

Schriften zum Strafrechtsvergleich

Band 5

**Preventing and Combating Cybercrime
in East Africa**

Lessons from Europe's Cybercrime Frameworks

By

Abel Juma Mwiburi



Duncker & Humblot · Berlin

ABEL JUMA MWIBURI

Preventing and Combating Cybercrime in East Africa

Schriften zum Strafrechtsvergleich

Herausgegeben von

Prof. Dr. Dr. Eric Hilgendorf, Würzburg und
Prof. Dr. Brian Valerius, Bayreuth

Band 5

Preventing and Combating Cybercrime in East Africa

Lessons from Europe's Cybercrime Frameworks

By

Abel Juma Mwiburi



Duncker & Humblot · Berlin

The Faculty of Law and Economics of the University of Bayreuth
accepted this work as thesis in the year 2018.

Bibliographic information of the German national library

The German national library registers this publication in
the German national bibliography; specified bibliographic data
are retrievable on the Internet about <http://dnb.d-nb.de>.

All rights reserved

© 2019 Duncker & Humblot GmbH, Berlin
Typesetting: L101 Mediengestaltung, Fürstenwalde
Printing: buchbücher.de gmbh, Birkach
Printed in Germany

ISSN 2364-8155

ISBN 978-3-428-15601-6 (Print)

ISBN 978-3-428-55601-4 (E-Book)

ISBN 978-3-428-85601-5 (Print & E-Book)

Printed on no aging resistant (non-acid) paper
according to ISO 9706 ☺

Internet: <http://www.duncker-humblot.de>

*To my parents Juma Chazenga Mwiburi and
Faustina Zablon Msangi;
my wife Violeth Zacharia Mwiburi and
my children Abigail, Aaron, Abdiel, and Ariel*

Foreword

Technological development in the world has tremendously assisted human beings to improve their lives in various sectors from engineering, medicine, law to performing arts. Huge search engines are making research take shorter time than before as the whole world is at your desk. In the older days, when the Radio could also play music on a tape and also record sounds we all thought we are at the edge of the highest level of science. However, the human mind is restless and probes further. Currently, your simple smart phone in your hand can do hundreds of functions. It is your communication device, your camera, your Television with all facilities, device for playing games etc. There is no doubt that we are enjoying the highest level of scientific advancement making our lives easy, enjoyable at affordable level.

However, advancement in science comes with its twin brother/sister – crime. The same device can make your life miserable through abuse of advancement in science. This can happen through cybercrime – the topic chosen by Dr. Abel Juma Mwiburi for this book. The cyber space – the fifth and newest space to be accessed by human beings after land, sea, air and outer space can be accessed via internet. The problem is once a person is on the internet he or she is vulnerable and defenceless potential victim of cybercrime.

Those involved in cybercrime target governments and individuals as well. The motive might be political, criminal or social. Politically, we have witnessed elections in powerful States being influenced from thousands of kilometres through internet. This is because cybercrime, like air pollution, knows of no borders and crosses from one country to another without visas. Criminals are accessing Credit Cards and Bank Accounts of unsuspecting people and emptying them. At personal level, couples are harassing each other through the internet. Recently, a newspaper explained “How husband’s two years of e-mail terror turned wife towards suicide.” It is bad.

Faced with such a threat, Dr. Mwiburi makes a strong case for the States in East Africa to work together to address this threat. He notes that notwithstanding their technological backwardness, East African States, while having diverse national frameworks, have not developed a strong joint regional legal framework to address cybercrime. He recommends that the region take leaf from European Union where they have successfully worked together and established effective institutions to fight cybercrime. This is a timely clarion

call which should be taken seriously. That is the value of this book. The author has managed to reduce heavy scientific material into simple language understandable to all. It is a must read for all those interested in understanding this menace – which is always around us!

Dar es Salaam, December 2018

*Chris Maina Peter**

* Professor of Law, School of Law, University of Dar es Salaam, Tanzania; and Member, United Nations International Law Commission (ILC).

Acknowledgements

This book would have not been fruitful, if the required support was not offered by colleagues and friends. First of all, I am very grateful to the financiers of my Ph.D. studies, the Government of the United Republic of Tanzania, and the Federal Government of Germany through the Tanzania-Germany Postgraduate Training Programme 2015. Without their financial support, realizing this dream would have not been possible.

More importantly, I am sincerely grateful to Prof. Dr. Brian Valerius, my Ph.D. supervisor, and academic mentor. Prof. Dr. Valerius unswervingly offered his support and guidance to me in a very friendly and flexible manner. He was always close and available whenever I sought his guidance. I am very proud to pursue my doctoral studies under his academic guardianship.

Also, I thank my family for heartening me and being relentlessly supportive, especially, whenever I seemed to lose hope. My wife, Violeth and my children, Abigail, Aaron, Abdiel and Ariel endured tough moments of my absence with firm and sincere hope that this undertaking will end fruitfully.

In similar vein, I extend my appreciations to Prof. Dr. Hamudi Majamba, the Dean of the University of Dar es Salaam School of law. Prof. Dr. Majamba accorded me his full support, inspiration, and guidance. Also, I am indebted to Prof. Dr. Ulrike Wanitzek who deserves a special mention for both motherly and academic guidance and support during my studies at the University of Bayreuth. Exceptionally, I further extend my sense of appreciation to my friend and colleague, FAYaz Bhojani, and FB Attorneys, for their all sorts of support and encouragement in making this project successful.

In a very special way, I would like to thank my colleague and friend, Comrade Dr. Goodluck Kiwori, with whom I traveled miles of plains, hills, and slopes when he was undertaking a similar project at the University of Bayreuth. We engaged each other with constant and productive consultations which were very helpful in molding our studies. It is my earnest admission that I cannot account for his unwavering contribution towards the completion of this book.

Lastly, I appreciate a hand of support extended by my friends and colleagues, Dr. Alexander Saba, Dr. Mary Zacharia, Imani Shayo, Kimatha Said Kimatha, Amani Lwila, Veronica Buchumi, Goodluck Temu, and Florencia Kimario. Also, I admit that it is not humanly possible to mention all those

who rendered assistance in the preparation and completion of this work. For that reason, I generally thank all those who made this work possible.

I would like to finally state that the order in which my appreciations are expressed herein is not, anyhow, an attempt to rank the importance or the extent of support rendered, rather it becomes necessary to do so for convenience and portrayal purposes. Otherwise, to all of you, I say, *“thank you so much”*.

Table of Contents

Chapter 1

General Introduction	19
A. General Introduction and Background	19
B. Cybercrime as a Challenge in East Africa and Beyond	21
C. Focus of the Book	23

Chapter 2

Cyberspace as an Emerging Phenomenon in Criminal Jurisprudence	25
A. Introductory Remarks	25
B. Understanding Cyberspace, Computer Crime, and Cybercrime	26
I. Cyberspace	26
II. Computer Crime and Cybercrime	28
C. Nature and Evolution of Modern Cybercrime	30
I. Nature of Cybercrime	30
II. Evolution of Modern Cybercrime	31
1. The Era of Mainframe Computers	32
2. Evolution of Networked Computers	32
3. The Epoch of Personal Computers and the Internet	33
D. Forms of Cyber Criminality	34
I. Categorization by Individuals and Experts	34
II. Categorization by Institutions	37
III. General Observations from the Categorization	38
E. Features of Cybercrimes	39
I. Cybercrimes are Committed in Computer Environment	39
II. Veil of Anonymity	40
III. Requirement of Technical Knowledge	41
IV. Cybercrimes are Easy to Commit	41
V. Cybercrime as a Cross-Border Phenomenon	42
F. Approaches to Cyberspace and ICT Governance	43
I. Regulation by Norms	45
II. Regulation by Law	46

III. Regulation by Market Forces	46
IV. Regulation by Code or Architecture	47
V. Pillars of Cybersecurity	47
G. Contemporary Issues and Challenges on Cyberspace	48
I. Borderlessness and Jurisdictional Issues	49
II. Harmonization of Laws	49
III. Speedy Technological Developments and Flexibility	51
IV. Striking a Balance Between Regulation and Enjoyment of Individual Rights	52
V. Increased Criminal Capability and Child Protection	53
VI. Anonymity and Lack of Statistics	54
H. Concluding Remarks	55

Chapter 3

**Systemic and Institutional Synergies
Among the East African Community, the European Union and
the Council of Europe** 57

A. Introductory Remarks	57
B. The East African Community	57
I. The East African Community in Historical Perspectives	57
II. Revival of the East African Community	61
III. Principles Governing the East African Community	63
IV. The East African Community's Organs and Institutions	65
V. Scope and Competences of the East African Community	69
C. The European Union	71
I. History and Establishment of the European Union	71
II. Principles Governing the European Union	78
III. European Union's Organs and Institutions	80
IV. Competencies and Functions of the European Union	83
D. The Council of Europe	88
I. History and Establishment of the Council of Europe	88
II. Principles Governing the Council of Europe	91
III. Council of Europe's Organs and Institutions	91
IV. Competencies and Functions of the Council of Europe	93
E. Synergies Among the East African Community, the European Union, and the Council of Europe as Intergovernmental Organizations	94
F. Concluding Remarks	96

Chapter 4

**The War Against Cybercrime:
Europe's Legal and Institutional Frameworks** 100

A. Introductory Remarks	100
B. General Background to the Cooperation in Criminal Matters Among the Council of Europe Member States	101
C. The Council of Europe Convention on Cybercrime	102
I. Harmonization of Rules and Criminalization of Some Acts	104
II. Criminal Procedural Issues	107
III. International Cooperation in Cybercrime and Related Matters	108
IV. The Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems	109
D. Institutions Under the Council of Europe Cybercrime Framework	111
I. European Committee on Crime Problems (CDPC)	111
II. Cybercrime Convention Committee (T-CY)	113
III. Directorate of Information Society and Action Against Crime	115
IV. Cybercrime Programme Office of the Council of Europe (C-PROC) ..	115
E. Historical and Legal Basis of Cooperation in Penal Matters Among the EU Member States	117
F. An Overview of the European Union's Cybercrime Framework	121
I. The European Union's Cybercrime Legal Framework	121
1. Council Framework Decision on Combating Fraud and Counterfeiting of Non-Cash Means of Payment	122
2. Council Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography	123
3. Framework Decision on Attacks Against Information Systems	125
4. Directive of the European Parliament and the Council on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA	126
5. Council Framework Decision on Combating Certain Forms and Expressions of Racism and Xenophobia by Means of Criminal Law	128
G. Cyberlaw Enforcement Mechanisms and Institutions Under the European Union	129
I. The European Arrest Warrant (EAW)	129
II. The European Police College (CEPOL)	130
III. The European Police Office (Europol)	131
IV. Eurojust	133
V. European Union Agency for Network and Information Security (ENISA)	134
VI. European Crime Prevention Network (EUCPN)	135
H. Concluding Remarks	137

Chapter 5

Preventing and Combating Cybercrime in East Africa: Legal and Institutional Frameworks	139
A. Introductory Remarks	139
B. Rationale for Approximation and Harmonization of Criminal Laws in the EAC	141
C. Legal Basis for Harmonization and Approximation of Laws in the EAC Framework	143
D. An Overview of the EAC's Anti-Cybercrime Framework	144
I. Policy and Legislative Measures Adopted in the EAC Region.....	145
1. The EAC Customs Management Act, 2004	145
2. The Regional e-Government Framework, 2006	146
3. The EAC Legal Framework for Cyberlaws, 2008	147
4. The EAC Protocol on Peace and Security, 2013	149
II. Anti-Cybercrime Institutions in the EAC.....	150
1. The East African Communications Organisation (EACO)	150
2. The EAC Cyberlaws Task Force	152
E. Individual Countries' Cyberspace Frameworks	153
I. Cybercrime Policy, Laws and Institutions in Tanzania	153
1. The National Information and Communications Technologies Policy, 2003	154
2. The Electronic and Postal Communications Act, 2010	156
3. The Cybercrime Act, 2015	157
4. Tanzania Communications Regulatory Authority	162
5. Tanzania Cybercrime Unit	163
II. Cybercrime Policies, Laws and Institutions in Kenya	164
1. National Information and Communications Technology Policy, 2006	165
2. The Kenya Information and Communications Act, 1998	166
3. The National Cybersecurity Strategy, 2014	168
4. The Communications Authority of Kenya	169
5. Kenya Cybercrime Unit	170
III. Cybercrime Policies, Laws and Institutions in Uganda	170
1. The National Information and Communications Technology Policy for Uganda, 2014	170
2. National Information Security Strategy, 2011	172
3. The Computer Misuse Act, 2011	173
4. The Uganda Communications Commission	180
5. The National Information Technology Authority, Uganda	181
6. Uganda Cybercrime Unit	182
F. Concluding Remarks	182

Table of Contents	15
-------------------	----

Chapter 6

Comparative Assessment of Anti-Cybercrime Initiatives Between Europe and East Africa	184
A. Introductory Remarks	184
B. Basic Integration Frameworks Among the EAC, EU, and CoE	184
C. Approximation and Harmonization of Laws in Europe and East Africa	186
D. Comparison of the Efficiency and Efficacy of Anti-Cybercrime Legisla- tive Measures in Europe and East Africa	188
I. Substantive Cybercrime Provisions	188
II. Proportionality of Sanctions and Other Dissuasive Measures Against Offenders	198
E. Efficiency and Efficacy of Anti-Cybercrime Enforcement and Institu- tional Mechanisms in Europe and East Africa	205
I. Anti-Cybercrime Watchdog and Coordination Institutions and Mecha- nisms in Europe and the EAC	206
II. Other Anti-Cybercrime Institutions	209
F. Concluding Remarks	213

Chapter 7

General Conclusion	215
References	220
List of Cases	231
List of Legislation	232
Online Materials	235
Subject Index	240

List of Tables

Table 1:	List of the Current EU Members and Their Year of Admission	77
Table 2:	List of Categories and Areas of Competencies in the EU	85
Table 3:	The Current Member States of the Council of Europe	89
Table 4:	Sanctions Under the Computer Misuse Act, 2011	178
Table 5:	Comparison of Cybercrime Regimes Between the CoE and Selected EAC Countries	190
Table 6:	Proportionality of Sanctions and Other Dissuasive Measures Against Offenders Between the CoE and Selected EAC Countries	199

List of Abbreviations and Acronyms

ACCP	African Centre for Cyberlaw and Cybercrime Prevention
ARPANET	Advanced Research Projects Agency Network
CAK	Communications Authority of Kenya
CDPC	European Committee on Crime Problems
CEPOL	European Police College
Chap.	Chapter
CoE	Council of Europe
C-PROC	Cybercrime Programme Office of the Council of Europe
CSIRT	Computer Security Incident Response Team
DPP	Director of Public Prosecution
EAC	East African Community
EACJ	East African Court of Justice
EACO	East African Communications Organisation
EACSO	East African Common Services Organization
EALA	East African Legislative Assembly
EARPTO	East Africa Regulators, Postal and Telecommunication Operators Organisation
EAW	European Arrest Warrant
EC3	European Cybercrime Centre
ECSC	European Coal and Steel Community
ED/EDS	Editor/Editors
EEC	European Economic Community
ENISA	European Union Agency for Network and Information Security
EU	European Union
EUCPN	European Crime Prevention Network
EURATOM	European Atomic Energy Community
Europol	European Police Office
FIU	Financial Intelligence Unit
GDP	Gross Domestic Product
ICT	Information and Communications Technology
INTERPOL	International Criminal Police Organization
IT	Information Technology
ITU	International Telecommunication Union

KES	Tanzanian Shilling
LHRC	Legal and Human Rights Center
NATO	North Atlantic Treaty Organization
NBC	National Bank of Commerce
NISS	National Information Security Strategy (Uganda)
NITA-U	National Information Technology Authority, Uganda
NMB	National Microfinance Bank
OECD	Organization for Economic Cooperation and Development
PC-CY	Committee of Experts on Crime in Cyberspace
TBA	Tanzania Bankers Association
TCRA	Tanzania Communications Regulatory Authority
T-CY	Cybercrime Convention Committee
TZS	Kenyan Shilling
UCC	Uganda Communications Commission
UGX	Ugandan Shilling
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNODC	United Nations Office on Drugs and Crime
Vol.	Volume
vs.	versus

Chapter 1

General Introduction

A. General Introduction and Background

Since men are arguably evil in nature,¹ criminality has the main characteristic of always being attached to human life at all times and circumstances. This is the reason why crimes are committed in both poor and rich countries, the difference being only that levels of development sometimes determine the extent, type, nature and effects of those crimes. Technological developments similarly have been providing fertile grounds for criminals to accomplish their evil missions. Developments in Information and Communications Technology (ICT) were meant to increase, among other things, accuracy, simplicity, and efficiency in various aspects of life. However, despite the fact that the world has registered tremendous achievement in realizing these goals, ICT has also turned into an avenue for criminals, thereby posing incalculable threats to the world through cyber criminality.²

Explaining the complexities of crime, Singh makes the following observations:

Crime is not a single phenomenon that can be examined, analyzed and described in one piece. It occurs in every part of the country and in every stratum of society. The offenders and its victims are people of all ages, income and backgrounds. Its trends are difficult to ascertain. Its causes are legion. Its cures are speculative and controversial. Computer related crimes, popularly called as Cyber Crimes, are most the latest among all the crimes.³

It is a fact currently that almost every aspect of human life interacts with ICT in one way or another. For example, in 2011 and 2014, studies showed that more than one-third of the world's total population had access to the Internet.⁴ Moreover, over sixty percent of all internet users are in developing countries, with forty-five percent of all internet users being below the age of twenty-five years.⁵ Also, it was expected that by 2017 more than seventy

¹ *Paranjape*, p. 1.

² *Mwiburi*, p. 1.

³ *Singh* (2007), pp. 3–4.

⁴ *United Nations Office on Drugs and Crime* (2013), p. 1. Also see: *Chawki*, p. 4.

⁵ *Chawki*, p. 4.

percent of the world's population will be connected to the Internet.⁶ It is further said that, mobile telephone services that are also used to access the Internet, are accessible to ninety six percent of the world's population.⁷

This being the case, there has been a tendency of criminal behaviours to develop simultaneously and instantaneously with the use of the technology, a situation which calls for more serious and concerted efforts to address. This is because of the fact that criminality is becoming very common in the area (cyberspace) where a significant portion of the world's population meets. Perhaps, the worst thing about cyber criminality is the fact that for the perpetrator to commit the intended crime, one must not necessarily be within the locality or jurisdiction where the criminal conduct or its effect occurs, or where the victim of that illegal conduct resides.⁸

Rampancy of cybercrimes globally is one of the reasons that have attracted individual and collective global initiatives and efforts in addressing the problem. Rapid developments in ICTs are considered to be one of the factors contributing to these contemporary emerging trends of criminality.⁹ Associating the developments in ICT and the challenges they pose in criminal jurisprudence, Lunker, observes:

The rapid development of Internet and Computer technology globally has led to the growth of new forms of transnational crime especially Internet related. These crimes have virtually no boundaries and may affect any country across the globe. Thus, there is a need for awareness and enactment of necessary legislation in all countries for the prevention of computer-related crime.¹⁰

Furthermore, one of the challenging characteristics of cybercrime is the fact that it is borderless and cross territorial in nature, and its impacts are much wider than those of traditional crimes.¹¹ This means that while the legal and institutional frameworks are grounded on real geographical locations, cybercrimes are not affected by physical boundaries as such. For that matter, cybercrime poses threats not only to the confidentiality, integrity or availability of computer systems, but also to the security of critical infrastructure.¹² It is for this reason that a call for the fight against this contemporary form of criminality inevitably necessitates employing individual and the collective initiatives and efforts among States at regional and inter-regional levels to combat the same.

⁶ *Chawki*, p. 4.

⁷ *Clough* (2014), p. 699.

⁸ *United Nations Office on Drugs and Crime* (2013), p. 6.

⁹ *Lunker*, *Cyber Laws: A Global Perspective*.

¹⁰ *Lunker*, *Cyber Laws: A Global Perspective*.

¹¹ *Johnson/Post*, pp. 1367–1402.

¹² *United Nations Office on Drugs and Crime* (2011), p. 2.

Emphasizing the seriousness and threats posed by cybercrime, the then Interpol Secretary General observed that:

Cybercrime is emerging as a very concrete threat.... Considering the anonymity of cyberspace, it may, in fact, be one of the most dangerous criminal threats we will ever face.¹³

Similarly, the East African Community (EAC)¹⁴ is not far and safe from what is happening in the world, in terms of technological developments and also criminal threats and trends. The East African region covers a land area of 1.82 million square kilometers and it is home to 149.7 million people.¹⁵ This population as a whole can, therefore, be contemplated as comprising potential victims of cyber criminality. Under the East African Community portfolio, the region has been forging cooperation among Member States in addressing common problems facing its inhabitants. The most recent and remarkable initiative, in so far as a war against cybercrime is concerned, was the Workshop on Effective Cybercrime Legislation in East Africa, held in Dar es Salaam, Tanzania from 22 to 24 August 2013.¹⁶ Since then, there have been hardly very little collective concerted efforts against cybercrime worth reporting in the East Africa region.

B. Cybercrime as a Challenge in East Africa and Beyond

According to the available records, cybercrime victimization rate globally is significantly higher than for conventional crime forms.¹⁷ For example, the rates of victimization for online credit card fraud, identity theft, responding to phishing attempts and unauthorized access to emails are as high as seven-teen percent of the online population.¹⁸ Victimization to cybercrime has gone too far in other jurisdictions, for example, hackers are said to have attacked computer networks of the Pentagon, the White House, NATO's military web-

¹³ Noble, R.K., the then Interpol Secretary General (2000–2014) as quoted in *KPMG International*, p. 6. Also see: *PricewaterhouseCoopers* (2014), pp. 14–15.

¹⁴ Reference to the East African Region and the East African Community in this book is limited to the countries forming the East African Community which is the regional intergovernmental organization of the Republics of Burundi, Kenya, Rwanda, the United Republic of Tanzania, and the Republic of Uganda, with its headquarters in Arusha, Tanzania. Although South Sudan was officially admitted to EAC Membership on 2 March 2016, this book intends not to cover South Sudan for the obvious reason that her statistics and records are not yet very well incorporated and integrated into various EAC reports.

¹⁵ *The East African Community Secretariat*, p. 15.

¹⁶ *The African Centre for Cyberlaw and Cybercrime Prevention*.

¹⁷ *United Nations Office on Drugs and Crime* (2013), p. 25.

¹⁸ *United Nations Office on Drugs and Crime* (2013), p. 25.