SpringerBriefs in Cybersecurity

Cybersecurity is a difficult and complex field. The technical, political and legal questions surrounding it are complicated, often stretching a spectrum of diverse technologies, varying legal bodies, different political ideas and responsibilities. Cybersecurity is intrinsically interdisciplinary, and most activities in one field immediately affect the others. Technologies and techniques, strategies and tactics, motives and ideologies, rules and laws, institutions and industries, power and money—all of these topics have a role to play in cybersecurity, and all of these are tightly interwoven.

The *SpringerBriefs in Cybersecurity* series is comprised of two types of briefs: topic- and country-specific briefs. Topic-specific briefs strive to provide a comprehensive coverage of the whole range of topics surrounding cybersecurity, combining whenever possible legal, ethical, social, political and technical issues. Authors with diverse backgrounds explain their motivation, their mindset, and their approach to the topic, to illuminate its theoretical foundations, the practical nuts and bolts and its past, present and future. Country-specific briefs cover national perceptions and strategies, with officials and national authorities explaining the background, the leading thoughts and interests behind the official statements, to foster a more informed international dialogue.

More information about this series at http://www.springer.com/series/10634

Aamo Iorliam

Cybersecurity in Nigeria

A Case Study of Surveillance and Prevention of Digital Crime

Springer

Aamo Iorliam
Department of Mathematics
and Computer Science
Benue State University
Makurdi, Nigeria

ISSN 2193-973X ISSN 2193-9748 (electronic)
SpringerBriefs in Cybersecurity
ISBN 978-3-030-15209-3 ISBN 978-3-030-15210-9 (eBook)
https://doi.org/10.1007/978-3-030-15210-9

Library of Congress Control Number: 2019933714

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To God Almighty

Foreword

This five-chapter book titled Cybersecurity in Nigeria—A Case Study of Surveillance and Prevention of Digital Crime by Dr. Iorliam is a handbook containing all you need to know about cyber surveillance in Nigeria. It looks at how cyber surveillance could stop digital crimes in Nigeria and by extension the world.

The author knows his stuff, having earned an M.Sc. in Forensic Computing with a distinction from Coventry University and a Ph.D. in Computer Science with a thesis focusing on the Application of Power Laws to Biometrics, Forensics and Network Traffic Analysis from the University of Surrey, both in UK. From these universities, he was able to sharpen and cut his academic teeth.

The book demonstrates his knowledge of his research areas which include Power laws, machine learning, data mining, image analysis, digital and multimedia forensics, cybersecurity, biometrics, computer forensics and network traffic analysis.

From his research standpoint, the author delved into areas of the application of forensic science to solve problems in network traffic analysis, fake news detection and the development of a digital surveillance software to prevent/detect digitally facilitated crimes in Nigeria.

This book is divided into five chapters;

Chapter 1 provides the necessary introduction that a reader needs to be able to understand and get the best out of the book.

Chapter 2 shows how Natural laws can effectively detect malicious traffic on the Internet.

Chapter 3 shows how Natural laws can solve a very important challenge in Nigeria—fake news detection.

Chapter 4 provides an explanation to how cyber crimes occur in Nigeria and the need for cybersecurity and mobile device forensics to solve this challenge.

Chapter 5 proposes a digital surveillance software (A-BOT) that can effectively stop digital crimes in Nigeria.

This book is a must read for forensic scientists, cryptographers, stenographers and all law enforcement agencies in Nigeria. It is a gift from Dr. Iorliam to a world in dire need of the knowledge on the secrets of forensic science in solving different types of crimes. I strongly recommend this book to you!

Lokoja, Nigeria
January 2019

Prof. Sunday Eric Adewumi, Ph.D., fncs
Dean, Faculty of Science
Federal University Lokoja

Preface

It is not new that the Nigerian cyber space and its cyber infrastructure is very porous and has given much room to cyber attackers to freely operate. In 2017, 3500 cyber attacks on the Nigerian cyber space were successful. This led to Nigeria losing 450 million dollars [1].

These cyber crimes are hampering Nigeria's digital economy. This further explains why many Nigerians are not convinced about Internet marketing and online transactions that involve money. This is worrisome even for the Nigerian military intelligence. If sensitive conversations using digital devices (e.g. phones or computers) are not well monitored, then Nigeria will be defeated in the cyber warfare. If Nigeria loses the cyber warfare, then our digital economy, military intelligence and related sensitive firms will also crumble.

The Nigerian Army Cyber Warfare Command was instituted in 2018 with a task to solve terrorism, banditry and other attacks by criminal groups in Nigeria [2]. This is a right step by the Nigerian government. However, there is every need to provide digital surveillance to the Nigerian cyber space to assist law enforcement agencies in Nigeria to prevent/detect these digitally facilitated crimes.

Therefore, monitoring of Nigeria's cyber space and its cyber infrastructure has become imperative given that the rate of criminal activities has increased tremendously using technology. Cyber infrastructure consists of computing systems, data storage systems, advanced instruments and data repositories, visualization environments and people, all linked by high-speed networks to make possible scholarly innovation and discoveries not otherwise possible. Information technology systems that provide particularly powerful and advanced capabilities could also be referred to as cyber infrastructure [3]. This book proposes the use of digital surveillance aimed at investigating, detecting, uncovering and interpreting any fraud associated with the cyber space and critical cyber infrastructures in Nigeria. This will make the Nigerian digital ecosystem free of cyber attackers. This digital surveillance includes

passive forensic investigations (investigations where an attack has already occurred) and active forensic investigations (real-time investigations to track attackers). Hence, producing a zero-cyber crime Nigeria.

Makurdi, Nigeria
January 2019

Dr. Aamo Iorliam

References

1. The Paradigm (2017) Nigerias cyberspace has become very porous-senate. http://www.theparadigmng.com/2017/05/24/nigerias-cyberspace-become-porous-senate/. Accessed 27 Nov 2018
2. Sunnewsonline (2018) Insurgency: army establishes cyber warfare command. http://sunnewsonline.com/insurgency-army-establishes-cyber-warfare-command/. Accessed 27 Nov 2018
3. Indiana University (2018) What is cyberinfrastructure?. https://kb.iu.edu/d/auhf. Accessed 27 Nov 2018

Acknowledgements

Special thanks to the following:

- Springer Team: For your support towards making the publication of this book a huge success.
- My Ph.D. supervisors: Prof. Anthony T. S. Ho, Prof. Shujun Li, Dr. Norman Poh and Prof. Adrian Waller who mentored me.
- To my friends: Dr. Santosh Tirunagari, Shangbum Caleb Faveren, Dr. Nyinoh Iveren, Oshido Barnabas, Ode Egena, Dr. Ikyanyon Darius.
- To my family members: Mr. and Mrs. Iorliam (Dad and Mum), Eng. Dr. and Dr. (Mrs.) Yala Iorliam, Pastor and Mrs. Aondowase Tsuaa, Mr. and Barr. (Mrs.) Nguetar Iorliam, Mr. and Mrs. Ukaan.
  And most importantly, my wife Iveren (Udookwase), and my two daughters, Afam and Asoose, who supported and encouraged me throughout the whole process of writing this book.

Contents