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.

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 vide internet. The problem is once a person in 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*

*Chapter 2*

*Chapter 3*

*Chapter 4*

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

*Chapter 5*

*Chapter 6*

**Comparative Assessment of Anti-Cybercrime Initiatives Between Europe and East Africa** 184

*Chapter 7*

**General Conclusion** 215

# List of Tables

# 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 seventeen 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.