

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
LAW AND REGULATION**

Uchenna Jerome Orji

ISBN: 9789058508577

Published by:

Wolf Legal Publishers (WLP)
P.O. Box 31051
6503 CB Nijmegen
The Netherlands
Tel: +31 24 355 19 04
Fax: +31 84 837 67 00
E-Mail: info@wolfpublishers.nl
www.wolfpublishers.com

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the publisher. Whilst the authors, editors and publisher have tried to ensure the accuracy of this publication, the publisher, authors and editors cannot accept responsibility for any errors, omissions, misstatements, or mistakes and accept no responsibility for the use of the information presented in this work.

© WLP 2012 / the Author

“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. Okechukuwu Ekwanya 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.
January 15, 2012.

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.	<i>Cybersecurity as a Field of Law</i>	16
1.2.1.1.	<i>Cybercrime</i>	17
1.3.	An Overview of the Scope and Basic Concepts of Cybersecurity	19
1.3.1.1.	<i>Telecommunications Security</i>	20
1.3.1.2.	<i>Data Protection</i>	22
1.3.1.3.	<i>Information Security</i>	23
1.3.1.4.	<i>Security of Critical Infrastructures Critical information Infrastructures</i>	24
1.3.2.	<i>The Basic Concepts of Cybersecurity</i>	30
1.3.2.1.	<i>Confidentiality</i>	30
1.3.2.2.	<i>Integrity</i>	32
1.3.2.3.	<i>Availability</i>	33
1.3.2.4.	<i>Accountability</i>	33
1.4.	Critical Components of Cybersecurity Governance	33
1.4.1.	<i>Legal Aspects</i>	34
1.4.2.	<i>Technical Aspects</i>	36
1.4.3.	<i>Institutional/Organizational Aspects</i>	38
1.4.3.1.	<i>Computer Emergency Response Teams (CERTs)</i>	39
1.4.4.	<i>End-User Education</i>	40
1.4.5.	<i>Research and Development</i>	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.	<i>Pornographic Materials</i>	56
1.5.6.2.	<i>Child Pornography</i>	57
1.5.6.3.	<i>Publication of Xenophobic Materials</i>	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.	<i>Cyber-Squatting</i>	62
1.5.10.2.	<i>Domain name or Web hijacking</i>	64
1.5.10.3.	<i>Copyright Infringements</i>	64
1.5.11.	Computer Related Offences	64
1.5.11.1.	<i>Computer Related Forgery</i>	65
1.5.11.2.	<i>Computer Related Fraud</i>	65
1.5.12.	<i>Cyber Terrorism</i>	67
1.5.13.	Cyber Warfare	70
1.5.13.1.	<i>Cyber Warfare under International Laws of Armed Conflict</i>	73
1.5.13.2.	<i>Challenges to Cyber Arms Control</i>	76
1.5.13.3.	<i>Cyber Deterrence</i>	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:

INTER NATIONAL RESPONSES AND LEGAL MEASURES ON CYBERSECURITY

2.	Introduction	95
2.1.	International responses on cybersecurity	96
2.1.1.	The United Nations	96
2.1.1.1.	<i>The Eighth United Nations Congress on the Prevention of Crime and Treatment of Offenders</i>	96
2.1.1.2.	<i>The United Nations Resolution 55/63 on Combating the Criminal Misuse of Information Technology</i>	98
2.1.1.3.	<i>The United Nations Resolution 56/121 on Combating the Criminal Misuse of Information Technology</i>	99
2.1.1.4.	<i>United Nations Resolution 57/239 on the Creation of a Global Culture of Cyber Security</i>	100

2.1.1.5.	<i>United Nations Resolution 58 199 on the Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures</i>	102
2.1.1.6.	<i>United Nations Resolutions on Developments in the Field of Telecommunications in the Context of International Security</i>	104
2.1.1.7.	<i>Other Notable United Nations Resolutions on Cybersecurity</i>	104
2.1.1.8.	<i>The Internet Governance Forum (IGF)</i>	106
2.1.1.9.	<i>Recent Developments</i>	106
2.1.2.	<i>The International Telecommunications Union (ITU)</i>	107
2.1.2.1.	<i>The World Summit on the Information Society (WSIS)</i>	108
2.1.2.2.	<i>The ITU High Level Expert Group (HLEG) on Cybersecurity</i>	111
2.1.3.	<i>The Group of Eight (G8)</i>	112
2.1.4.	<i>The Interpol</i>	116
2.1.5.	<i>The Council of Europe</i>	117
2.1.6.	<i>European Union (EU)</i>	120
2.1.7.	<i>The Asian Pacific Economic Cooperation (APEC)</i>	122
2.1.8.	<i>The Organization for Economic Cooperation and Development (OECD)</i>	124
2.1.9.	<i>The Commonwealth</i>	126
2.1.10.	<i>The Organization of American States (OAS)</i>	128
2.1.11.	<i>The Association of South-East Asian Relations (ASEAN)</i>	130
2.1.12.	<i>The North Atlantic Treaty Organization (NATO)</i>	131
2.1.13.	<i>The Arab League and Gulf Cooperation Council</i>	132
2.1.14.	<i>The Stanford Proposal</i>	132
2.1.15.	<i>The Global Protocol on Cybersecurity and Cybercrime</i>	133
2.1.16.	<i>The International Multilateral Partnership Against Cyber Threats (IMPACT)</i>	134
2.2	<i>An analysis of international legal frameworks on cybersecurity</i>	135
2.2.1	<i>The Council of Europe Convention on Cybercrime</i>	135
2.2.1.1.	<i>Measures to be taken at the National Level with Regards to Substantive Criminal Law</i>	137
2.2.1.2.	<i>Measures to be taken at the National Level with regards to Procedural Law</i>	154
2.2.1.3.	<i>Measures to be taken at the National Level with regards to the establishment of Jurisdiction</i>	162
2.2.1.4.	<i>Measures to be taken with regards to International Cooperation</i>	163
2.2.2.	<i>The Commonwealth Model Law on Computer and Computer Related Crime</i>	174
2.2.2.2.	<i>Introduction- Matters Regarding the Usage of Terms and State Jurisdiction</i>	175
2.2.2.3.	<i>Offences</i>	176
2.2.2.4.	<i>Procedural Powers</i>	178
2.2.3.	<i>The Draft International Convention to Enhance Protection from Cybercrime and Terrorism</i>	183

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

CHAPTER THREE:

NATIONAL REGULATORY RESPONSES TO CYBERSECURITY IN SELECT JURISDICTIONS

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

3.1.3.4.	<i>The United States International Strategy for Cyberspace</i>	236
3.1.4.	Recent Developments	236
3.1.4.1.	<i>The United States International Cybercrime Reporting and Cooperation Bill</i>	236
3.2.	The United Kingdom	237
3.2.1.	Legal Measures	238
3.2.1.1.	<i>The Computer Misuse Act</i>	238
3.2.2.2.	<i>Other Enactments on Cybersecurity</i>	254
3.2.2.2.1.	<i>The Terrorism Act</i>	254
3.2.2.2.2.	<i>The Counter-Terrorism Act</i>	255
3.2.2.2.3.	<i>Regulation of Investigatory Powers Act</i>	256
3.2.2.2.4.	<i>The Fraud Act</i>	256
3.2.2.2.5.	<i>The Police and Justice Act</i>	257
3.2.3.	Institutional Regulatory Mechanisms	257
3.2.3.1	<i>The Serious and Organized Crime Agency (SOCA)</i>	257
3.2.3.2	<i>The Communications Electronics Security Group (CESG)</i>	258
3.2.3.3.	<i>The UK Computer Emergency Response Team (GovCertUK)</i>	258
3.2.3.4.	<i>The Center for the Protection of National Infrastructure (CPNI)</i>	258
3.2.3.5.	<i>The Office of Cyber Security</i>	259
3.2.3.6.	<i>The Cyber Security Operations Centre</i>	260
3.2.3.7.	<i>The Internet Watch Foundation (IWF)</i>	260
3.2.4	Policy Mechanisms	260
3.2.4.1.	<i>The Cyber Security Strategy of the United Kingdom</i>	260
3.3.	Singapore	261
3.3.1.	Legal Measures	261
3.3.1.1.	<i>The Computer Misuse Act of Singapore</i>	261
3.3.1.2.	<i>Other Enactments on Cybersecurity</i>	275
3.3.1.2.1.	<i>The Spam Control Act of Singapore</i>	275
3.3.2.	Institutional Regulatory Mechanisms	275
3.3.3.	Policy Mechanisms	277
3.3.3.1.	<i>The Infocomm Security Master Plan 2</i>	277
3.3.3.2.	<i>The National Trust Framework (NTF)</i>	278
3.4.	India	279
3.4.1.1.	<i>The Indian Information Technology Act</i>	280
3.4.1.2.	<i>Other Enactments on Cybersecurity</i>	306
3.4.1.2.1.	<i>The Information Technology (Guidelines for Cyber Cafe) Rules 2011</i>	306
3.4.2.	Institutional Regulatory Mechanisms	309
3.4.2.1.	<i>Adjudicatory Mechanisms</i>	309
3.4.2.2.	<i>The Department of Information Technology</i>	311
3.4.2.3.	<i>The Indian Computer Emergency Response Team</i>	311
3.4.2.4.	<i>The National Nodal Agency</i>	312
3.4.3.	Policy Mechanisms	312
3.4.3.1.	<i>The Indian Cybersecurity Strategy</i>	312
3.5.	The People's Republic of China	314
3.5.1.	Legal Measures	316

3.5.1.1.	<i>The Computer Information Network and Internet Security, Protection and Management Regulations</i>	316
3.5.1.2.	<i>The Chinese Regulations on Safeguarding Computer Information Systems</i>	328
3.5.1.3.	<i>The State Secrecy Protection Regulations for Computer Information Systems on the Internet</i>	330
3.5.1.4.	<i>The Criminal Law of the People’s Republic of China</i>	332
3.5.2.	<i>Institutional Regulatory Mechanisms</i>	344
3.5.2.	<i>Policy Mechanisms</i>	345
3.5.2.1.	<i>China’s National Defense Strategy 2010</i>	345
3.6.	<i>The Russian Federation</i>	346
3.6.1.	<i>Legal Measures</i>	348
3.6.1.1.	<i>The Criminal Code of the Russian Federation</i>	348
3.6.1.2.	<i>The Law of the Russian Federation on the Legal Protection of Computer Programmes and Data Bases</i>	354
3.6.2.	<i>Institutional Regulatory Mechanisms</i>	355
3.6.3.	<i>Policy Mechanisms</i>	356
3.6.3.1.	<i>The Russian Information Security Doctrine</i>	356
3.6.4.	<i>Russia and the Council of Europe Convention on Cybercrime</i>	358
3.7.	<i>An Overview of Some Major Regulatory Challenges</i>	361
3.7.1.	<i>Use of Cyber Devices for Dual Purposes and the Availability of Malicious Cyber Tools</i>	361
3.7.2.	<i>The Constant Evolution of Malicious Cyber Tools</i>	362
3.7.3.	<i>Under-Reporting</i>	362
3.7.4.	<i>High Costs of Investigating and Prosecuting Cybercrime</i>	363
3.7.5.	<i>Challenges of Obtaining and Preserving Digital Evidence</i>	363
3.7.6.	<i>Investigation and Prosecution of Suspects Located Abroad</i>	364
3.7.7.	<i>Proof of Offences</i>	367
3.7.8.	<i>“Forum Shopping” by Criminal Actors</i>	368
3.7.9.	<i>Other Challenges</i>	368

**CHAPTER FOUR:
MULTILATERAL REGULATORY RESPONSES TO
CYBERSECURITY IN AFRICA**

4.	<i>Introduction</i>	371
4.1.	<i>Regional Multilateral Responses</i>	374
4.1.1.	<i>The African Union (AU)</i>	374
4.1.1.1.	<i>The Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa</i>	376
4.1.1.1.1.	<i>Basic Principles to Promote Cybersecurity in African States</i>	377
4.1.1.1.2.	<i>Provisions Relating to the Establishment of Cybercrime Offences</i>	385
4.1.1.1.3.	<i>Some Perceived Problems of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity</i>	394
4.2.	<i>Sub-Regional Multilateral Responses</i>	397
4.2.1.	<i>The Economic Community of West African States (ECOWAS)</i>	397

4.2.2.	<i>The Southern African Development Community (SADC)</i>	398
4.2.3.	<i>The East African Community (EAC)</i>	398

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.	<i>The Electronic Communications and Transactions Act</i>	403
5.1.1.2.	<i>The Interception and Monitoring Prohibition Act and Other Related Enactments on Cybersecurity</i>	416
5.1.2.	Institutional Regulatory Mechanisms	417
5.1.2.1.	<i>Cyber Inspectors</i>	417
5.1.2.2.	<i>ECS-CSIRT</i>	417
5.1.4.	Policy Mechanisms	418
5.1.3.1.	<i>The Draft Cybersecurity Policy of South Africa</i>	418
5.2.	Botswana	419
5.2.1.	Legal Measures	420
5.2.1.1.	<i>The Cybercrime and Computer Related Crimes Act</i>	420
5.2.2.	Institutional Regulatory Mechanisms	445
5.3.	Mauritius	445
5.3.1.	Legal Measures	446
5.3.1.1.	<i>The Computer Misuse and Cybercrime Act</i>	446
5.3.2.	Institutional Regulatory Mechanisms	447
5.3.2.1.	<i>The Mauritian national Computer Security Incident Response Team (CERT-MU)</i>	448
5.4.	Senegal	448
5.4.1.	Legal Measures	449
5.4.1.1.	<i>The Senegalese Law on Cybercrime</i>	449
5.5.	Kenya	459
5.5.1.	Legal Measures	459
5.5.1.1.	<i>The Kenya Communications (Amendment) Act</i>	459
5.5.2.	Policy Mechanisms	460
5.5.2.1.	<i>The Kenyan Information and Communications Technology Policy</i>	460
5.5.3.	Institutional Regulatory Mechanisms	460
5.5.3.1.	<i>The Kenya Computer Security Incident Response Team (CSIRT-Kenya)</i>	460
5.6.	Ghana	461
5.6.1.	Legal Measures	462
5.6.1.1.	<i>The Electronic Transactions Act</i>	462
5.6.2.	Institutional Regulatory Mechanisms	470
5.7.	Brief Overviews of Regulatory Responses in other African States	472
5.7.1.	Algeria	472

5.7.2.	<i>Angola</i>	472
5.7.3.	<i>Cameroon</i>	473
5.7.4.	<i>Egypt</i>	474
5.7.5.	<i>Ethiopia</i>	475
5.7.6.	<i>Gambia</i>	476
5.7.7.	<i>Lesotho</i>	476
5.7.8.	<i>Morocco</i>	477
5.7.9.	<i>Namibia</i>	477
5.7.10.	<i>Niger</i>	478
5.7.11.	<i>Seychelles</i>	478
5.6.12.	<i>Swaziland</i>	478
5.7.13.	<i>Tanzania</i>	479
5.7.14.	<i>Tunisia</i>	480
5.7.15.	<i>Uganda</i>	481
5.7.16.	<i>Zambia</i>	482

CHAPTER SIX:

CYBERSECURITY LAW AND REGULATION IN NIGERIA

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

6.5.	An Analysis of Proposed Legal Measures	508
6.5.1.	<i>The Computer Security and Critical Information Infrastructure Protection Bill</i>	508
6.5.2.	<i>Comments on the Computer Security and Critical Information Infrastructure Protection Bill</i>	534
6.5.3.	<i>The Nigerian Cybersecurity and Data Protection Agency Bill</i>	535
6.6.	Peculiar Causes of Cyber-insecurity and the Regulatory Challenges of Cybersecurity in Nigeria	537
6.6.1.	<i>Legal Challenges</i>	538
6.6.1.1.	<i>Lack of appropriate legal frameworks on cybersecurity</i>	538
6.6.1.2.	<i>Challenges arising from the legal status of digital evidence</i>	540
6.6.2.	<i>Weak Institutional Capacities</i>	542
6.6.3.	<i>Absence of Effective Synergy and Cooperation between Regulatory Institutions on Cybersecurity</i>	542
6.6.4.	<i>Poor Regulatory Oversight</i>	543
6.6.5.	<i>Digital Divide</i>	544
6.6.6.	<i>Lack of Resources and Skilled Manpower</i>	544
6.6.7.	<i>Under Reporting</i>	544
6.6.9.	<i>The Deployment of Internet Services without Technical Security Solutions</i>	547
6.6.10.	<i>Lack of End-User Awareness</i>	548
6.6.11.	<i>Poor Socio-Economic Conditions and the Deterioration of Societal Values</i>	549
6.6.12.	<i>Massive Influx of Electronic Waste</i>	553
6.7.	Implications of Inadequate Regulatory Responses to Cyber(in)security on National Security, Human Security, Human Rights, International Relations and Economic Development in Nigeria	554
6.7.1.	<i>National Security</i>	554
6.7.2.	<i>Human Security</i>	555
6.7.3.	<i>Human Rights</i>	557
6.7.4.	<i>International Relations</i>	558
6.7.5.	<i>National Economic Development</i>	559

**CHAPTER SEVEN:
POLICY AND REGULATORY PROPOSALS TO ENHANCE
CYBERSECURITY**

7.	Introduction	563
7.1.	Policy and Regulatory Proposals to Enhance Cybersecurity in Africa	563
7.1.1.	<i>Legal Strategies</i>	566
7.1.2.	<i>Building Capacities in Legislative and Regulatory Institutions</i>	567
7.1.3.	<i>Building Capacities in Business Organizations</i>	568
7.1.4.	<i>Building Capacities for End-User Education</i>	570
7.1.5.	<i>Building Capacities to enhance the implementation of Technical</i>	

	<i>Solutions to Cybersecurity</i>	571
7.1.6.	<i>The establishment of Computer Emergency Response Teams (CERTs)</i>	572
7.1.8.	<i>The Establishment of Fraud Complaints Units</i>	574
7.1.9.	<i>Regulation of Money Transfer Services</i>	574
7.1.10.	<i>Enhancing the Participation of National Governments</i>	575
7.1.11.	<i>Private Sector Participation</i>	576
7.1.12.	<i>Bridging the Digital Divide in African Countries</i>	577
7.1.13.	<i>Enhancing Social and Economic Conditions and Strengthening Societal Values</i>	578
7.2.	Policy and Regulatory Proposals to Enhance Global Cybersecurity	579
7.2.1.	<i>The Need for a Global Legal Framework on Cybersecurity</i>	579
7.2.2.	<i>Cyber Diplomacy</i>	581
7.2.3.	<i>Enhancing Global Capacities for Incident Management</i>	581
7.3.	Concluding Remarks: Towards the Collective Responsibility of States for Global Cybersecurity	585
	Selected Bibliography	591
A.	Textbooks	591
B.	Chapters in Textbooks	595
C.	Journal Articles	598
D.	Reports	608
E.	Thesis	614
F.	Conference Proceedings	615
G.	Articles in Newspapers and Magazines	618
H.	Internet Sources	619
I.	Dictionaries	626
J.	Movies /Music Videos	626
	Index	628

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

Abacha v. Fawehinmi (2000) 6 NWLR (pt. 660) 540

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

E.F.C.C. v. Fani Kayode (2009) [Unreported] <<http://www.efcc.org/cases>> 540

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

Nuba Commercial Farms Limited v. Nal Merchant Bank Ltd (2002) 24 WRN 157 (2003) FWLR (Pt 145) 661 C.A 540

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

S.B.N Ltd v. De Lluch (2004) 18 NWLR (pt, 905) 578

Singapore

Public Prosecutor v. Muhammad Nuzaihan bin Kamal Luddin (2000) 1 S.L.R. 34; (1999) SGHC 275 261,264,269,423

Prosecutor v. Navaseelan Balasingam (2006) SGDC 156 265

South Africa

Narlis v. South African Bank of Athens (1976) (2) SA 573 (A) 409

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

S v. Ndiki (2008) (2) SACR 252 409

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

DPP v. Bignell (1988) 1. Cr. App. Rep. 1 242

<i>Edward Yearly v. Crown Prosecution Service</i> (1997) QB EWHC Admin 30821/03/1997	243
<i>Harrods v. UK Network Services Limited and Others.</i> (Unreported, Chancery Division, 9/12/1996)	63,521
<i>Marks and Spencer v. One in a Million Ltd</i> (Unreported, Court of Appeal, 23/7/98 23)	63,521
<i>Morgans v. DPP</i> (2000) 2 WLR 386; (1999) 1 WLR 968	253
<i>R v. Aaron Caffrey.</i> (Unreported, Southwark Crown Court, 17/10/2003)	367,368
<i>R v. Alfred Whittaker</i> (Unreported, Scunthorpe, Magistrates Court)	246,515
<i>R v. Bow Street Magistrates Court and Adeniyi Momodu Allison ex parte United States Government</i> (1999) 4 All ER	242,253
<i>R v. Daniel Cuthbert</i> (Unreported, Horseferry, Road Magistrates Court 07/10/2005)	243
<i>R v. Emma Pearce and Malcolm Farquhason.</i> (Unreported, Croydon Magistrate Court, 9/12/1993)	245
<i>R v. Gold & Schifreen</i> (1988) AC 1063; (1988) 2 WLR. 984	239
<i>R v. Governor of Brixton Prison Exp. Levin</i> (1997) QB G5: affd (1997)3 All ER 289, HL Unreported. November, 1992)	253
<i>R v. Ian Morris and Richard Airlie</i> (Unreported Cardiff Crown Court)	247
<i>R v. Michelle Begley</i> (Unreported, Coventry Magistrates Court)	243
<i>R v. Mark Hopkins</i> (Unreported, Westminster Magistrates Court 09/08/2007)	243
<i>R v. Matthew Byrne</i> (Unreported, Southwark Crown Court 07/11/2006)	247
<i>R v. Ross Pearlstone</i> (Unreported, Bow Street Magistrates Court)	.245
<i>R v. Pile</i> (Unreported, Plymouth Crown Court, 1995)	247, 268
<i>R v. Pryce</i> (Unreported, Bow Street Magistrate Court, 21/3/1997)	252
<i>R v. Richard Goulden</i> (Unreported, Southwark Crown Court, June 1992)	246,515
<i>R v. Simon Vallor</i> (Unreported, Southwark Crown Court, 21/01/2003)	246,247
<i>R v. Stephen Carey</i> (Unreported, Hove Crown Court 19/09/2002)	247
<i>R. v. Thompson</i> (1984) 1 WLR 962	238
<i>Rubicon Computer Systems v. United Paints Limited</i> (2000) 2 TCLR 453	37
<i>Saltman Engineering Co. Ltd v. Campbell Engineering Co. Ltd</i> (1948) 65 RPC 203	31
<i>Simkins Partnership v. Reeves Lund & Co. Ltd</i> (Lawtel, 2003)	299
<i>Thomas Marshall (Exports) Ltd. v. Guinle</i> (1979) Ch. 227	31
<i>Yarimaka v. Governor of HM Prison Brixton</i> , (2002) QB, EWHC 589 (Admin) 47,254	
<i>Zezex and Yarimaka v. Governor of HM Prison Brixton and Government of the United States of America</i> (2002) QB, EWHC 589 (Admin)	254
 United States	
<i>America Online, Inc. v. LCGM, Inc.</i> 46 F. Supp. 2d 444, 444 (E.D. Va. 1998)	60
<i>America Online, Inc. v. National Health Care Discount, Inc.</i> , 121 F. Supp. 2d 1255 (N.D.Iowa 2000)	32,219
<i>Hotmail Corp. v. Van Money Pie, Inc.</i> No., 98-20064, 1998 U.S. Dist. LEXIS 10729 (N.D. Cal April 16, 1998)	60
<i>Intermatic Inc. v. Dennis Toeppe</i> n (pre-ACPA), No. 96 C, 1982. United States	

District Court, N.D. Illinois, Eastern Division. Nov. 26, 1996	63,521
<i>International Airport Centers, L.L.C. v. Citrin</i> , 440 F.3d 418, 420-21 (7th Cir. 2006)	32
<i>Ognibene v. Citibank</i> (446 NYS 2d 845 (CIV.Ct.1981)	570
<i>Pearl Investments v. Standard I/O</i> , 257 F.Supp.2d 326, 349 (D.Me. 2003)	217
<i>People v. Casey</i> , 225 Ill. App.3d 82 (Ill. App. Ct. 1992)	285,423
<i>Re America Online, Inc.</i> 168 F. Supp. 2d 1359 (S.D Fla. 2001)	221
<i>Re Grand Jury Subpoena to Sebastien Boucher</i> , WL 424718 (United States District Court for the District of Vermont 19/2/2009)	160,364
<i>Shaw v. Toshiba America Information Systems</i> , 91 F. Supp. 2d 926, 931, (E.D. Tex. 1999)	223
<i>Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.</i> , 119 F. Supp. 2d 1121, 1124 (W.D. Wash. 2000)	32
<i>Trans World Airlines Inc. v. Franklin Mint Corp.</i> (1984) 466 U.S 243	210
<i>United States v. Bae</i> , 250 F.3d 774 (D.C. Cir. 2001)	221
<i>United States v. Gajdik</i> (2002) 292 F.3d 555	67
<i>United States v. Gorshkov</i> , WL 1024026 (W.D. Wash. 2001)	227,365
<i>United States v. Ivanov</i> , 175 F. Supp. 2d 367 (D. Conn. 2001)	64,227,284, 365, 435
<i>United States v. Lindsley</i> (2001) WL 502832 (5th Cir. 2001)	221,423
<i>United States v. Lloyd</i> , 269 F.3d 228, 231 (3d Cir. 2001)	224
<i>United States v. Middleton</i> , 231 F.3d	224
<i>United States v. Mitra</i> , 405 F.3d 492 (7th Cir.2005)	225
<i>United States v. Morris</i> , 928 F.2d 504 (2d Cir. 1991)	216,223,242
<i>United States v. Pirello</i> , 255 F.3d 728 (9th Cir. 2001)	230
<i>United States v. Riggs</i> , 739 F. Supp. 414 (N.D. Ill. 1990)	219
<i>United States v. Rushdan</i> , 870 F.2d 1509, 1514 (9th Cir. 1989)	226
<i>United States v. Scartz</i> , 838 F.2d 876, 879 (6th Cir. 1988)	226
<i>United States v. Sullivan</i> , 40 Fed. Appx. 740 (4th Cir. 2002)	223
<i>United States v. Tucker</i> , 150 F Supp 2d 1263 (D Utah 2001) 305 F 3d 1193 (10th Cir, 2002)	147
<i>United States v. Willis</i> , 476 F.3d 1121, 1125 (10th Cir. 2007)	219

International Arbitration and Court Cases

<i>August v. the United Kingdom</i> .(January 2003) no. 36505/02, 21	587
<i>Calvelli and Ciglio v. Italy</i> [GC], (2002) no. 32967/96, ECHR 2002-IX	587
<i>Cyprus v. Turkey</i> (2001) ECHR No.25781/94	586
<i>Gallup Inc. v. Jerome Obinabo</i> (The American National Arbitration Forum Claim No. FA0110000100756, 2/1/2002)	63,521
<i>Shell International Petroleum Co. v. Allen Jones</i> (WIPO Case No D2003-0821, 18/12/2003)	63,521
<i>Osman v. the United Kingdom</i> , judgment of 28 October 1998, Reports 1998-VIII, p. 3164	587
<i>Telstra Corporation Limited v. Nuclear Marshmallow</i> (Case No. D 2000-0003 Administrative Panel Decision at the WIPO Arbitration and Mediation Center)	63,521

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

Senegalese Law on Cybercrime No. 2008-11 (2008)

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 (RICPCRIA) 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

Consumer Protection and Respect of Intellectual Property Law,
N°1994-36

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 Computer Information Network and Internet Security,
Protection and Management Regulations 1997

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

Law of the Russian Federation on the Legal Protection of Computer
Programmes and Data Bases 1992

Russian Information Security Doctrine 2000

Singapore

Computer Misuse Act of Singapore, Cap.50A, Rev. Ed., 2007

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

CAN-SPAM Act 2003, Pub. L. No. 108-187, 117

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

Federal Information Security Management Act, P.L.107-347, Title III
2002

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:
Presidential Decision Directive No. 63, May 22, 1998

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

African Charter on Human and Peoples Rights (1981)
Constitutive Act of the African Union (2001)
Draft African Union Convention on the Establishment of a Credible
Legal Framework for Cybersecurity in Africa, AU Draft0 010111,
Version 01/01.2011

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)
Regulation (EC) No 460/2004 establishing the European Network and
information security Agency (2004)
The European Union Directive on Privacy and Electronic Communication
Directive 2002/58/EC Concerning the Processing of Personal Data and
the Protection of Privacy in the Electronic Communications Sector (12
July, 2002)

EU Communication on a General Policy on the Fight against Cybercrime, COM (2007)

EU Data Retention Directive 2005/0182/COD

EU Communication -Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer Related Crime 26.1 2001, COM (2000)

EU Framework Decision on Attacks against Information Systems 2005/222/JHA (24 February 2005)

EU Council Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography 2004/68/JHA (2003)

EU (2001) Network and Information Security- A European Policy Approach (6 June 2001)

EU Directive on Privacy and Electronic Communications (2002)

Group of Eight (G8)

G8 Okinawa Charter on Global Information Society (2000)

G8 Communiqué Annex: Principles to Combat High-Tech. Crime (1997)

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

United Nations Convention on the Rights of the Child (1989)

Universal Declaration of Human Rights

Optional Protocol to the Convention on the Rights of the Child on Sale of Children, Child Prostitution and Child Pornography (1989)

United Nations Convention against Transnational Organized Crime (2000)

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

Resolution 58/199 on the Creation of a Global Culture of Cybersecurity and Protection of Critical Information Infrastructures (A/RES 58/199) 23 December 2003

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 Code on Peace and Security in Cyberspace - A Global Protocol on Cybersecurity and Cybercrime

Draft International Convention to Enhance Protection from Cybercrime and Terrorism

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (25 July 2002)

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
Principles, Building the Information Society: A Global challenge in the New
Millennium* (2003)
World Summit on the Information Society (WSIS) *Plan of Action* (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