This book is an attempt to discuss the legal and regulatory aspects of cybersecurity. It examines international, regional and national regulatory responses to cybersecurity. It particularly examines the response of the United Nations and several international organizations to cybersecurity. It provides an analysis of the Council of Europe Convention on Cybercrime, the Commonwealth Model Law on Computer and Computer Related Crime, the Draft International Convention to Enhance Protection from Cybercrime and Terrorism and the Draft Code on Peace and Security in Cyberspace. The book further examines policy and regulatory responses to cybersecurity in the United States, the United Kingdom, Singapore, India, China and Russia. It also examines the African Union’s regulatory response to cybersecurity and renders an analysis of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa. It considers the development of cybersecurity initiatives by the Economic Community of West African States, the Southern African Development Community and the East African Community. The book further provides an analysis of national responses to cybersecurity in South Africa, Botswana, Mauritius, Kenya, Ghana and Nigeria. It also examines efforts to develop policy and regulatory frameworks for cybersecurity in sixteen other African countries (Algeria, Angola, Cameroon, Egypt, Ethiopia, Ghana, Lesotho, Morocco, Namibia, Niger, Seychelles, Swaziland, Tanzania, Tunisia, Uganda and Zambia). Nigeria is used as a case study to examine the peculiar causes of cyber-insecurity and the challenges that hinder the regulation of cybersecurity in African states as well as the implications of poor cybersecurity governance on national security, economic development, international relations, human security and human rights. The book suggests several policy and regulatory strategies to enhance cybersecurity in Africa and the global information society with emphasis on the collective responsibility of all states in preventing trans-boundary cyber harm and promoting global cybersecurity. This book will be useful to policy makers, regulators, researchers, lawyers, IT professionals, law students and any person interested in seeking a general understanding of cybersecurity governance in developed and developing countries.

Uchenna Jerome Orji is a Barrister and Solicitor of the Supreme Court of Nigeria. He holds a Bachelor of Laws (LL.B) honours Degree from the University of Nigeria and a Masters of Laws (LL.M) Degree from the University of Ibadan, Nigeria with a research specialization in Information Technology Law. He is also a Consultant to the African Center for Cyber Law and Cybercrime Prevention (ACCLP) of the United Nations, African Institute for the Prevention of Crime and the Treatment of Offenders, Kampala, Uganda.
CYBERSECURITY
LAW AND REGULATION

Uchenna Jerome Orji

Barrister and Solicitor of the Supreme Court of Nigeria
LL.B (Hons) (University of Nigeria), BL (Nigerian Law School),
LL.M (University of Ibadan)
Dedication

To Sir & Lady Moses Orji (KSJ).

To my siblings:

Ify,

Ngozi,

Tobechukwu, and;

Ugochukwu.

To Emmanuel Orji;

And;

To the living memory of Barrister Orji Jerome Arochukwu (1973-2009).

“...And even in our sleep, pain that cannot forget, falls drop by drop upon the heart, against our will comes wisdom to us by the awful grace of God”.

Agamemmon of Aeschylus.
“Cybersecurity looms as the 21st century’s most vexing security challenge…Technology continues to race ahead of the ability of policy and legal communities to keep up”.

John Edwin Mroz,
President and CEO EastWest Institute.
Preface

During the 20th century, technological advances brought about the convergence of telecommunications and computer technologies. This signified the beginning of an era known as the information age. The information age is characterized by the rise of digitalization which basically implies a technological shift from analog and electro-mechanical technologies to digital technologies. A very distinctive feature of the information age is the continuous integration of computer and digital communications technologies in virtually all aspects of life and critical services that support modern societies and the tendency towards “connecting everything to everything”. This has given rise to the emergence of the information society. However, the emergence of the information society as a result of the integration of computer and digital communications technologies in all aspects of life has also redefined traditional notions of security. The security of digital data, computers, digital communications technologies and information networks now have an overwhelming influence on almost all aspects of life and society including the global economy. Thus, with the emergence of the information society, malicious conducts against information systems such as computer systems and networks now have the potential of affecting individuals, countries and the global economy in ways previously unimagined. The most critical challenges of the information society have been the security of digital data and information systems and the prevention of the malicious misuse of information communications technologies by criminals, terrorist groups, or state actors. Measures to address these security challenges of the information society have given rise to a new concept known as “cybersecurity”. Cybersecurity seeks to promote and ensure the overall security of digital information and information systems with a view to securing the information society. Thus, the concept is broadly concerned with social, legal, regulatory and technological measures that will ensure the integrity, confidentiality, availability and the overall security of digital information and information systems in order to achieve a high degree of trust and security necessary for the development of a sustainable information society.

This book is an attempt to discuss the legal and regulatory aspects of cybersecurity. It presents an analysis of international, regional and national regulatory responses to cybersecurity in both developed and developing countries. It highlights the limits and challenges of these regulatory responses in the promotion of cybersecurity and explores several regulatory measures to address the highlighted challenges with a view to promoting global cybersecurity. The book suggests several regulatory measures to enhance global cybersecurity and also emphasizes the need for the collective
responsibility of states for global cybersecurity. Although, developments in
the criminal use of information communications technologies “continues to
race ahead of the ability of regulatory frameworks to keep up”, nevertheless,
this book will be useful to policy makers, regulators, researchers, lawyers,
students and any person interested in seeking an understanding of
cybersecurity governance in developed and developing countries - especially
in African countries.

This book is divided into seven chapters.
Chapter one sets out an introduction to cybersecurity law and regulation. It
sets out definitions of cybersecurity and then examines the scope and basic
concepts of cybersecurity as well as the critical components of cybersecurity
governance. It examines a range of malicious conducts which cybersecurity
laws seek to prohibit and other contextual legal issues affecting cybersecurity.
The chapter then explores several “real world” perspectives to cybersecurity.

Chapter two examines several international responses and initiatives
in the field of cybersecurity. It provides an analysis of the Council of
Europe Convention on Cybercrime and other proposed international
legal frameworks on cybersecurity such as the Commonwealth Model
Law on Computer and Computer Related Crime, the Draft International
Convention to Enhance Protection from Cybercrime and Terrorism,
and the Global Protocol on Cybersecurity and Cybercrime. The chapter
also examines the limitations of international regulatory responses on
cybersecurity.

Chapter three examines the responses of some developed and technologically
advanced countries as well as developing countries to cybersecurity. In
this regard, the chapter basically examines legal, policy and institutional
regulatory responses to cybersecurity in countries such as the United States,
the United Kingdom, Singapore, India, China and Russia. It also looks at
some of the major challenges that hinder cybersecurity governance in these
countries.

Chapter four generally examines African multilateral regulatory responses
to cybersecurity at the regional and sub-regional levels. It looks at the
development of cybersecurity initiatives by the African Union and renders
an analysis of the Draft African Union Convention on the Establishment of
a Credible Legal Framework for Cybersecurity in Africa. It highlights some
problems of the Draft Convention and also looks at cybersecurity initiatives
developed by sub-regional multilateral organizations such as the Economic
Community of West African States, the Southern African Development
Community and the East African Community.
Chapter five examines the national responses of African countries to cybersecurity. It provides an analysis of cybersecurity laws in several African countries that have established legal frameworks for cybersecurity such as South Africa, Botswana, Mauritius, Senegal, Kenya and Ghana. It also renders an assessment of ongoing efforts to develop legal and institutional frameworks for cybersecurity as well as other relevant cybersecurity initiatives in African countries.

Chapter six examines Nigeria’s regulatory response to cybersecurity. It renders an analysis of existing and proposed regulatory frameworks on cybersecurity to determine the adequacy of these regulatory frameworks to the development of a secure and responsible information society. Nigeria is used as a case study to examine the peculiar causes of cyber-insecurity in African states as well as the peculiar challenges that hinder the effective regulation of cybersecurity in African states. The chapter also uses Nigeria as a case study to examine the implications of poor cybersecurity governance on national security, economic development, international relations, human security and human rights.

Chapter seven explores policy and regulatory strategies to enhance cybersecurity at the national, regional and global levels. It provides a summary of cybersecurity initiatives within the African region and proposes several policy and regulatory measures to enhance cybersecurity in Africa. This is then followed by proposals for policy and regulatory measures to enhance global cybersecurity. The chapter is concluded with a proposal for the collective responsibility of states for global cybersecurity. In this regard, the chapter suggests that the norm that states may be held responsible for acts and omissions within their territories which produce trans-boundary harm in other countries may also be applied for the purpose of promoting the concept of the collective responsibility of states for global cybersecurity.

This book is a modified version of a Master of Laws (LL.M) thesis originally titled: Legal Governance of Information Technology in Nigeria and African States: An Assessment of Responses to Computer Security which was undertaken at the Faculty of Law, University of Ibadan, Nigeria between February and April 2010 and submitted in May 2010 during the 2009/2010 academic session. However, since my graduation from the University of Ibadan in September 2010, I have taken time to modify and broaden the research to reflect some current regulatory developments in cybersecurity. I take this opportunity to express my profound gratitude to Dr. Peter Chukwuma Obutte of the Department of Public and International Law, who supervised my LL.M thesis. Dr. Obutte is one of Nigeria’s leading experts in telecommunications regulation. His constructive comments and
able guidance helped in putting this work together. This made the research a cherished experience. Also his erudite guidance and tolerant disposition during our LL.M seminars is highly commendable. Following my graduation, he has also encouraged my intention to study for a Doctorate degree in Law. I would also like to express my immense gratitude to Professor Johnson O. Anifalaje for his fatherly guidance and encouragement. I am equally grateful to the Staff of the Faculty of Law Library who helped me in finding some relevant texts during the research; their devotion to duty was great.

I would also like to register my immense gratitude and appreciation to my colleagues in the LL.M Class of the 2009/2010 academic session for creating a stimulating academic environment that was favourable to intellectual growth. I would also like to thank Barr. Onyeka Kanu for his good comradeship during the short period of our study. I am very thankful to Barr. Okechukwu Ekwanyi for his assistance and good will. Barr. Okoli Pontian displayed an unwavering commitment while proof reading the manuscript and made some helpful comments of which I am very grateful.

I wish to specially thank Engr. Emmanuel Orji – a very good brother and friend, for his immense goodwill and support during my stay in Ibadan. I am equally grateful to my brother and very good friend Mr. Fredrick Onu for his sincere encouragements and goodwill. I am also grateful to my big brother Late Barr. Orji Jerome Arochukwu for his guidance and support while he was alive.

I am eternally grateful to my parents Sir & Lady Moses Orji for sponsoring my education up the Postgraduate level and also for their constant support and encouragement. I am also eternally grateful to my siblings: Engr. Ifeyinwa Orji, Dr. Ngozi Orji, Tobechukwu Orji and Ugochukwu Orji for their constant affection and support. Nothing can really describe my indebtedness to my family; hence, I am dedicating this book to them.

Uchenna Jerome Orji
Onyiba Villa,
Akanu, Amagu, Ishiagu,
Ebonyi State, Nigeria.
Author’s biography

Uchenna Jerome Orji is a Barrister and Solicitor of the Supreme Court of Nigeria. He holds a Bachelor of Laws (LL.B) honours Degree from the University of Nigeria and a Masters of Laws (LL.M) Degree with honours and distinctions from the University of Ibadan, Nigeria where he majored in Information Technology Law. Uchenna holds a national award for the best overall essay in the Fourth Edition of the Nigerian Ships and Ports Annual National Essay Competition in 2010. He is the author of Realizing Agenda 21: A Nigerian Perspective (Vdm Verlag: Germany, 2010) and has also been published in leading international journals including: the Journal of International Banking Law and Regulation, the International Company and Commercial Law Review, the Computer and Telecommunications Law Review, the Journal of African Law, the Commonwealth Law Bulletin and the Business Law Review. Uchenna is also an Associate and Consultant to the African Center for Cyber Law and Cybercrime Prevention (ACCP) of the United Nations, African Institute for the Prevention of Crime and the Treatment of Offenders, Kampala, Uganda (www.cybercrime-fr.org/index.pl/the_center_in_brief). He is presently undertaking Doctoral research on the regulation of telecommunications in Sub-Saharan African countries. His research seeks to explore how the regulation of telecommunications can enhance sustainable socio-economic development in Sub-Saharan Africa using Nigeria, Ghana and South Africa as case studies. The thesis involves research questions on the regulation of competition, universal access, environmental sustainability and consumer protection in the telecommunications industry. Email: jeromuch@yahoo.com.
# Summary of Contents

Dedication III

Preface VII

Author’s Biography XI

Summary of Contents XIII

Table of Contents XV

Table of Cases XXV

Table of Legislations and Policies XXIX

List of Tables and Figures XXXVII

Chapter One: An Introduction to Cybersecurity Law and Regulation 1

Chapter Two: International Responses and Legal Measures on Cybersecurity 95

Chapter Three: National Regulatory Responses to Cybersecurity in Select Jurisdictions 213

Chapter Four: Multilateral Regulatory Responses to Cybersecurity in Africa 371

Chapter Five: Cases Studies of National Regulatory Responses to Cybersecurity in African States 401

Chapter Six: Cybersecurity Law and Regulation in Nigeria 485

Chapter Seven: Policy and Regulatory Proposals to Enhance Cybersecurity 563

Selected Bibliography 591

Index 627
Table of Contents

Dedication III
Preface VII
Author’s Biography XI
Summary of Contents XIII
Table of Contents XV
Table of Cases XXV
Table of Legislations and Policies XXIX
List of Tables and Figures XXXVII

CHAPTER ONE: AN INTRODUCTION TO CYBERSECURITY AND REGULATION

1.1 Introduction 1
1.2. Defining Cybersecurity 10
1.2.1. Cybersecurity as a Field of Law 16
1.2.1.1. Cybercrime 17
1.3. An Overview of the Scope and Basic Concepts of Cybersecurity 19
1.3.1.1. Telecommunications Security 20
1.3.1.2. Data Protection 22
1.3.1.3. Information Security 23
1.3.1.4. Security of Critical Infrastructures/ Critical information Infrastructures 24
1.3.2. The Basic Concepts of Cybersecurity 30
1.3.2.1. Confidentiality 30
1.3.2.2. Integrity 32
1.3.2.3. Availability 33
1.3.2.4. Accountability 33
1.4. Critical Components of Cybersecurity Governance 33
1.4.1. Legal Aspects 34
1.4.2. Technical Aspects 36
1.4.3. Institutional/Organizational Aspects 38
1.4.3.1. Computer Emergency Response Teams (CERTs) 39
1.4.4. End-User Education 40
1.4.5. Research and Development 41
1.5. Contextual Legal Issues in Cybersecurity: Malicious Conducts, Illicit Contents and Liability of Internet Service Providers 42
1.5.1. Unauthorized/ Illegal Access (Hacking or Cracking) 42
1.5.2. Unauthorized Interception 46
1.5.3. Data Interference 48
1.5.4. System Interference 48
1.5.5. Data Espionage 53
1.5.6. Illegal Content 55
1.5.6.1. Pornographic Materials 56
1.5.6.2. Child Pornography 57
1.5.6.3. Publication of Xenophobic Materials 58
1.5.7. Spam Mails 58
1.5.8. Misuse of Computing Devices and Related Digital Technologies 60
1.5.9. Computer Related Identity Theft 61
1.5.10. Cyber-Squatting, Web hijacking and other Copyright and Trade Mark Issues 62
1.5.10.1. Cyber-Squatting 62
1.5.10.2. Domain name or Web hijacking 64
1.5.10.3. Copyright Infringements 64
1.5.11. Computer Related Offences 64
1.5.11.1. Computer Related Forgery 65
1.5.11.2. Computer Related Fraud 65
1.5.12. Cyber Terrorism 67
1.5.13. Cyber Warfare 70
1.5.13.1. Cyber Warfare under International Laws of Armed Conflict 73
1.5.13.2. Challenges to Cyber Arms Control 76
1.5.13.3. Cyber Deterrence 79
1.5.14. Responsibility/ Liability of Internet Service Providers (ISPs) 81
1.6. Exploring “Real World” Perspectives of Cybersecurity 83
1.6.1. National Security 83
1.6.2. Economic Security 87
1.6.3. Human Rights 89
1.6.4. Human Security 91

CHAPTER TWO:
INTERNATIONAL RESPONSES AND LEGAL MEASURES ON CYBERSECURITY
2. Introduction 95
2.1. International responses on cybersecurity 96
2.1.1. The United Nations 96
2.1.1.2. The United Nations Resolution 55/63 on Combating the Criminal Misuse of Information Technology 98
2.1.1.3. The United Nations Resolution 56/121 on Combating the Criminal Misuse of Information Technology 99
2.1.1.4. United Nations Resolution 57/239 on the Creation of a Global Culture of Cyber Security 100
2.1.5. United Nations Resolution 58/199 on the Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures

2.1.6. United Nations Resolutions on Developments in the Field of Telecommunications in the Context of International Security

2.1.7. Other Notable United Nations Resolutions on Cybersecurity

2.1.8. The Internet Governance Forum (IGF)

2.1.9. Recent Developments

2.1.2. The International Telecommunications Union (ITU)

2.1.2.1. The World Summit on the Information Society (WSIS)

2.1.2.2. The ITU High Level Expert Group (HLEG) on Cybersecurity

2.1.3. The Group of Eight (G8)

2.1.4. The Interpol

2.1.5. The Council of Europe

2.1.6. European Union (EU)

2.1.7. The Asian Pacific Economic Cooperation (APEC)

2.1.8. The Organization for Economic Cooperation and Development (OECD)

2.1.9. The Commonwealth

2.1.10. The Organization of American States (OAS)

2.1.11. The Association of South-East Asian Relations (ASEAN)

2.1.12. The North Atlantic Treaty Organization (NATO)

2.1.13. The Arab League and Gulf Cooperation Council

2.1.14. The Stanford Proposal

2.1.15. The Global Protocol on Cybersecurity and Cybercrime

2.1.16. The International Multilateral Partnership Against Cyber Threats (IMPACT)

2.2 An analysis of international legal frameworks on cybersecurity

2.2.1 The Council of Europe Convention on Cybercrime

2.2.1.1. Measures to be taken at the National Level with Regards to Substantive Criminal Law

2.2.1.2. Measures to be taken at the National Level with regards to Procedural Law

2.2.1.3. Measures to be taken at the National Level with regards to the establishment of Jurisdiction

2.2.1.4. Measures to be taken with regards to International Cooperation

2.2.2. The Commonwealth Model Law on Computer and Computer Related Crime

2.2.2.1. Introduction- Matters Regarding the Usage of Terms and State Jurisdiction

2.2.2.2. Offences

2.2.2.3. Procedural Powers

2.2.3. The Draft International Convention to Enhance Protection from Cybercrime and Terrorism

2.2.3.1. Introduction- Matters Regarding the Usage of Terms and State Jurisdiction

2.2.3.2. Offences

2.2.3.3. Procedural Powers

2.2.4. The Draft International Convention to Enhance Protection from Cybercrime and Terrorism
2.2.3.1. Definitions and Use of Terms 184
2.2.3.2. Offences against Cyber Systems and Critical Infrastructures 185
2.2.3.3. Enactment of Domestic Laws by State Parties 188
2.2.3.4. Jurisdiction 188
2.2.3.5. Mutual Legal Assistance and Cooperation in Law Enforcement 189
2.2.3.6. Protection of Privacy and other Human Rights 192
2.2.3.7. The Agency for Information Infrastructure Protection (AIIP) 194
2.2.4. The Draft Code on Peace and Security in Cyberspace - A Global Protocol on Cybersecurity and Cybercrime 196
2.2.4.2. The Model Law on Cybercrime 198
2.3. Limits of International Responses and Legal Measures 199
2.3.1. Lack of Broad Participation 199
2.3.2. The Absence of a Global Treaty of all Nations on Cybersecurity 201
2.3.3. Digital Divide 203
2.3.4. Lack of consensus 204
2.3.5. Lack of International Cooperation 207
2.3.6. National Implementation 210

CHAPTER THREE:
NATIONAL REGULATORY RESPONSES TO CYBERSECURITY IN SELECT JURISDICTIONS
3. Introduction 213
3.1. The United States of America 213
3.1.1. Legal Measures 214
3.1.1.1. The Computer Fraud and Abuse Act 214
3.1.1.2. Other Enactments on Cybersecurity 228
3.1.1.2.1. Controlling the Assault of Non-Solicited Pornography and Marketing Act (The CAN – SPAM Act) 228
3.1.1.2.2. The Digital Millennium Copyright Act 229
3.1.1.2.3. The Economic Espionage Act 229
3.1.1.2.4. The Electronic Communications Privacy Act 230
3.1.1.2.5. The Wire Fraud Act 230
3.1.1.2.6. The United States PATRIOT Act 230
3.1.1.2.7. The Federal Information Security Management Act 231
3.1.1.2.8. The Cyber Security Research and Development Act 231
3.1.2. Institutional Regulatory Mechanisms 231
3.1.2.1. The Department of Homeland Security (DHS) 232
3.1.2.2. The United States Computer Emergency Readiness Team (US-CERT) 233
3.1.2.3. Other Institutional Regulatory Mechanisms 233
3.1.3. Policy Mechanisms 234
3.1.3.1. The National Strategy to Secure Cyberspace 234
3.1.3.2. The Comprehensive National Cybersecurity Initiative (CNCI) 234
3.1.3.3. The Cyberspace Policy Review 235

XVIII
3.1.3.4. The United States International Strategy for Cyberspace

3.1.4. **Recent Developments**

3.1.4.1. The United States International Cybercrime Reporting and Cooperation Bill

3.2. **The United Kingdom**

3.2.1. **Legal Measures**

3.2.1.1. The Computer Misuse Act

3.2.2. Other Enactments on Cybersecurity

3.2.2.1. The Terrorism Act

3.2.2.2. The Counter-Terrorism Act

3.2.2.3. Regulation of Investigatory Powers Act

3.2.2.4. The Fraud Act

3.2.2.5. The Police and Justice Act

3.2.3. **Institutional Regulatory Mechanisms**

3.2.3.1. The Serious and Organized Crime Agency (SOCA)

3.2.3.2. The Communications Electronics Security Group (CESG)

3.2.3.3. The UK Computer Emergency Response Team (GovCertUK)

3.2.3.4. The Center for the Protection of National Infrastructure (CPNI)

3.2.3.5. The Office of Cyber Security

3.2.3.6. The Cyber Security Operations Centre

3.2.3.7. The Internet Watch Foundation (IWF)

3.2.4. **Policy Mechanisms**

3.3. **Singapore**

3.3.1. **Legal Measures**

3.3.1.1. The Computer Misuse Act of Singapore

3.3.1.2. Other Enactments on Cybersecurity

3.3.1.2.1. The Spam Control Act of Singapore

3.3.2. **Institutional Regulatory Mechanisms**

3.3.3. **Policy Mechanisms**

3.3.3.1. The Infocomm Security Master Plan 2

3.3.3.2. The National Trust Framework (NTF)

3.4. **India**

3.4.1. **Legal Measures**

3.4.1.1. The Indian Information Technology Act

3.4.1.2. Other Enactments on Cybersecurity

3.4.1.2.1. The Information Technology (Guidelines for Cyber Cafe) Rules 2011

3.4.2. **Institutional Regulatory Mechanisms**

3.4.3. **Policy Mechanisms**

3.4.3.1. The Indian Cybersecurity Strategy

3.5. **The People’s Republic of China**

3.5.1. **Legal Measures**
3.5.1.1. The Computer Information Network and Internet Security, Protection and Management Regulations 316
3.5.1.2. The Chinese Regulations on Safeguarding Computer Information Systems 328
3.5.1.3. The State Secrecy Protection Regulations for Computer Information Systems on the Internet 330
3.5.1.4. The Criminal Law of the People’s Republic of China 332
3.5.2. Institutional Regulatory Mechanisms 344
3.5.2.1. China’s National Defense Strategy 2010 345
3.6. The Russian Federation 346
3.6.1. Legal Measures 348
3.6.2. Institutional Regulatory Mechanisms 355
3.6.3. Policy Mechanisms 356
3.6.3.1. The Russian Information Security Doctrine 356
3.6.4. Russia and the Council of Europe Convention on Cybercrime 358
3.7. An Overview of Some Major Regulatory Challenges 361
3.7.1. Use of Cyber Devices for Dual Purposes and the Availability of Malicious Cyber Tools 361
3.7.2. The Constant Evolution of Malicious Cyber Tools 362
3.7.3. Under-Reporting 362
3.7.4. High Costs of Investigating and Prosecuting Cybercrime 363
3.7.5. Challenges of Obtaining and Preserving Digital Evidence 363
3.7.6. Investigation and Prosecution of Suspects Located Abroad 364
3.7.7. Proof of Offences 367
3.7.8. “Forum Shopping” by Criminal Actors 368
3.7.9. Other Challenges 368

CHAPTER FOUR:
MULTILATERAL REGULATORY RESPONSES TO CYBERSECURITY IN AFRICA
4. Introduction 371
4.1. Regional Multilateral Responses 374
4.1.1. The African Union (AU) 374
4.1.1.1.1. Basic Principles to Promote Cybersecurity in African States 377
4.1.1.1.2. Provisions Relating to the Establishment of Cybercrime Offences 385
4.2. Sub-Regional Multilateral Responses 397
4.2.1. The Economic Community of West African States (ECOWAS) 397
CHAPTER FIVE:
CASES STUDIES OF NATIONAL REGULATORY RESPONSES TO CYBERSECURITY IN AFRICAN STATES

5.  Introduction  401
5.1.  South Africa 403
5.1.1.  Legal Measures 403
5.1.1.1.  The Electronic Communications and Transactions Act  403
5.1.1.2.  The Interception and Monitoring Prohibition Act and Other Related Enactments on Cybersecurity 416
5.1.2.  Institutional Regulatory Mechanisms 417
5.1.2.1.  Cyber Inspectors 417
5.1.2.2.  ECS-CSIRT 417
51.4.  Policy Mechanisms 418
5.1.3.1.  The Draft Cybersecurity Policy of South Africa 418
5.2.  Botswana 419
5.2.1.  Legal Measures 420
5.2.1.1.  The Cybercrime and Computer Related Crimes Act 420
5.2.2.  Institutional Regulatory Mechanisms 445
5.3.  Mauritius 445
5.3.1.  Legal Measures 446
5.3.1.1.  The Computer Misuse and Cybercrime Act 446
5.3.2.  Institutional Regulatory Mechanisms 447
5.3.2.1.  The Mauritian national Computer Security Incident Response Team (CERT-MU) 448
5.4.  Senegal 448
5.4.1.  Legal Measures 449
5.4.1.1.  The Senegalese Law on Cybercrime 449
5.5.  Kenya 459
5.5.1.  Legal Measures 459
5.5.1.1.  The Kenya Communications (Amendment) Act 459
5.5.2.  Policy Mechanisms 460
5.5.2.1.  The Kenyan Information and Communications Technology Policy 460
5.5.3.  Institutional Regulatory Mechanisms 460
5.5.3.1.  The Kenya Computer Security Incident Response Team (CSIRT-Kenya) 460
5.6.  Ghana 461
5.6.1.  Legal Measures 462
5.6.1.1.  The Electronic Transactions Act 462
5.6.2.  Institutional Regulatory Mechanisms 470
5.7.  Brief Overviews of Regulatory Reponses in other African States 472
5.7.1.  Algeria 472
5.7.2. Angola 472
5.7.3. Cameroon 473
5.7.4. Egypt 474
5.7.5. Ethiopia 475
5.7.6. Gambia 476
5.7.7. Lesotho 476
5.7.8. Morocco 477
5.7.9. Namibia 477
5.7.10. Niger 478
5.7.11. Seychelles 478
5.6.12. Swaziland 478
5.7.13. Tanzania 479
5.7.14. Tunisia 480
5.7.15. Uganda 481
5.7.16. Zambia 482

CHAPTER SIX:
CYBERSECURITY LAW AND REGULATION IN NIGERIA
6. Introduction 485
6.1. Legal Measures 491
6.1.1. The Advance Fee Fraud and other Fraud Related Offences Act 491
6.1.1.1. Duties of Electronic Communications Service Providers 492
6.1.1.2. Liabilities for Breach of Duties imposed on Electronic Communications Service Providers 493
6.1.2. The Nigerian Communications Act 494
6.1.2.1. Powers of the Nigerian Communications Commission with respect to Cybersecurity 495
6.2. Policy Mechanisms 496
6.2.1. The Nigerian National Policy for Information Technology 496
6.3. An Overview of National Efforts to Develop Broad Legal and Institutional Regulatory Mechanisms on Cybersecurity 496
6.3.1. The Presidential Committee on 419 Activities in the Cyberspace 497
6.3.2. The Nigerian Cybercrime Working Group (NCWG) 497
6.3.2.1. Some Achievements of the Nigerian Cybercrime Working Group (NCWG) 500
6.3.3. Recent Developments 501
6.4. Institutional Regulatory Mechanisms 501
6.4.1. The Directorate for Cybersecurity (DFC) 501
6.4.2. The Economic and Financial Crimes Commission (EFCC) 503
6.4.2.1. Some Achievements of the EFCC on Cybersecurity 504
6.4.2.1.1. The EFCC – ATCON Partnership 504
6.4.2.1.2. The EFCC and Microsoft Partnership on Cybersecurity 505
6.4.2.1.3. The EFCC-G8 24/7 Network 505
6.4.2.1.4. The EFCC Transaction Clearing Platform 506
6.4.3. The National Information Technology Development Agency 506
6.5. An Analysis of Proposed Legal Measures

6.5.1. The Computer Security and Critical Information Infrastructure Protection Bill

6.5.2. Comments on the Computer Security and Critical Information Infrastructure Protection Bill

6.5.3. The Nigerian Cybersecurity and Data Protection Agency Bill

6.6. Peculiar Causes of Cyber-insecurity and the Regulatory Challenges of Cybersecurity in Nigeria

6.6.1. Legal Challenges

6.6.1.1. Lack of appropriate legal frameworks on cybersecurity

6.6.1.2. Challenges arising from the legal status of digital evidence

6.6.2. Weak Institutional Capacities

6.6.3. Absence of Effective Synergy and Cooperation between Regulatory Institutions on Cybersecurity

6.6.4. Poor Regulatory Oversight

6.6.5. Digital Divide

6.6.6. Lack of Resources and Skilled Manpower

6.6.7. Under Reporting

6.6.9. The Deployment of Internet Services without Technical Security Solutions

6.6.10. Lack of End-User Awareness

6.6.11. Poor Socio-Economic Conditions and the Deterioration of Societal Values

6.6.12. Massive Influx of Electronic Waste


6.7.1. National Security

6.7.2. Human Security

6.7.3. Human Rights

6.7.4. International Relations

6.7.5. National Economic Development

CHAPTER SEVEN: POLICY AND REGULATORY PROPOSALS TO ENHANCE CYBERSECURITY

7. Introduction

7.1. Policy and Regulatory Proposals to Enhance Cybersecurity in Africa

7.1.1. Legal Strategies

7.1.2. Building Capacities in Legislative and Regulatory Institutions

7.1.3. Building Capacities in Business Organizations

7.1.4. Building Capacities for End-User Education

7.1.5. Building Capacities to enhance the implementation of Technical
# Table of Cases

### Germany

*BVerfG* (German Federal Constitutional Court, NJW 2008, 822- 27/2/2008,) 89

### India

*State of Tamil Nadu v. Suhas Katti* (C.C.NO.4680/2004) 92,293

### Nigeria


*Anyeabosi v. R.T. Briscoe* *(Nig)* Ltd (1987) 3 NWLR (Pt 59), 84 2 NSCC Vol. 18 (pt.2) 805 540


*Esso West Africa Inc v. Oyegbola* (1969) 1 NNLR 194 SC 540


*Ogolo v. IMB* *(Nig)* Ltd (1995) 9 NWLR (Pt. 419) 314 C.A 540


### Singapore


1 S.L.R. 34; (1999) SGHC 275 261,264,269,423


### South Africa


*Ndlovu v. Minister of Correctional Services* (2006) (4) All SA 165 (W) 409

*R v. Douvenga* (Unreported, District Court of Northern Transvaal, Pretoria- Case No. 111/150/2003, 19/8/2003 405

*S v. Harper* (1981) (2) SA 638 (D) 403

*S v. Howard* (Unreported case No. 41/258/02, Johannesburg Regional Magistrates Court) 404

*S v. Manuel* (1953) (4) SA 526 403


### Uganda

*Uganda v. Garuhanga and Mugerwa* (Unreported, Buganda Road Court, CR 17 of 2004) 482

### United Kingdom

*A.G’s Reference (No.1 of 1999)* (1993) QB 94 247

*BT v. One in a Million Ltd* (Unreported, The Times, 2/12/9) 63,521

*Cox v. Riley* (1986) 83 Cr. App. R.54 238


XXV

Harrods v. UK Network Services Limited and Others (Unreported, Chancery Division, 9/12/1996) 63,521

Marks and Spencer v. One in a Million Ltd (Unreported, Court of Appeal, 23/7/1998) 23 63,521

Morgans v. DPP (2000) 2 WLR 386; (1999) 1 WLR 968 253

R v. Aaron Caffrey (Unreported, Southwark Crown Court, 17/10/2003) 367,368

R v. Alfred Whittaker (Unreported, Scunthorpe, Magistrates Court) 246,515


R v. Daniel Cuthbert (Unreported, Horseferry, Road Magistrates Court 07/10/2005) 243

R v. Emma Pearce and Malcolm Farquhason (Unreported, Croydon Magistrate Court, 9/12/1993) 245


R v. Ian Morris and Richard Airlie (Unreported Cardiff Crown Court) 247

R v. Michelle Begley (Unreported, Coventry Magistrates Court) 243

R v. Mark Hopkins (Unreported, Westminster Magistrates Court 09/08/2007) 243


R v. Ross Pearlstone (Unreported, Bow Street Magistrates Court) 245

R v. Pile (Unreported, Plymouth Crown Court, 1995) 247, 268

R v. Pryce (Unreported, Bow Street Magistrate Court, 21/3/1997) 252

R v. Richard Goulden (Unreported, Southwark Crown Court, June 1992) 246,515

R v. Simon Vallor (Unreported, Southwark Crown Court, 21/01/2003) 246,247


Saltman Engineering Co. Ltd v. Campbell Engineering Co. Ltd (1948) 65 RPC 203 31

Simkins Partnership v. Reeves Lund & Co. Ltd (Lawtel, 2003) 299

Thomas Marshall (Exports) Ltd. v. Guinle (1979) Ch. 227 31


United States

America Online, Inc. v. LCGM, Inc. 46 F. Supp. 2d 444, 444 (E.D. Va. 1998) 60


Intermatic Inc. v. Dennis Toeppen (pre-ACPA), No. 96 C, 1982. United States

XXVI
District Court, N.D. Illinois, Eastern Division. Nov. 26, 1996 63,521

*International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006) 32

*Ognibene v. Citibank* (446 NYS 2d 845 (CIV.Ct.1981) 570


*Re America Online, Inc.* 168 F. Supp. 2d 1359 (S.D Fla. 2001) 221


*United States v. Bae*, 250 F.3d 774 (D.C. Cir. 2001) 221


*United States v. Ivanov*, 175 F. Supp. 2d 367 (D. Conn. 2001) 64,227,284, 365, 435

*United States v. Lindsley* (2001) WL 502832 (5th Cir. 2001) 221,423

*United States v. Lloyd*, 269 F.3d 228, 231 (3d Cir. 2001) 224

*United States v. Middleton*, 231 F.3d 224

*United States v. Mitra*, 405 F.3d 492 (7th Cir.2005) 225

*United States v. Morris*, 928 F.2d 504 (2d Cir. 1991) 216,223,242

*United States v. Pirello*, 255 F.3d 728 (9th Cir. 2001) 230


*United States v. Rushdan*, 870 F.2d 1509, 1514 (9th Cir. 1989) 226

*United States v. Scartz*, 838 F.2d 876, 879 (6th Cir. 1988) 226


*United States v. Tucker*, 150 F Supp 2d 1263 (D Utah 2001) 305 F 3d 1193 (10th Cir, 2002) 147

*United States v. Willis*, 476 F.3d 1121, 1125 (10th Cir. 2007) 219

**International Arbitration and Court Cases**

*August v. the United Kingdom* (January 2003) no. 36505/02, 21 587

*Calvelli and Ciglio v. Italy* [GC], (2002) no. 32967/96, ECHR 2002-IX 587

*Cyprus v. Turkey* (2001) ECHR No.25781/94 586


*Shell International Petroleum Co. v. Allen Jones* (WIPO Case No D2003-0821, 18/12/2003) 63,521


*Telstra Corporation Limited v. Nuclear Marshmallow* (Case No. D 2000-0003 Administrative Panel Decision at the WIPO Arbitration and Mediation Center) 63,521

XXVII
Table of Legislations and Policies

AFRICAN COUNTRIES

**Algeria**
Cybercrime Act 2008

**Angola**
Basic Telecommunication Law 2001

**Botswana**
Cybercrime and Computer Related Crimes Act 22, 2007

**Cameroon**
Cybercrime Act 2011

**Egypt**
E-Signature Law No. 15, 2004

**Ethiopia**
Criminal Code of the Federal Republic of Ethiopia, Proclamation No. 414, 2004

**Gambia**
Information and Communications Act, No.2, 2009

**Ghana**
Electronic Transactions Act, No.772, 2008
National Information Technology Agency Act, No.771, 2008

**Kenya**
Kenyan Communications (Amendment) Act No. 1, 2009
Kenyan Information and Communications Technology Policy, 2006

**Lesotho**
Lesotho ICT Policy of 2005

**Mauritius**
Computer Misuse and Cybercrime Act No XI, 2003

**Morocco**
Penal Code, Law No. 07.003 of Morocco, November, 2003
Namibia
Computer Misuse and Cybercrime Act 2003

Niger
Cybercrime Law 2003

Nigeria
Advance Fee Fraud and other Fraud Related Offences Act 2006
Computer Security and Critical Information Infrastructure Protection Bill-Sb 254 2005
Constitution of the Federal Republic of Nigeria, 1999
Economic and Financial Crimes Commission (Establishment) Act 2004
Nigerian Criminal Code, Cap. 77 LFN 1990
Nigerian Communications Act 2003
National Information Technology Development Agency Act 2007
National Information Technology Policy 2001
Nigerian Cybersecurity and Data Protection Agency Bill- HB, 154 C 4443, 2008

Senegal

Seychelles
Computer Misuse Act 1998
Data Protection (Amendment) Act No. 6, 2003

South Africa
South African Electronic Communications and Transactions Act No. 25, 2002
Interception and Monitoring Prohibition Act No. 127, 1992
Regulation of Interception of Communications and Provision of Communication Related Information Act (RICPCR1A) 2002
Draft Cybersecurity Policy of South Africa Government Gazette No. 32963, 19 February, 2010

Kingdom of Swaziland
Kingdom of Swaziland National Information and Communication Infrastructure (NICI) Policy 2003

Tanzania
National Information and Communications Technology Policy 2003
Tunisia
Cybercrime Act, N°1999-89, Art 199
Electronic Signature and e-commerce Law, N° 2000-83
Data Protection Law, N°2004-63

Uganda
Computer Misuse Bill
Electronic Signature Act
E-transactions Act

Zambia
Computer Misuse and Crimes Act 2004

FOREIGN JURISDICTIONS

Brazil
Law No.9983, July 14, 2000 Article 213-13

China
Chinese Regulations on Safeguarding Computer Information Systems 1996
State Secrecy Protection Regulations for Computer Information Systems on the Internet 2000
Criminal Law of the People’s Republic of China
Chinese National Defense Strategy 2010

India
Information Technology Act, No. 21, 2000
Information Technology (Amendment) Act 2008, No. 10, 2009
Information Technology (Guidelines for Cyber Cafe) Rules 2011
The Indian Cybersecurity Strategy

Mexico
Penal Code Part 9, Chapter II Article 211

Russia
Criminal Code of the Russian Federation
Russian Information Security Doctrine 2000

Singapore
Spam Control Act of Singapore 2007
The Infocomm Security Master Plan 2
The National Trust Framework (NTF)

United Kingdom
Anti-terrorism, Crime and Security Act 2001 (c. 24)
Computer Misuse Act 1990(c.18)
Counter-Terrorism Act 2008 (c.28)
Criminal Damage Act 1971
Extradition Act 1989
Fraud Act 2006
Police and Justice Act 2006 (c.48)
Terrorism Act 2000 (c.11)
Terrorism Act 2006 (c. 11)
Regulation of Investigatory Powers Act 2000(c.23)
The Cyber Security Strategy of the United Kingdom 2009

United States
Comprehensive National Cybersecurity Initiative (CNCI) 2008
Computer Fraud and Abuse Act,18 U.S.C S.1030
Cyber Security Research and Development Act, P.L. 107-305, 2002
Digital Millennium Copyright Act 1998
Economic Espionage Act, 18 U.S.C. 1832
Electronic Communications Privacy Act 1986 (ECPA) P.L. 99-508
Identity Theft Restitution Act 2008
National Information Infrastructure Protection Act 1996
National Infrastructure Protection Plan 2006
National Security Presidential Directive 54/Homeland Security
Presidential Directive 23 (NSPD-54/HSPD-23, January 8, 2008)
Nigerian Advance Fee Fraud Prevention Act of 1998, HR 3916 IH, 105th Congress 2d Session H. R. 3916 (Bill)
United States Cyberspace Policy Review 2009
United States National Policy on Critical Infrastructure Protection:
United States National Strategy to Secure Cyberspace 2003
United States International Strategy for Cyberspace 2011
United States International Cybercrime Reporting and Cooperation Bill S. 3155 and H.R. 4692 2011
United States PATRIOT Act 2001 P.L. 107-56
Wire Fraud Act 18 U.S.C Section 1343

INTERNATIONAL TREATIES, CONVENTIONS, RESOLUTIONS AND POLICY INSTRUMENTS

African Union
Constitutive Act of the African Union (2001)

The Commonwealth
Model Law on Computer and Computer Related Crime LMM (02) 17

Council of Europe
Council of Europe, Convention on Cybercrime, 41 I.L.M. 282 (Budapest, 23.XI, 2001)
Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, ETS No. 189
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No. 108 (Strasbourg, 28.I.1981)
Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse CETS No.201 (2007)

The Economic Community of West African States (ECOWAS)
ECOWAS Supplementary Act on Cybercrime and Personal Data Protection (2008)

European Union (EU)
European Convention on Human Rights (1950)
EU Data Retention Directive 2005/0182/COD

**Group of Eight (G8)**

**Organization of American States (OAS)**
OAS General Assembly Resolution AG/RES.2004 (XXXIV-o/04)
OAS General Assembly Resolution, AG/RES.2266 (XXXVII-o/07)

**United Nations Conventions**
Universal Declaration of Human Rights

**United Nations Resolutions**
Resolution 55/59 (4/12/2000)
Resolution 60/177 (16/12/2005)
Rio Declaration on the Environment and Development (1992)
Stockholm Declaration (1972)

**United Nations Resolutions on Combating the Criminal Misuse of Information Technology**
Resolution 55/63 (A/RES/55/63) of 4 December 2000
Resolution 56/121 (A/RES/56/121) of 19 December 2001
United Nations Resolutions on the Creation of a Global Culture of Cybersecurity
Resolution 57/23 (A/RES/57/239) 20 December 2002

United Nations Resolutions on Developments in the Field of Telecommunications in the Context of International Security
Resolution 55/28 (20/11/2000)
Resolution 56/164 (A/56/164)
Resolutions 53/70 (4/12/1998)
Resolution 55/28 (28/11/2000)
Resolution 54/49 (12/1999)
Resolution 56/19 (29/11/2001)
Resolution 58/32 (18/12/2003)
Resolution 59/61 (3/12/2004)
Resolution 60/45 (8/12/2005)
Resolution 61/54 (6/12/2006)
Resolution 62/17 (5/12/2007)
Resolution 63/37 (2/12/2008)

United Nations Economic and Social Council (ECOSOC) Resolutions
(ECOSOC) Resolution 2002/10
ECOSOC Resolution 2004/26
ECOSOC Resolution 2007/20 (26/7/2007)
ECOSOC Resolution 2004/42
ECOSOC Resolution 2009/22 (30/7/2009)

Resolutions of the United Nations Commission on Narcotic Drugs
Resolution 48/5 on Strengthening International Cooperation in Order to Prevent the Use of the Internet to Commit Drug Related Crime

Subsidiary Legal and Policy Instruments
Draft International Convention to Enhance Protection from Cybercrime and Terrorism
Resolution 52 – Countering and Combating Spam (WTSA-08 –
Resolution 52) World Telecommunication Standardization Assembly
Johannesburg, (21-30 October 2008)
World Summit on the Information Society (WSIS) Declaration of
Millennium (2003)
World Summit on the Information Society (WSIS) The Tunis Agenda for
the Information Society (2005)
List of Tables and Figures

Table 1: The Infrastructure Threat Matrix 28

Table 2: A Case Study of Internet Activity Profile in South Western Nigeria 488

Table 3: A Summary of National Regulatory Responses to Cybersecurity in Africa 564

Figure 1: Anonymous Electronic Communications Services and the Tracing of Cybercrime 545