strategies and Plans

As noted above Uganda has adopted several plans and strategies to ensure an effective and efficient ICT environment. These strategies and plans have been effective in providing an efficient ground for promoting and development of the ICT infrastructure in Uganda. They have helped to build and continue to build on the existing skill manpower through acting as guidelines for the different institutions in promoting awareness and capacity building. They have enabled to develop a basis for fighting against cybercrimes in Uganda. Some of these strategies include:

6.5.1.1 First National Development Plan (NDPI) 2010/11-2013/14

This plan focused on “Growth, Employment and Socio-economic Transformation for Prosperity.” The main objective was to promote science, technology innovation and ICT to enhance competitiveness. The achievements made in ICT infrastructure as per the NDPI included
the extension of the National Backbone Infrastructure (NBI)\textsuperscript{167} to a number of districts like Busia, Tororo, Mbale, kasese, Fort Portal, Jinja, Mukono, Lira, Gulu, among others, so as to provide faster internet speeds. 4G technologies were also rolled out using the Long Term Evolution (LTE). The fibre optic cables were laid out by the Government and the private sector, thus providing seamless connection across the country. That is from Masaka, Mutukula border post, Mbarara, Kabale and the Katuna border post.

\textbf{6.5.1.2 The Second National Development Plan (NDPII) 2015/16 – 2019/20}

This Second Development Plan was undertaken as a response to challenges identified while implementing the First Development Plan.\textsuperscript{168} The NDPII focuses at strengthening Uganda’s competitiveness for sustainable wealth, employment and inclusive growth. The key objectives of the Second Development Plan include the increase in sustainable production, productivity and value addition in key growth opportunities, increase stock and quality of strategic infrastructure to accelerate the country’s competitiveness, enhance human capital development, and strengthening mechanisms for quality, effective and efficient service delivery. More so, it also aims at honoring Uganda’s emerging developments at national, regional (EAC), the African Agenda (2063), and at global level (the Post 2015 Development Agenda).\textsuperscript{169}

\textsuperscript{167}National Backbone Infrastructure Project and e-Government Infrastructure 2006/2007 is a government initiative through the Ministry of ICT and National Guidance which involves the implementation of the National Data Transmission Backbone Infrastructure and e-Government Infrastructure with the aim of providing connectivity to Government Ministries and Departments in the country. This involves the laying of Optical Fiber Cable across all major towns with transmission stations in these towns available at: https://www.nita.go.ug/projects/national-backbone-infrastructure-project-nbiegi/, accessed on 28\textsuperscript{th} March, 2019.


\textsuperscript{169}Ibid., pp. xi-xii.
6.5.1.3 ICT Sector Strategy and Investment Plan 2015/16–2019/20

The Ministry of ICT and National Guidance developed a five-year ICT strategic and investment plan in 2015 to guide the systematic deployment of ICT for adequate development and service delivery in accordance with the Uganda’s Vision 2040 and NDPII. The Plan aims at developing a knowledge-based and vibrant ICT sector in Uganda. This is intended to provide an enabled leadership and environment for the promotion of the ICT industry, which in turn transforms Uganda into a well knowledge-based community. The main thematic areas of focus of the SIP are elucidated as ICT Governance, ICT Infrastructure, Human Capital Development and Planning, Information Society, Research, Innovation and Development, ICT Health, Safety and Environment, Cross-cutting Areas, Promotion of e-Services and Local Content, e-Government, ICT Industry Promotion in Target Markets, and Promotion and Coordination of ICT in other Sectors. The broadband target is anticipated to increase from 512kbps to 4Mbps and 30Mbps for rural and urban households respectively.

6.5.1.4 NITA-Uganda Strategic Plan 2012/13 – 2017/18

NITA-Uganda developed a five-year strategic plan 2012/13 – 2017/18 to guide and enable it intervene the IT subsector in Uganda. This plan aims at strategically positioning NITA-U at the helm of IT revolution countrywide. The long-term vision of NITA-U is having a globally competitive Uganda enabled by IT. That is use IT as strategic source to transform Uganda into a highly productive and globally competitive country in both quality human resource, and production of goods and services for socio-economic development. The mission of the plan is to strategically use IT as a resource to leverage and transform Uganda

---

171 Ibid.
172 Ibid.
into a knowledge-based society through enhancing government services, enhancing businesses and empowering the citizenry.\textsuperscript{173}

The main strategic goals of this plan in achieving IT development for social and economic transformation include; achieving a rationalized and integrated national information technology infrastructure as well as transaction level e-Government services for at least 50% of the MDA IT systems.

\textbf{6.5.1.5 National Information Security Strategy (NISS)}

The NISS vision is to provide direction for the national information security in order to promote trust and enable business as well as economic growth in Uganda. This aims at providing a guideline, which will reduce the probability of successful information security breaches. This in turn will lower the risks of consequential damage within the national digital infrastructure.\textsuperscript{174} In this regard, the NISS provides a strategic guideline for the harmonization of national efforts, EAC, and the international community to address information security and promote economic growth through the use of ICT by the Government itself, businesses, organizations and individual citizens.\textsuperscript{175}

\textbf{6.5.1.6 National Broadband Strategy (2016-2020)}

The aim of this strategy is to regulate the network space used by telecommunications companies in providing affordable and efficient service delivery to all citizens. This will for insistence seek to simplify internet access via wireless networks like Wi-Fi, and 3G and 4G as examples of advanced connections. This will enable Uganda to achieve one of its Vision 2040 goals of providing efficient ICT in enhancing

\footnotesize{\textsuperscript{173} Ibid., p. 10.  
\textsuperscript{174} Ibid., p. 9.  
\textsuperscript{175} Ibid., p. 8.}
better service delivery as well as creating employment opportunities and wealth.\textsuperscript{176}

The strategy focuses on mainly five (5) areas, namely: Infrastructure, Connectivity and Devices; Content, Applications and Innovation; Capacity Building and Creating Awareness; Policy, Legal and Regulatory Framework; and Finance and Investment.\textsuperscript{177} The strategy targets that by 2020 it would have enabled the provision of minimum broadband speed at 3mps, broadband penetration to be at 50\% for rural areas and 100\% for urban areas. That is in areas of district and sub-county headquarters, health centre IVs, tertiary institutions and secondary schools. Also, the cost of broadband to have reduced by 10\%, ensure digital literacy of the citizenry by 40\%, and registration of business online to be at 50\%. These are therefore intended to provide adequate telecommunications services to all Ugandans.\textsuperscript{178}

6.5.2 ICT Policies

As discussed in the preceding paragraphs, the Government of Uganda has adopted several policy measures to address cyber-related issues. The next section analyses these policies with a view to identify the strength and weaknesses.

6.5.2.1 National Information and Communications Technology Policy

This Policy envisions an ICT- knowledgeable society in all spheres of the citizenry. That is to leverage ICT transformation of the citizens by 2025. The main Policy objectives include: building a knowledge based human capital; promoting innovation in economic and social systems;

\textsuperscript{176} Joel, O., National Broadband Strategy for Uganda Rolled Out: Here’s all You Need to Know About it, 19\textsuperscript{th} September 2018, available At: http://www.guru8.net/2018/09/national-broadband-strategy-for-uganda-rolled-out-heres-all-you-need-to-know-about-it/, accessed on 15\textsuperscript{th} April, 2019.

\textsuperscript{177} Ibid.

\textsuperscript{178} Ibid.
expanding ICT infrastructure and its integration throughout the country; deepening utilization of ICT services by government, private sector, NGOs and citizenry at large; enhancing research and innovation in ICT products, applications and services, and improving ICT governance and environment in Uganda.\textsuperscript{179}

The Policy also enlisted key priority action areas in ICT infrastructural development. The first being expansion of ICT infrastructure and its integration in the country. This included the expansion of the National Backbone Infrastructure (NBI) in the entire country, promotion of reliable and affordable ICT infrastructure in rural remote areas, integration of communication, broadcasting and information systems, and implementation of the analogue to digital broadcasting migration roadmap.\textsuperscript{180} As of 2019, the NBI has been extended to a number of districts as per the NDPI such as Busia, Tororo, Jinja, Mukono, Gulu, and Lira, among others. More so, Uganda now operates a digital system of broadcasting as was coordinated and implemented by Uganda Communications Commission.

The second is the deepening of utilization of ICT services by the Government, private sector, Not-for-profit ICT organizations and the citizenry in general. The actions include the implementation of the national e-government strategy and Master plan, creation of awareness, and increasing ICT equipment, services and applications.\textsuperscript{181}

The third is enhancement of research and innovation in ICT products, applications and services. This entails the development and implementation of an ICT research and strategy, promoting of industrial production and assembling ICT products, promoting software and applications’ development, and setting up ICT parks to

\textsuperscript{179} Ibid., p. 15.  
\textsuperscript{180} Ibid., pp. 15-16.  
\textsuperscript{181} Ibid.
support research innovation and development.\textsuperscript{182} The NDPII seeks to extend the NBI with a view of having an efficient ICT backbone infrastructure, which aims at ensuring the construction of the ICT incubation hubs in Uganda. The Government plans to build five incubation hubs countrywide. The Government as per NDPII seeks to construct these incubation hubs in Kampala, Mbarara, Mbale, Gulu and Arua so as to facilitate ICT development in the country. These centres will serve as resource centres for Ugandan innovators through the provision of free necessary ICT services such as internet and computers among others. The first centre is still under construction and is situated in Nakawa, Kampala.\textsuperscript{183}

6.5.2.2 National Information Security Policy (NISP)

This Policy applies in accordance with the Computer Misuse Act, 2011 which is the principle legislation in combating cybercrime in Uganda. It provides for both the Critical Infrastructure (CI) and Critical Information Infrastructure (CII). Critical Infrastructure relates to all systems used directly in connection with or necessary for protected computer activities, handling of official communications and personal data.\textsuperscript{184} Critical Information Infrastructure refers to information and communication technologies that form the basic operation and control of national sectors such as health, water, transport, communications, government, energy, food, finance, and emergency services, among others.\textsuperscript{185}

\textsuperscript{182}Ibid.
\textsuperscript{183}Javira, N., Dates for Opening National ICT Innovation Hub Set. 23\textsuperscript{rd}July, 2018 Sautitech, Innovation Village, Uganda https://www.sautitech.com/tech/dates-for-opening-national-ict-innovation-hub-set/ as assessed on 23\textsuperscript{rd} April, 2019.
\textsuperscript{185}Ibid., p.7. The NSIP adopted the definition of “CI” and “CII” from the International Telecommunications Union (ITU) which was originally founded in 1865. The ITU is a United Nations Agency tasked with coordinating telecommunication operations and services throughout the world, available at: http://www.un.cv/agency-itu.php/, accessed on 20\textsuperscript{th} March, 2019.
Moreover, the NISP structure seeks to address four (4) aspects, namely: Security Governance, Information Security, Personal Security and Physical Security. These are considered to be the most important aspects being addressed by the Ministry of ICT and National Guidance as per cyber welfare in Uganda. Currently, this policy structure implementation is at its third stage of Personal Security.\textsuperscript{186}

Third is Personnel Security, which involves employees and staff of organizations who may be potential sources of threat. It is important it protecting the cyber-supply chain against state and industrial espionage threats. Organizations must take appropriate measures before granting individuals access to sensitive information by ensuring their trustworthiness, integrity and reliability. This is because risks are inevitable and it cannot be presumed that individuals can be reliable at all times. Organizations should, therefore, be alert and investigate any suspicious behavior, which may pose a threat to that organization’s critical infrastructure.\textsuperscript{187}

\textbf{6.5.2.3 National Broadband Policy (NBDP)}

The broadband Policy emphasizes the role of broadband Internet in promoting socio-economic development through supporting the objectives of the NDPII and Uganda’s Vision 2040. It is to be implemented for a period of five (5) years before being reviewed to access its effectiveness and efficiency. The policy also seeks to address the existing impediments by developing an appropriate framework to address infrastructural development gaps, legal and regulatory environment and capacity gaps among citizens to adequately exploit the existing ICTs in place.\textsuperscript{188}

\textsuperscript{186} Interview with Ministry of ICT and National Guidance on 4\textsuperscript{th} March 2019.
\textsuperscript{187} \textit{Ibid.}, pp. 38-43.
The main objective of the Policy is to harmonize and regulate the plan and development of broadband infrastructure, define the appropriate technology MIX which will enable universal connectivity while reforming the licensing framework. This will in turn improve on quality service delivery in the industry while meeting the overall national goals and aspirations. The existing regulated broadband infrastructural development has mainly been due to limited connectivity, high internet costs, poor last mile connectivity which only connects government agencies, and very slow internet speed.\textsuperscript{189}

This Policy is also in line with Government’s mandate of providing digitalized services due to the advancing scientific technological developments in the country. These on line digital platforms such as e-government and e-commerce services will provide easy accessibility of services to the citizenry. Having these services close to the people will enable them to avoid tracking long distances to have access to these services.

\textbf{6.5.3 Legal Framework/Status of Cyberlaws}

Currently, Uganda has drafted a number of legislation as per the recommendations of the EAC Task Force. Various stakeholders have jointly coordinated efforts in the legislative drafting process specifically Ministry of Information, Communications Technology and National Guidance, Ministry of Justice and Constitutional Affairs, Uganda Communications Commission, Uganda Law Reform Commission, and National Information Technology Authority-Uganda, among others. These have enabled the development of policies, laws, regulations, and strategies for ensuring a secure and effective information technology environment. Of recent, the President of Uganda assented to the Data Protection and Privacy Act, 2019 which has been pending since 2015. These pieces of legislation are summarized below.

\textsuperscript{189}\textit{Ibid.}, pp. 13 – 19.
6.5.3.1 The Computer Misuse Act, 2011 (Act No. 2 of 2011)

The Computer Misuse Act (CMA) makes provision for the safety and security of electronic transactions and systems. It also aims at preventing unlawful access to and misuse of information systems including computers. The Act also makes provision for securing the conduct of electronic transactions in trustworthy electronic environment. In this regard, it:

• Prescribes liability for offences related to computers such as child pornography, cyber-harassment, offensive communications, and cyber-stalking. With the exception of child pornography, which can generate the maximum prison sentence of 15 years, the penalties range from one to five years of prison.

• Penalizes unauthorized access to computer programs and data, unauthorized modification of computer material, unauthorized use of interception of computer service. The maximum penalties for these offences are between 10-15 years.

• Penalizes unauthorized disclosure of information with a maximum prison sentence of 15 years (section 18).

• Empowers Police officers with far-reaching powers of search and seizure if they suspect an offence under CMA

• Empowers Magistrate to issue a warrant authorizing a police officer to enter and search the premises, using reasonable force as is necessary (section 28).

6.5.3.2 The Electronic Transaction Act, 2011 (Act No. 8 of 2011)

The major objective of the Electronic Transactions Act (ETA) is to remove the legal and operational barriers to electronic transactions by facilitating the use of electronic communications and applying existing legislation to electronic communications. The Act in effect gives a functional equivalent of electronic communications or transactions to
the traditional paper-based communications or transactions. Whatever can be done in the traditional physical paper environment can now be done electronically. It covers the following aspects:

- Provides for the use, security, facilitation and regulation of electronic communications and transactions.
- Enforceability and form requirements for electronic contracts.
- Regulation of domain names which are a new form of digital property.
- Privacy protection for consumers and users of electronic media.
- Establishment of a regulatory frame work that is complaint with the rapid technological charges.
- Determining the levels of responsibility in tort and contract attached to enhanced abilities of machines.
- Classification of trade in information products especially where the relationship between the producer and ultimate consumer is remote.
- The use, validity, security, facilitation and regulation of electronic communications and transactions and encourages the use of e-Government services.

6.5.3.3 The Electronic Signatures Act, 2011 (Act No. 2 of 2011)\(^{190}\)

This Act regulates the use of electronic signatures in Uganda. The use of electronic signatures has been regarded as a positive development in the ICT arena. However, the use of electronic poses several challenges especially in identifying the signatory and to avoid forgeries.

\(^{190}\) There are subsidiary legislation made under the Act which include the Electronic Signatures Regulations (Statutory Instrument No. 43 of 2013) which provide for the use of electronic signatures and ensure consumer protection against unauthorized access and modification of consumer information. The Electronic Transactions Regulations (Statutory Instrument No. 42 of 2013) which provide for the use, security, facilitation and regulation of electronic communications and transactions.
In doing so, the Act criminalizes unauthorized access and modification of electronic signatures. The Act has modernized and harmonized the laws relating to computer generated evidence, and admissibility and evidential weight of electronic communications.

6.5.3.4 The National Information Technology Authority, Uganda Act, 2009 (Act No. 4 of 2011)

This law establishes the National Information Technology Authority in Uganda (NITA-U). It is a Government Agency under the general supervision of the Minister responsible for Information Technology. The goals of the NITA-U listed under section 4 include diverse ways to promote information technology in Uganda and most of these aims are commendable. The functions of the NITA-U listed in section 5 are many (18) and rather broadly formulated. Section 5 (18) extends the functions of the authority to undertake any other activity necessary for the implementation of the objects of the authority.

6.5.3.5 The Regulation of Interception of Communications Act, 2010 (Act No. 18 of 2010)

The Regulation of Interception of Communications Act, 2010 (RICA) provides for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Uganda. RICA also provides for the establishment of a Monitoring Centre for the interception of communications.

An application for the lawful interception of any communication may be made by the Chief of Defence Forces, the Director General of the External Security Organization, the Director General of the Internal Security Organization, the Inspector General of Police or their

---

191 Sections 3 (3) and 2.
192 Section 3.
nominees. A warrant to intercept communications shall be issued by a designated Judge after considering grounds listed under section 5 of the Act.

The Act imposes an obligation on service providers to install relevant equipment with capability to enable the interception of communications. Failure to install such equipment is punishable by an imprisonment of up to five years. Similarly, telecommunications service providers have a duty to ensure that subscribers register their SIM-cards and provide service providers with comprehensive information about e.g. their identity and address.

6.5.3.6 The Uganda Communications Act, 2013 (Act No. 1 of 2013)

The Uganda Communications Act (UCA) regulates the Ugandan communications services. It provides for the establishment of the Ugandan Communications Commission (UCC). Functions of the UCC include, for example, to monitor, inspect, licence, supervise, control and regulate communications services; to receive, investigate and arbitrate complaints relating to communications services and take necessary action; establish an intelligent network monitoring system to monitor traffic, revenue and quality of service of operators and to set standards, monitor and enforce compliance relating to content. The UCC shall exercise its functions independently while the Minister may, in writing, give policy guidelines to the Commission regarding the

---

193 Section 4 (1), also referred to as authorized persons section 1.
194 A judge designated by the Chief Justice to perform the functions of a designated judge for purposes of RICA see sections 4 & 5.
195 Section 8.
196 Section 9.
197 Section 4.
198 Section 5.
199 Section 8.
performance of its functions and it shall comply with these guidelines.200

The functions of the UCC open up for extensive possibilities to supervise and control the communications falling under the scope of UCA. This also makes it possible for it to act in a way that infringes both privacy and freedom of expression. Section 5(u) has, for example, been used to establish the Social Media monitoring centre and the interception of Communication monitoring centre under RICA to conduct communication surveillance of individuals’ communications for example on the Internet. Government has also recently threatened to completely block the usage of social media platforms such as Facebook and What Sapp. The effect of these types of actions on the Internet freedom of citizens with regard to both freedom of expression and privacy is obviously extremely hampering.

6.5.3.7 The Anti-Pornography Act, 2014 (Act No. 1 of 2014)

The Anti-Pornography Act (APA) was adopted in 2014 and criminalizes all forms of pornography. In terms of section 13(1), it is a criminal offence to produce, traffic in, broadcast, procure, import, export, sell or abet any form of pornography. This offence is punishable by imprisonment of up to ten years.201 In the same vein, section 14(1) criminalizes the same actions concerning child pornography in which case the maximum sentence is fifteen years.

Section 17 of APA also stipulates responsibility for Internet service providers. In this regard, an internet service provider who, by not using or enforcing the means recommended by the Committee to control pornography, permits to be uploaded or downloaded through its service any content of pornographic nature, commits an offence which can result in a prison sentence of maximum of five years. Further to

200 Section 7.
201 Section 13 (2).
that, the court has powers to suspend the business of Internet service providers who has committed an offence under the Act.\textsuperscript{202}

\textbf{6.5.3.8 The Data Protection and Privacy Act, 2019}

The major objectives of the Act are protection of the privacy the individual and or personal data by regulating the collection and processing of person information. In addition, the Act provides for the rights of the persons whose data is collected and the obligation of data collectors, data processers and data controllers. The Act also regulates the use and disclosure of personal information.

Section 3 of the Act specifically sets the principles of data protection to be observed by any data collector, data processor or data controller or any person who collects, processes, holds or uses personal data. These principles include a accountability for the data subject for data collected, processed held or used; collecting and processing data fairly and lawfully; collecting, processing, using or holding adequate, relevant and not excessive or unnecessary personal data; retain personal data for the period authorized by law or for which the data is required; ensuring quality of information collected, processed, used or held; ensuring transparency and participation of the data subject in the collection, processing, use and holding of the personal data; and observing security safeguards in respect of the data.

Section 4 of the Act establishes the personal data protection office responsible for personal data protection under the National Information Technology Authority –Uganda that shall report directly to the Board. Section 5 provides for the functions of the personal data protection office.

As regards to data collection and processing, the Act provides that collection or processing of personal data requires consent of data

\textsuperscript{202} Section 17(2).
subject and in case of children, consent from parents or guardian.\textsuperscript{203} The Act also prohibits individuals or private entities from collecting or processing personal data which relates to the religious or philosophical beliefs, political opinion, sexual life, financial information, health status or medical records of an individual.\textsuperscript{204} The Act requires that the processing of data must be compatible with purpose of collection\textsuperscript{205} and that the period for retention of such data should not be longer is necessary to achieve the purpose for which the data is collected and processed.\textsuperscript{206} The law imposes an obligation on the controller, data collector or data processor to secure the integrity of personal data\textsuperscript{207} and notify the responsible authority where there are security breaches.\textsuperscript{208}

There are several offences for non-compliance with the Act. These offences include unlawful obtaining or disclosing of personal data,\textsuperscript{209} unlawful destruction, deletion, concealment or alteration of personal data\textsuperscript{210} and sale of personal data. A person shall not sell or offer for sale personal data of any person.\textsuperscript{211}

\section*{6.5.4 Institutional Framework}

The legal and policy framework has been put in place so as to provide ICT regulation and usage in Uganda. Institutions have also been put in place to coordinate and regulate ICT infrastructure. That is Ministry of ICT and National Guidance, which is the policy body at national level. Under the Ministry are two (2) institutions, which are NITA-U, which regulates IT, and UCC, which regulates communications in Uganda.

\begin{footnotesize}
\textsuperscript{203} Sections 7 & 8.
\textsuperscript{204} Section 9.
\textsuperscript{205} Section 17.
\textsuperscript{206} Section 18.
\textsuperscript{207} Section 20.
\textsuperscript{208} Section 23.
\textsuperscript{209} Section 35.
\textsuperscript{210} Section 36.
\textsuperscript{211} Section 37.
\end{footnotesize}
The functions of these institutions and legal mandate are discussed below.

6.5.4.1 Ministry of Information, Communications Technology and National Guidance (MoICT& NG)

The Ministry of Information and Communications Technology was established in June 2006 so as to coordinate ICT developments and implementation programmes within the different Government Ministries and Agencies. It is now referred to as the Ministry of ICT and National Guidance. Its mandate is to provide strategic and technical leadership, overall coordination, support and advocate on all matters of laws, regulations, policy and strategy for ICT sector. This is done through ensuring an efficient ICT legal and regulatory environment, securing ICT usage and access for all, increasing employment and growth opportunities, increasing awareness as well as citizenry participation in government programs. The Ministry is further tasked with ensuring sustainable, efficient and effective development, harnessing and utilization of ICT in all spheres so as to achieve the country’s national development goals.²¹²

This Ministry is divided into three (3) directorates for better service delivery, that is, the Directorate of ICT Infrastructure and Investment, Directorate of Information Technology Services, and Directorate of Information and National Guidance. The Directorate of ICT Infrastructure and Investment consists of the Department of ICT Infrastructure Planning and Technology Support, and Communication Network. The Directorate of IT Services is categorized by the Department of ICT Research and Development, and Department of E-services. The Directorate of Information and National Guidance comprises the Department of Information Dissemination and Public Relations, and the Department of National Guidance. These departments work hand in hand with other administrative and financial

departments within the Ministry for an efficient and effective service delivery.\textsuperscript{213}

Other different government institutions in achieving its mandate support the Ministry. These institutions coordinate with the Ministry in providing sensitization programmes to the citizenry in both public and private sectors as elucidated below.

a) Uganda Communications Commission (UCC), which is tasked with regulating the communications sector and broadcast. It ensures effective and efficient management of scarce communications resources, healthy competition, consumer protection, research and development of human resource in the sector;

b) National Information Technology Authority, Uganda (NITA-U) being responsible for ensuring a rationalized and integrated national IT infrastructure as well as regulating IT in public and private sectors;

c) Uganda Post Limited (UPL) responsible for offering a wide range of postal, communications and logistical services, financial services, passenger transport and parcel delivery service;

d) Uganda Institute of Information and Communications Technology (UICT) tasked with conducting training courses, seminars, workshops as well as creating public awareness in communication;

e) Uganda Broadcasting Corporation (UBC) which is the national Broadcaster providing radio and television broadcasting services and programmes;

f) Uganda Media Centre (UMC) which provides professional media and communication services to government departments, as

\textsuperscript{213} \textit{Ibid.}
well as a conducive communication environment between government and media;

g) Media Council which regulates and promotes ethical standards and discipline of journalists, settle disputes between the public and media;

h) Vision Group which is a multimedia business providing newspapers, magazines, internet publishing, television, radio, commercial printing, advertising and distribution services;

i) Parliamentary Committee on Information, Communication Technology and National Guidance which oversees the Ministry of ICT and National Guidance;

j) The ICT and National Guidance Sector Working Group which harmonizes, coordinates, monitors, evaluates and reports on sector vision and goals, policy frameworks, plans and performance of all sector Ministries, Departments and Agencies (MDAs).214

The Ministry in securing a conducive IT environment has and continues to conduct awareness programmes as a government entity as well as by its different institutions in ensuring cyber-security and combating cybercrimes and threats in the country. Of recent in March 2019, the UK Government in collaboration with the Ugandan Government through the Ministry held a cyber-capacity building event under the Common Wealth Cyber Declaration as agreed upon at the 2018 Common Wealth Heads of Government meeting which commits Common Wealth States to collective cyber-security and building foundations.215 This comes at the time when Uganda is in the process of updating its National Risk Register. The workshop centered on National Cyber Security Risk Assessment as part of the National Cyber Security Capacity Building Initiative. The National Cyber Risk

214 Ibid.
Assessment Report will be able to give an indicator of the country’s Risk Profile.216

The Ministry also partnered with IT experts from South Africa and Botswana to train IT personnel from ministries and agencies on fighting cybercrime. This five (5) day training programme aimed at equipping Ugandans in both public and private sector with knowledge so as to guard against cyber fraudsters and conmen in their organizations. That is protecting online data, early detection of hackers, safe online transactions of data and risk factors. It is important to note that cybercriminals do also target information, which is very vital and secret to many organizations other than money. People need to be enlightened on the risks involved once information is stolen and also be able to detect signs of data that could be at risk of being stolen. The training equipped the trainees with the necessary skills that will enable them protect their organizations against cyber threats. It was also recommended that they train other colleagues and workmates on how to deal with cybercriminals. 217

The Ministry has not faced much of cyber-attacks because of the continuous monitoring and secured IT system infrastructure in place. However, it cannot be ruled out that it has not faced such attacks since its establishment. In 2012, the Ministry faced an incident when the Office of Prime Minister was anonymously attacked website was hacked by gay activists who were condemning the actions of the government of Uganda through Parliament on enacting the Anti-Homosexuality law. The Bill was being debated upon and passed into law in December 2013 and assented to in February 2014 (The Anti Homosexuality Act, 2014) prohibiting all forms of homosexual acts and related practices in the country. The Ministry had to pull down these websites because of the inappropriate posts and footages that were

216 Ibid.
being sent which were rendered to be invading the “person” of the Prime Minister.218

Therefore, the Ministry of ICT and National Guidance being the policy maker involves all other parastatals like NITA-Uganda and UCC as regulatory bodies for IT and Communications respectively to continuously create awareness and sensitization programmes to fight cybercrimes in the country. The Ministry also encourages the involvement of other law enforcement agencies such as the Police, Defence, Judiciary and DPP (Prosecutors) as the law enforcement agencies in these projects in effectively prosecuting and determining cybercrimes in courts of law. These trainings and workshops help to continuously train and equip them with skills and knowledge so as to be alert and monitor their ICT systems.

6.5.4.2 National Information Technology Authority, Uganda (NITA-U)

NITA-U is established under section 3 as the principle statutory agency responsible for coordination, promotion and monitoring the development of information technology in the essence of promoting national social and economic development in Uganda.219 It became operationalized in 2010. It is the regulatory body responsible for information services in Uganda. The Ministry of ICT and National Guidance monitor it. It envisions transforming Uganda into a knowledge-based society by leveraging information technology as a strategic resource to enhance government services, enrich businesses and empower citizens. 220 NITA-U promotes values of integrity, innovation, team work, customer centricity and quality which are all essentials in having an effective ICT environment in Uganda. This is in terms of encouraging honesty and discouraging unethical corruption

---

218 Interview with Ministry of ICT and National Guidance on 4th March 2019.
219 NITA, Uganda Act, No. 4 of 2009.
tendencies, develop new ideas which aim at ensuring customer satisfaction, and have quality and improved IT works thus ensuring excellent service delivery to all.\textsuperscript{221}

The main objectives of NITA-U are to:

a) Provide high quality information technology services to government;

b) Promote standardization of IT equipment and services through planning, acquisition, implementation, delivery, support and maintenance for better usage and reliability countrywide;

c) Assist and offer guidance to other IT users and providers as maybe required from time to time;

d) Promote cooperation, coordination and rationalization among IT users and providers at both national and local levels to avoid duplication efforts;

e) Promote and be the focal point of cooperation of IT at both regional and international levels; and

f) Take into consideration special interest groups in accessing and utilization of IT.\textsuperscript{222}

The Authority is tasked with providing first level technical support and advice for critical government IT systems as well as the establishment of e-Government, e-Commerce and other e-Transactions, advice government on matters of IT development; coordinate, supervise and monitor utilization of IT in public and private sectors; regulate and enforce standards for IT hardware; create and manage the national databank; regulate electronic signature infrastructure and other

\textsuperscript{221} Ibid.
\textsuperscript{222} Section 4, NITA, Uganda Act, No. 4 of 2009.
electronic transactions; regulate IT profession; and commission IT research in the country among others.\textsuperscript{223}

NITA-Uganda being the IT statutory regulatory body has and continues to carry out capacity development and skills training programmes in the event of addressing the challenges faced in the fight against cybercrime and threats. These are done through workshop seminars and organizing sensitization training programmes for the essence of impacting IT knowledge on different forums and sectors within the country. Law enforcement agencies such as Police, Defence, State Attorneys, Director of Public Prosecution (Prosecutors) are especially trained on matters relating to white-collar crimes on prosecution.

The Authority derives its mandate to conduct such trainings from the NITA-U (Authentication of IT Training) Regulations, Statutory Instrument No.70 of 2016. These Regulations authorize the Authority to train different personal and institutions in cybercrime awareness. Such trainings are to be done in conjunction and consultation with the Ministry responsible for education.\textsuperscript{224} The Authority further signed a Memorandum of Understanding with the National Council of Higher Education and Ministry of Education and Sports to ensure that ICT is incorporated in the National Curriculum. Some of the trainings done have been on management of Active Directory Services; Cyberlaws, Cybercrime and Security; Website and Social Media Management; Microsoft Office Suite; and Communication and Online Content Management (training for the blind and deaf inclusive).\textsuperscript{225}

The recently assented to Data Protection and Privacy Act 2019 authorizes NITA-Uganda to investigate complaints made against any data collector, data processor or data collector where a breach has

\textsuperscript{223} Section 5.

\textsuperscript{224} Section 3, 4 and 5 on Authentication of Information Technology Training.

been believed to have been committed against a data subject. The Authority may be directed to restore the integrity of the data collected, processed or held by the data collector.226 Where one feels aggrieved by the decision of the Authority, they may appeal that decision made by the Authority to the Minister within thirty days (30) from the notice of the decision.227 The Minister responsible shall be the Minister of ICT and National Guidance.

In January 2019, NITA-U in collaboration with the Internet Corporation for Assigned Names and Numbers (ICANN)228 held a training session for law enforcement officers (detectives) to equip them with knowledge on investigation of cybercrime that involves the misuse and abuse of Domain Name System. The Domain Name System (DNS) is an Internet service that translates domain names into Internet Protocol addresses and vice versa. The trainees were enhanced in understanding of the DNS infrastructure, its ecosystem, Internet protocols as well as improve case preparation and investigation. This is because the DNS has continuously been manipulated and misused for criminal Internet activities such as electronic fraud, phishing, spam, data corruption, privacy invasion, intellectual property infringement, malware distribution, and other cyber-enabled crime.229

The Authority also in February 2019 held another training session on cyber-security for journalists at the Ministry of ICT and National Guidance headquarters. It involved journalists from broadcasting houses (Radio and Television), print and online media. It aimed at

226 Section 32.
227 Section 34.
228 ICANN is a non-profit organization, which was incorporated in California (USA) on the 18th September, 1998. It is tasked with overseeing the administrative duties associated with running Internet in USA. That is overseeing the top-level domains, registering and maintaining the directory of domain names used in the Internet Protocol (IP) as well as resolving trademark disputes over domain names. http://www.britannica.com/topic/ICANN, accessed on 25th March, 2019.
enlightening journalists on existing cyberlaws and online internet crime so as to widen their knowledge base as well as reporting from an informed point of view.\textsuperscript{230}

It is, therefore, important to credit the Authority for the tremendous efforts and steps it has taken in conducting awareness and sensitizing programmes across government agencies (MDAs) so that every individual gets to understand the relevance of information technology in the fight against cybercrime. As an organization, its employees are and continue to be involved in these projects and programmes thus having not experienced any cyber-threats as of yet. However, it has been noted that these trainings are mostly done in urban areas that is Kampala, being the capital city as compared to other areas in the country. These programmes are yet to be availed to those areas. Therefore, implementation of cyberlaws and regulations is still inefficient thus making the determination and prosecution of such crimes difficult in the least sensitized areas.

Furthermore, NITA-Uganda in collaboration with CIPESA carried out a National IT survey amongst MDAs, LGs and Individual citizens. The 2017/2018 survey aimed at “\textit{enhancing the availability of relevant and accurate information on access, usage and satisfaction related to IT in Uganda for regular internal and external reporting purposes.}\textsuperscript{231} The survey evaluated the adequacy of telecommunications infrastructure, accessibility of e-government and e-public services, e-commerce, availability of human resource to promote ICT usage, availability of online services, and content, security and privacy.\textsuperscript{232} NITA-Uganda evaluated the awareness of cyberlaws within MDAs, LGs and among the citizens.

\textsuperscript{232} Ibid., p. XVII.
The report showed that 83.1% of MDAs have knowledge of Ugandan cyberlaws on electronic communications and transactions. 90.6% could cite the Computer Misuse Act 2011, 70.3% - the Electronic Transactions Act 2011, 67.2% - the Electronic Signatures Act 2011 and 9.4% could not state any law. 82.8% could at least mention two offences under the Computer Misuse Act amongst which hacking, and malicious and offensive communications as the commonest crimes. In reporting these cyber offences, 46.4% reported to the Uganda Police Force or any other law enforcement agency while 42.9% lodged their complaints with NITA-Uganda.233

At local government level, 61.9% were aware of Ugandan cyberlaws. 38.5% could not ably cite the Computer Misuse Act 2011, 23.1% - the Electronic Transactions Act 2011, 23.1% - the Electronic Signatures Act 2011, and 38.5% were not able to mention any law. Also, the most common cyber-offences were, namely; hacking, malicious and offensive communications and disclosure of private sexual images without consent. Most of these were also lodged to the Uganda Police Force (71.4%) and to institutional Internet service providers. None managed to report to NITA-Uganda and CERT.Ug being the coordinating response bodies in cyber security threats.234

On an individual level, most of them are still unaware of these cyberlaws. Only 18.5% had knowledge of the cyberlaws. The majority were in the urban areas (23.8%) as compared to those in the rural areas (8.6%). 73.5% could not ably and correctly cite any law. 17.9% could correctly cite the Computer Misuse Act 2011 being the commonest cyberlaw, 6.4% - the Electronic Transactions Act 2011, and 2.8% - the Electronic Signatures Act 2011.235 20.1% knew of reporting cyber-offences to law enforcement agencies under the Computer Misuse Act. However, only 3% had ever lodged complaints of cybercrimes committed against them. This makes it prone to

233 Ibid., pp. 81-82.
234 Ibid., pp. 106-108.
cybercriminals to target unsuspecting victims because of the weaknesses among individuals of having no knowledge on security awareness measures. Therefore, with the above-mentioned achievements by NITA-Uganda, there is a lot of work that remains to be done so as to create more public and private sector awareness on cyberlaws and cybercrimes in the country. This being a complex and rapid digital era, NITA-Uganda and other different stakeholders need to work together in educating and sensitizing all citizens on matters relating to cyber-security.

6.5.4.3 National Computer Emergency Response Team Uganda/ Coordination Center (CERT.UG/CC)

The National Information Security Strategy (NISS) mandates the creation of a National Computer Emergency Response Team under the NITA-U. Thus the government of Uganda through the Ministry of ICT and National Guidance and NITA-U established the National Computer Emergency Response Team/Coordination Center as the first official computer security response team. This Team endeavors to protect the nation’s critical information infrastructure, as well as drafting the overall plan on the Uganda’s approach to cyber-security related issues. It serves as a focal point for further building and implementing the National Culture of cyber-security. The CERT.UG/CC comprises of qualified personnel referred to as “Advisory Team”. They are basically in charge of administrative procedures and policy. The team provides adequate support services and also responds to cyber security threats in Uganda.237

The CERT.UG/CC intends to establish a management organization and structure to respond effectively to cyber-security incidents, improve information security awareness, accomplish maximum performance, provide analytical support, analysis, and advice on cyber-security in

---

236 Ibid., p. XXII.
Uganda. It further facilitates communication with experts both locally and internationally to assist in the solving of security incidents. The Team also invites cooperation and support from citizens and non-citizens so as to improve on the awareness and understanding of information and security concerns in Uganda.\textsuperscript{238}

It is important to note that CERT.UG/CC is a member of the Forum of Incident Response Team (FIRST). It was admitted into the programme during the annual FIRST conference that was held in Berlin, Germany on the 15\textsuperscript{th} June 2015. FIRST is the premier organization and recognized global leader in security incident response. It engages various computer security incident response teams from Government, commercial and educational organizations. FIRST aims to bridge cooperation and coordination in incident prevention, rapidly respond to cyber-incidents, and promote information sharing among members and the community as a whole. It recognizes the need to bring together security teams in various countries so as to become part of the global incident response community.\textsuperscript{239}

Furthermore, CERT-UG/CC offers services in handling security incidents and support the affected parties to recover from any breach. It is the trusted source of information and advice on cyber-security issues in Uganda in providing advisory support and guidance in many aspects from written advisories to sectoral briefs.\textsuperscript{240} Such services offered include:

\begin{itemize}
\item[a)] Reactive Services which involves alerts and warnings, incident handling, incident analysis and response coordination, response
\end{itemize}

\begin{footnotes}
\textsuperscript{238}Ibid.
\end{footnotes}
on site, vulnerability handling, analysis, response and response coordination.

b) **Proactive Services** involving online child protection, announcements, technology watch, security audits, configuration and maintenance of security, development of security tools, intrusion detection services and security-related information dissemination.

c) **Artificial Handling Services** comprising of Artifact analysis, response and response coordination. Artificial handling refers to analysis of any file found on a system that might be involved in malicious actions. It handles and distributes result information to vendors and interested parties thus preventing the further spread of malware as well as mitigating the risks involved.

d) **Security Quality Management Services**. These are basically long term goals and include consultancy and educational measures specifically risk analysis, business continuity and disaster recovery, security consulting, awareness building, education and product evaluation.

Furthermore, CERT has a website that acts a platform for alerting any threats. This website also informs users of any threats by sending out alerts via email, Twitter and Facebook. However, with the survey undertaken by NITA-Uganda 2017/2018, the report showed that CERT.Ug needs to engage more of the public and private sector being the coordinating response team in Uganda on cyber- security. For insistence, 10.7% of MDAs reported cybercrimes to the CERT team while at the local government level, there was no reference at any one instant. This implies that either there is no knowledge of the existence of the CERT and more especially at local government level and among the citizens. Therefore, CERT.Ug needs to engage and

---


involve other stakeholders by sharing advice on cyber security related incidences on the different available platforms where information can easily be accessed.

6.6 Challenges

Uganda in that regard has taken tremendous steps by putting in place a progressive policy, legal and institutional framework in fighting these cybercrimes. However, there are still challenges that continue to hinder the fight against these cybercrimes and threats as listed below.

6.6.1 Inadequate Computers and other Digital Equipment

There is limited supply of computers and other digital equipment both at individual and public level that can be used in running of the daily day to day activities. This is due to the high costs involved in purchasing and maintaining such equipment. In some other instances, some IT equipment is outdated and still operates an old model system compared to the increased technological advancements on the globe. This is also coupled with limited IT knowledge and skills in operating such digital equipment. For insistence, the National IT survey report of 2017/18 by NITA-Uganda revealed that internet usage at Local Government level had been branded to have negative impacts which in turn defeats government’s efforts in effectively ensuring that all persons at grass root level can have access to government services.

In addition, there are still ICT infrastructural gaps such as developing and constructing regional science parks and technology incubation centres as was anticipated under the NDPI. Other challenges included the high cost of internet bandwidth, limited ICT innovation exploitation for commercial orientation, low uptake of e-services, and vandalism and damage to the infrastructure.
6.6.2 Limited Public and Institutional Awareness

There are inadequate measures in terms of public and institutional awareness when it comes to cybercrime and threat concerns especially in areas outside the capital city Kampala and surrounding urban areas. There are questions as to whom one addresses his/her concerns in case of a threat and if organizations have skilled personnel to handle cyber-threats within. Majority of persons have limited knowledge or are unaware of matters relating to cybercrimes. The legislations on cybercrimes are in existence though people have not familiarized themselves with such laws. For instance, law enforcement agencies such as Police, Defence, Prosecutors (DPP) and State Attorneys have limited capacity to investigate and prosecute such cases. In Kampala, the Police Forensic Department suited at the police headquarters in Naguru is equipped with handling cybercrimes. However, out of the capital city and remote areas, there is still no operating system to fight cybercrimes and ensuring that follow-ups are made.

6.6.3 Information Sharing

Partner States have different platforms and standards on which they operate their security systems. The question then lies in what kind of information can be shared among the Partner States to ensure a safe cyber-security environment. This is because the information to be shared varies from one Partner State to another. There is no cooperation and coordination among the Partner States when it comes to information sharing although a Memorandum of Understanding on Cooperation and Information sharing was signed by the Ministers during the 14th Summit held in Nairobi, Kenya in June 2018 on the Northern Corridor Integration Projects (NCIP). Partner States have reluctantly failed to agree on what kind of information to share with each other. This has been greatly based on the aspect of SECURITY because at times this information may be categorized as CONFIDENTIAL and revealing it may pose as a security threat to that Partner State which has been asked to relinquish such. Even when it
comes to organizations within the Partner States, they are reluctant to inform enforcement authorities such as Police in case of any attack because they presume to be putting their reputation at risk. This has become very challenging especially when it comes to adducing evidence in courts of law and prosecuting cybercriminals.

The question posed is if Partner States are able to understand each other and willing to share information regarding cybercriminals in combating cybercrimes. This is because repatriation of such offenders is at the discretion of the country of origin of the culprit. More so, the evidence to be presented against these perpetuators is usually outside the country requesting for such information. Having access to such evidence is very difficult because countries are not willing to diverge such information. Also, trying to keep track of these crimes is very costly in terms of making follow ups, having the qualified personnel to deal with cybercrime and forensic equipment among others to ensure an effective justice system thus complicating the fight against cybercrimes.

6.6.4 Mutual Assistance

Partner States are still reluctant to assist each other in matters relating to cyber- security especially in prosecuting cybercriminals. They are reluctant to cooperate especially in repatriating cybercrime suspects who may want to evade prosecution. Countries are protective and not willing to present such culprits to the requesting Partner State for prosecution. This has greatly affected the fight against cybercrimes in East Africa which in turn has affected the working relations among the Partner States.

6.6.5 Evidence Submission

Proof of cybercrimes is very challenging especially in trial proceedings because in most instances evidence is electronic. It never exists on paper. This has made it difficult to be admissible in courts of law
because this evidence can easily be manipulated, altered or damaged. Also, authenticity and reliability on such evidence in terms of who generated it or who authored it makes the trial process very complex. This is also coupled with limited skilled personnel who have limited expertise in investigating and tackling cybercrimes because they require very high expertise and specialist training so as to be able to handle cybercrime investigations. Therefore, where electronic evidence is not properly collected and submitted, the prosecution process is rendered unsuccessful.

6.7 Conclusion

Uganda has made tremendous efforts in developing a comprehensive policy, legal and institutional framework in combating cybercrimes at the local level. Such have been drafted since 2010 as per the recommendations made by the EAC Task Force on harmonization of cyberlaws in East Africa. Uganda has been involved and continuous to be take part in many projects and programmes at national and regional level so as to have a harmonized cyber-legal framework as well as fighting cybercrimes within the country. However, there are challenges that are still affecting the fight against cybercrimes thus delaying the process of harmonization of cyberlaws within the region. Many factors are still in play, which the institutions responsible for building a conducive ICT environment are endeavoring to address so as to embrace the new emerging technological developments in the world.

6.8 Recommendations

Tremendous efforts have been put in place in terms of developing a comprehensive legal, policy and institutional framework in regulating and usage of ICT at both national and regional level. However, there are still challenges that are laying back the harmonization process in the fight against cybercrimes and threats that affect cyber security within the region. The following are among the recommendations that are suggested in having an effective and efficient ICT infrastructure in
combating cybercrimes as well as ensuring the harmonization of cyberlaws in East Africa.

6.8.1 Addressing the Existing Legal Gaps

Currently, there is gap analysis which is ongoing especially to matters relating to breach of ICT laws. NITA-Uganda is working towards the introduction of the aspect of “mutual assistance or cooperation” which will cause the repatriation of suspects who may want to evade persecution. This is because most of these cybercrimes are cross-border, and need the cooperation and assistance from or between countries where they have been committed.

6.8.2 Capacity and Resource Building

This involves continuous training of law enforcement agencies such as Police, Defence, Judiciary and Prosecutors (DPP) among others on understanding cyberlaws, and effective adjudication of these laws. Government in turn should endeavor to provide more IT equipment to these law enforcement agencies to smoothen their operations, and have the equipment availed to different parts of the country.

6.8.3 Strengthening Law Enforcement Institutions

There in need to give support both in terms of personnel and equipment so as to strengthen these agencies in the fight against cybercrimes. This is especially for Police operating outside the capital city, Kampala. They lack the knowledge and equipment in the fight against cybercrimes. On the side of the Judiciary, continuously facilitate them since they are responsible for the prosecution of the culprits who have been accused of such crimes. It is critical to put in place mechanisms to ensure involvement of people of different positions from the EAC Member countries to collectively find solutions to cyber-security challenges in the region.
CHAPTER SEVEN

OVERALL CONCLUSIONS AND RECOMMENDATIONS

Abel Juma Mwiburi and Hamudi Ismail Majamba

7.1 General Conclusion

As emphasized in this study, combating cybercrimes and enhancing cyber-security is no longer a national matter but a global concern. Therefore, countries need to combine efforts in addressing the issue. This is true for EAC Member States since it is better for the interests of the Community that there is minimal criminal activity. The EAC is also bound to provide services to its citizens and in the course provide a safe environment at both the regional and international levels.

This study has revealed that EAC Member States depend on each other in the fight against cybercrimes. It is until such efforts are realized and the cyberlaws are harmonized when the war towards cybercriminals may be said to be won. As revealed from the study, currently there are challenges when trying to address cybercrimes involving other regional states due to the fact that these crimes are defined and punished differently in the EAC States. What is a cybercrime in Kenya may not be a crime in Rwanda or Burundi.

Even though individual EAC Member States are making efforts in addressing cybercrimes at their national level more needs to be done towards establishing effective cooperation channels among each other. The institutions tasked with the research, investigation and prosecution of these offences should work with greater synergy. The study has identified a number of initiatives made and areas of convergence and divergence, challenges and proposed some direction in addressing these.
7.2 Initiatives to Harmonize Cybercrimes Legislation in East Africa

Efforts to harmonize cybercrimes in East Africa countries, that is to say, Kenya, Tanzania, Uganda, Rwanda and Burundi are ongoing. These countries have been using a multi-stakeholder approach that involves the Government, Industries and civil society organizations in combating cybercrimes. Some of the efforts that have been done so far are:

- Formulation of an East African Community Cyber Security Management Task Force, which is chaired by Kenya. The Task Force has the aim of coordinating activities aimed at rooting out cybercrimes in the five East African Community Members. It deals with cyber-security at legal, policy and regulatory levels.
- The East African countries, have also agreed to set up Computer Emergency Response Team (CERTS) to fight cybercrimes. The help of International Telecommunication Union (ITU) through East Africa Communication Organizations congress (EACO) will establish such programmes.
- In Kenya, for example, Kenyan Network Information Center (KENIC) which works under Ministry of Information Communication and Kenyan Police has established a Computer Response Team (CSIRT) to relay computer and network related security threats, and vulnerabilities to the local internet communities.
- Legislation of cybercrime and computer related Laws to facilitate security and combat cybercrimes. Legislation on cybercrimes in most African countries are to a very large extent similar. The reason is that they are legislated under model laws depending on which model law each country has subscribed to. For example, Tanzania has enacted the Cybercrimes Act and the Electronic transactions Act, the National Payments System Act, 2015 and

---

the National Payment Systems Regulation, 2015. In Kenya there is the Computer Misuse Act and Uganda has enacted the Computer Misuse Act of 2011.

7.3 Areas of Convergence and Divergence on Cybercrime among the EAC Partner States

There are various areas of convergences and divergences when the EAC Partner States’ pieces of legislation are compared and contrasted.

7.3.1 Areas of Convergence

a) All countries provide for basic cybercrimes such as unauthorized access to computers or computer network.

b) The regimes recognize admission of electronic evidence in court as a means of ensuring successful prosecution of cybercrimes.

c) The Partner States clearly outline aggravating cybercrimes. These mostly relate to terrorism and treason perpetrated through cyberspace. The punishments under these crimes are more stringent so as to act as deterrence.

d) The legal regimes on cybercrime take into consideration social aspects such as children rights, human trafficking, genocide and xenophobia among others. This is as a matter of public policy and public morality.

e) In countries that have specific laws on cybercrime, there is fixed definition of cybercrime, which is open-ended to accommodate new and emerging forms of cybercrimes.
7.3.2 Areas of Divergences

a) The countries differ in legal systems as regards legal instruments regulating cybercrime. Some countries have a specific law regulating cybercrime while others rely on provisions from various laws. Sudan and Burundi do not have specific laws whereas Rwanda, Uganda, Kenya and Tanzania have Cybercrime laws. It is, however, discernible that all countries intend to move to the position where there is regulation of cybercrime by a specific law.

b) The laws differ greatly in regard to the crimes that they provide for as cybercrime. The descriptions in Kenya legal regime provides a wider scope of cybercrimes such as unauthorized disclosure of password or access code, cybersquatting, phishing, wrongful distribution of obscene or intimate images, among others. The other jurisdictions provide a narrow scope. This can be attributed to the level of cyber-attacks stomached by Kenya since it is the most developed in the region and the fact that their law is as recent as 2018. This, therefore, calls for harmonization of laws within the various States to cater for emerging trends.

c) The countries differ in regard to the punishments accorded to cybercrimes. Kenya has the more punitive sentences with up to $100,000 and custody of 25 years for cybercrime. Tanzania follows with fines of up to $8000 and sentences of 7 years. Uganda has fines of up to $2000 and sentence of 15 years, except that for offences against critical/protected information infrastructure, Uganda has life imprisonment as punishment. The countries fail to address the issue of jurisdiction in regard to cybercrime. Some legal regimes provide for trans-boundary jurisdiction such as Tanzania under Section 30 of the Cybercrimes Act, 2015. This is not the case with other jurisdictions such as Burundi.

---

244 See section 20(1) of the Computer Misuse Act, 2011.
7.4 Challenges Facing the EAC in Harmonizing Cybercrimes Laws

7.4.1 Civil and Common Law Systems in the EAC

In the EAC, there are two different legal systems used by the Member States. Kenya, Tanzania, and Uganda follow a common law system, while Burundi and Rwanda both subscribe to a predominantly civil law system. The divergent legal systems have contributed to slowing down the process of harmonization efforts in the region.

7.4.2 Lack of Resources and Capacity for Technological Advancements

Apart from Tanzania, Uganda and Kenya other Rwanda and Burundi have not established the Single Window System in customs administration. These have remained as a challenge for automation of ICT in customs administration among the EAC Partner States making the older systems vulnerable to corruption and other cybercrimes.

7.4.3 Slow Progress in Passing Laws and Implementation

The EAC Partner States have been discussing cyber-security and drafted the East African Community Electronic Transactions Bill of 2014 that has not been assented to by the Heads of States of the Partner States. This poses a grave challenge to the cooperation between States to prevent cybercrimes and makes harmonization of laws on cybercrimes difficult. The progress on cyber-security within the EAC is extremely slow.

7.4.4 Lack of Political Commitment

Most EAC Partner States do not have the desire to advocate for harmonization of cyberlaws. Legislative organs in individual states can only enact cyberlaws to advance their political interest. A good
example is the Cyber Crimes Act 2015 of Tanzania which was viewed to be more political than technical. It is criticized for harsh provisions that stifle freedom of expression and deter dissenting voices in the country.

7.4.5 Territoriality

Cybercrime is trans-territorial in nature. Harmonization of cyberlaws means States are to yield to a legal regime that allows for destruction of the physical boundaries of States, a practice that does not augur well with African leaders. This, coupled with the mistrust among Member States, hinders harmonization of cyberlaws.

7.4.6 Budgetary Constraints and Balancing of Interests

The EAC lacks appropriate funding to ensure adequate harmonization of cyberlaws. The process requires sensitization, review meetings and various expenses. Harmonization of cybercrime, therefore, cannot be prioritized in the budgetary process against other aspects such as movement of labour.

7.4.7 Underdeveloped ICT Infrastructures

Partner States lack efficient infrastructure for which cyber-security should be put in place let alone harmonized. The countries have underdeveloped ICT infrastructures and lack the institutional capacity to implement any legislation that may be put in place by the EAC.

---

7.4.8 Lack of Basic Legal Regimes in Individual Partner States

Some EAC Partner States lack basic regimes on cybercrime. One cannot speak of harmonizing cyberlaws whereas countries like South Sudan do not have any law or regulation speaking about cybercrime.\footnote{Symnatec Corporation. (2016), supra p. 57.}

7.4.9 Absence of a Body Mandated to Harmonize Cyberlaws in East Africa

Unlike SADC, the EAC does not have a body purposely in place to harmonize cyber-laws. The load is left to the subcommittee on harmonization and approximation of laws, which has clearly reported that the process is cumbersome.\footnote{See generally Bande, L.C “Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities,’ International Journal of Cyber Criminology Vol. 12 Issue 1 Jan-June 2018, available at: https://www.cybercrimejournal.com/BandeVol12Issue1IJC2018.pdf, accessed on 29th November 2019.}

7.4.10 Cybercrime and Restraint of Human Rights

Most of the EAC Partner States resort to enactment of cybercrimes in order to crack down on essential freedoms such as the right to privacy, access to information and chiefly freedom of speech. The Cybercrime Act, 2015 of Tanzania and the Burundi Penal Code provisions on electronic media reveal a picture of the government trying to violate rights of individuals with wanton powers of seizure and arrest in relation to cyber-related activities.

This is a big hindrance to harmonization as the laws are only meant to protect interests of the government instead of addressing the issue of harmonized position on cybercrime.
7.4.11 Addressing the Challenges

To combat all these challenges of evolution of cybercrimes and development of technology, there must be taken various steps that must be taken as a way forward to overcome the same. These are enumerated below as follows:

7.4.12 Continuous Training of EAC Officials from Judiciary to EALA

The phenomenon of cybercrime is still relatively new to the African continent. The members of the EAC organs require continuous training to acclimatize with the peculiar nature of cybercrimes and mode of enforcement.

7.4.13 Enactment of Soft Law on Harmonization of Cybercrime

Soft law is a phenomenon that covers all social rules generated by States which are not legally binding but which are nevertheless of special legal relevance. These include codes, charter of rights, among others. This approach has been taken by South Africa as seen from use of soft law such as SADC Code on Social Security and the Charter on Fundamental Social Rights in SADC, United Nations Commission on Trade Law. This soft law can in most cases set the stage for future laws or Protocols in the EAC.

7.4.14 Soliciting for Partnerships and Working Relationships with other Jurisdictions

This will assist in developing a harmonized regional framework. Technical and financial support from the United States of America has

---


249 Ibid.
been suggested as a solution to developing strong cyber-security legislation in Regional Economic Communities in Africa.\textsuperscript{250}

### 7.4.15 Use of National and Regional Courts of law

Citizens from the EAC Partner States should file cases challenging cyberlaws with draconic provisions and have them adjudicated and decided by courts. This will set an appropriate jurisprudence that can be taken as the law on aspects of cybercrime. A case in point is the case of \textit{Burundi Journalists Union vs. the Attorney General of the Republic of Burundi, Reference No. 7 of 2013}. In the said case, the East African Court of Justice nullified parts of Law No.1/l/025 of 4\textsuperscript{th} June, 2013 of the Republic of Burundi that set out onerous and restrictive provisions against print and web media under the guise of computer crimes.

### 7.4.16 Ratifying Regional and International Instruments

The EAC Partner States can agree to adopt international instruments that provide for a harmonized system and regulation of cybercrime. This averts the burden of promulgating a fresh law.\textsuperscript{251} For instance, none of the EAC Partner States has ratified the African Union Convention on Cyber Security and Personal Data Protection, (Malabo Convention) 2014.\textsuperscript{252} The Malabo Convention establishes a legal framework for cyber-security and personal data protection by African Union Member States at sub-regional, regional and international level in an attempt to build a viable information society.

Efforts have also been made at the international level to build a commendable cyber-security framework which aggressively monitors and regulates the cyber-environment. The adoption of the Budapest Convention on Cybercrime of 2001 which is the first international

\textsuperscript{250} Terebey, S., (2017), supra.
\textsuperscript{251} Ibid., p. 140.
\textsuperscript{252} See: https://au.int/en/treaties, accessed on 17\textsuperscript{th} January 2019.
Treaty on crimes committed via the internet and other computer networks illustrates one of these initiatives. However, none of the EAC Partner States has adopted the Convention, as a non-member of the Council of Europe.253

Conventions developed at the regional and international levels would certainly form a strong basis in guiding the harmonization process of EAC cyberlaws thus providing grounds for the investigation and prosecution of cybercrimes at both domestic and international level. Therefore, obtaining international collaborations can facilitate in the combating of cybercrimes through ratifying these Conventions.

### 7.4.17 Cooperation with International Bodies

The EAC can initiate cooperation with other international bodies in order to have harmonized cybercrime laws. Cooperation with bodies such as the International Criminal Police Organization (INTERPOL), International Telecommunications Union (ITU) and the World Trade Organization to assist in coming up with a common position on cybercrime is vital.

### 7.4.18 ICT and Cyber-Security Education

The growth and advancement of technology and use of cyberspace in East Africa are not matched by the necessary skills to prevent commission of cybercrimes.254 East African countries need strong information and computer technology institutions so as to train cyber security experts and personnel with a strong expertise in system administration so as to deal with present and future challenges of cybercrime.255

---


254 Ibid.

7.4.19 Engagement of Key Stakeholders

It is important to engage important stakeholders, as cyber-security regulation cannot be placed on one man’s shoulders or institution. Combating cybercrimes requires the concerted efforts of members of the public, the Judiciary, the Executive, the Parliament, young people, law enforcers, academics and lawyers, to mention a few.

At the EAC level, despite the efforts made by the Partner States and EAC organs, cybercrimes’ common regime is a long way from being harmonized. This is mainly because of the attitude rendered to it where people perceive it as an issue regarding technology but far from the reality of free movement of factors of production in the Community.

Cybercriminals come up with new tactics on almost a daily basis while at the same time the technology is ever changing. Hence, it is essential that those combating cybercrimes are ahead of the game.

We conclude by pointing out the obvious: That the findings of this study have probably brought to light just a tip of ice-berg on the state of affairs relating to harmonization of EAC cybercrime laws, having been based on select Members States in the EAC. It is hoped that it will, nevertheless, trigger thoughts and open up more curiosity and consequently further research in this critical area.
Kenya


Waema, M.T. and Ndung’u, N. M. (2012), Understanding what is happening in ICT in Kenya, Research ICT Africa, (Available at
Tanzania


**Rwanda**


UNESCO, “Country Profile- Rwanda”, October 2017


**Uganda**


EAC Secretariat, Draft: EAC Legal Framework for Cyberlaws. EAC IRC Repository, UNCTAD and EAC, 2008 (Available at http://repository.eac.int/).


NITA-Uganda, National Information Technology Authority (NITA-) FY 2015/16 Annual Report (Available at
https://www.nita.go.ug/sites/default/files/publications/FY%202015_16%20ANNUAL%20REPORT%20FINAL.pdf/.


Burundi


ANNEXURE ‘A’ – SAMPLE INTERVIEW GUIDE

Harmonization of Cyberlaw among EAC Member Countries:
Multi Jurisdiction Initiatives in Combating Cyber Welfare Project

(KEY INFORMANT INTERVIEW GUIDE)

SEMI-STRUCTURED INTERVIEW GUIDE

Introduction (Salutation)
My names are...............................................................
I am a Research Assistant and a member of the research Team of the University of Dar-es-Salaam School of Law that has been commissioned to undertake a study on Harmonization of Cyberlaw among EAC Member Countries.

Overview of the Project/Study:
Most governments in Africa have promulgated legislation to regulate challenges that have emerged with the advancement on ICT and cyber related issues. Some of the challenges that have plagued many of the government is the loss of their borders in the cyber world and their citizens interact freely all over the world. Consequently, the governments’ efforts in addressing cyber welfare are rendered insufficient, as they are limited to their borders.

One of the strategies of overcoming the border challenge is by a process of harmonizing cyber legislative frameworks and working together in a situation where there are no border barriers, in addressing cyber welfare.

Governments in the East African region, under the auspices of the East African Community (EAC) have enacted cyber regulations. Efforts have been made under the Treaty Establishing the EAC to ensure that the laws are harmonized in efforts to create a 'Geo-World,’ enclosing one
merged border among themselves and hence having same jurisdiction implementations as far as cyber welfare is concerned.

**Regional Integration Initiatives**
There have been some efforts to harmonize cyberlaws in the East African Region. The notable initiative was done through the East African Development Strategy (2011/12 – 2015/16) which proposed that the key drivers for the realization of the EAC regional integration agenda in the next five years include, among others, creation of a strong legal framework. Strong legal framework underpins the need to harmonized legal framework, including cyberlaws.

Despite various efforts to harmonize cyberlaws in the EAC region, this ambition has never been fully and effectively realized. This is mainly due to the fact that member States are at various levels in enacting the national member states are at various levels in enacting the national cyberlaws.

**Objectives**
The main objective of this study is to undertake a study which focuses on the extent to which EAC countries have harmonized their legal, policy and institutional frameworks on cybercrimes.

Among the key institutions that have been targeted for purposes of getting data for the study include law enforcement organ/s, regulatory authorities charged with ICT, Central Banks, legislatures, judiciary, and stakeholders in the private sector dealing with ICT/telecommunications, among others, in each of the select States.

Our study seeks to probe onto the efforts that have been made in the EAC partner states to harmonize the Laws and identify challenges that still exist with a view to devising mechanisms to address such challenges. We need to know the factors that have made it difficult to meet this objective in each State by conducting.
Our main focus is to identify factors that have made it difficult to meet this objective in each State in implementing the obligations outlined in the Treaty Establishing the EAC with specific emphasis on the theme — Harmonizing laws on cybercrimes within the EAC jurisdiction.

One of the methodologies to get the information required is to interview select (Key) officials that we have targeted in institution dealing with enforcement of cyberlaws within the select EAC partner States.

The findings of the study will be shared with stakeholders in a validation workshop and there after we intend to disseminate the findings through a report and publication of papers.

**Leading question:**
Do you consider as the main challenges in addressing cybercrimes in your country?

**Checklist of issues:**

A

1. Do you perceive any challenges, which relates to laws, policy, and institutions in combating cybercrimes in your country?

2. Have these challenges been discussed in forums – probe on which forums, national, sector level?

3. Are you aware of any initiatives at the EAC level to address the challenges – which are these, has your institution been involved in any of the initiatives?

4. What How are the challenges being addressed is the problem affecting the day-to-day rights of workers in your Institute? (Probe for reasons and explanation for both YES and NO)
5. Do you think it interferes with the process of attaining the EAC objectives and goals –How?

6. What do you think is the main reason behind the lack of implementing the EAC initiative to harmonize laws and policies to address cybercrimes in your country?

7. Do you think you have any role to play in addressing the problem in your organization? (Probe for reasons, strategies and whether the mandate to do that is there, if not to propose how things could be made easier for people in different position to participate in the interventions)

8. Are there any specific programmes/interventions on cybercrimes that are being taken/implemented by your institution to address the challenges?

9. What is your opinion on the relevance and effectiveness of the steps стрategies (rules and regulations) adopted by your institution to address the identified challenges?

10. Do you think that the measures adopted by your institution/country are enough? Do you have any suggestions as to how more effective measures could be adopted?

B
1. Are you aware of the legislation, policies and institutional framework, which seek to address cybercrimes in your country? – In your opinion are these adequately equipped to combat cybercrimes and related challenges?

2. In your opinion what do you consider to be the most appropriate way to deal with the challenges?
C

1. Being one of the key stakeholders in the institution addressing cybercrimes in your country, what do you think will be the best way to deal with the problem at your Institution?

2. There are several intervention programmes adopted by the EAC States, are these effective? What do you recommend for improving the coordinated efforts/strategies at the level of the EAC Partner states in addressing the challenges?

Interviewer to probe on any other matter/opinion that the interviewee wishes to express

Seek and collect any Reports that have a bearing on the theme from the interviewee/institution.

Thank the interviewee for his/her time, and input and promise to revert when report is ready for stakeholders’ validation workshop and thereafter.
1.0 ABOUT THE PROJECT

1.1 Introduction and Background to the Project

EAC Countries have made a number of to harmonize their laws in an attempt to comply with the EAC Treaty. However challenges still exist in each of the Partner States of the EAC. These challenges are different in each of the State. This study intends to probe into factors that have made it difficult to meet this objective in each State by conducting a field research which would entails interviewing select officials in targeted Institution dealing with enforcement of cyberlaws.

1.2 Objectives of the Project

The Study seeks to undertake a study focusing primarily on the extent to which EAC countries have harmonized their legal, policy and institutional frameworks on cybercrimes as required by the Treaty Establishing the EAC.

2.0 SPECIFIC DUTIES AND RESPONSIBILITIES

I. Study and understand the Project’s objectives and expected outcomes.

II. Diligently collect primary data from the relevant offices through interviews and other possible means of field data collection.
III. Reporting any reasonable challenges or concerns encountered in the field before acting upon them.
IV. Documenting and reporting the findings obtained from the field on time.

3.0 DELIVERABLES
A final field report in soft copy via (email) within the specified time frame.

4.0 REPORTING
The research assistant shall report to the Principal Project Investigator.

5.0 TIMEFRAME
The task is expected to take place and be accomplished within the period of TWO calendar months to end in 30th April 2019.

6.0 PAYMENT MODALITIES
The research assistant shall be paid a total amount of 500,000 TZS for the task.

7.0 OWNERSHIP OF WORK
The entire work performed by the research assistant pursuant to this agreement becomes the property of the University of Dar es Salaam School of Law.

8.0 PROPRIETARY AND CONFIDENTIAL INFORMATION
All proprietary and confidential information relating to University of Dar es Salaam School of Law or its activities in the possession of or provided to the research assistant pursuant to this agreement, whether provided before or after this agreement and whether oral or written, shall not without the prior approval of the University of Dar es Salaam School of Law be used or disclosed by the research assistant to anyone for
any purpose other than in connection with her/his performance of obligations under this agreement.

9.0 ENTIRE AGREEMENT
This agreement constitutes the entire agreement between the parties and shall not be changed, modified, amended, extended, waived or discharged except by a written instrument signed by the parties herein.

IN WITNESS WHEREOF, the parties hereto execute this agreement or has caused this agreement to be executed by its duly authorized Officer on the day and year herein below written.

SIGNED BY THE PRINCIPAL INVESTIGATOR

.......................... ........................................
ON BEHALF OF UNIVERSITY OF DAR ES SALAAM SCHOOL OF LAW

DATE

SIGNED BY THE RESEARCH ASSISTANT

.......................... ........................................
RESEARCH ASSISTANT

DATE