1.

Record Nr.	UNINA9910337578403321
Autore	Iorliam Aamo
Titolo	Cybersecurity in Nigeria : A Case Study of Surveillance and Prevention of Digital Crime / / by Aamo Iorliam
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-15210-3
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (68 pages)
Collana	SpringerBriefs in Cybersecurity, , 2193-973X
Disciplina	005.8
Soggetti	Computer networks - Security measures Computer crimes Africa—Economic conditions Computer networks Biometry Computers Law and legislation Mobile and Network Security Cybercrime African Economics Computer Communication Networks Biometrics Legal Aspects of Computing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction -- Natural Laws (Benford’s Law and Zipf’s Law) for Network Traffic Analysis -- Combination of Natural Laws (Benford’s Law and Zipf’s Law) for Fake News Detection -- Cybersecurity and Mobile Device Forensic -- Proposed Digital Surveillance Software.
Sommario/riassunto	This book reviews the use of digital surveillance for detecting, investigating and interpreting fraud associated with critical cyberinfrastructures in Nigeria, as it is well known that the country’s cyberspace and cyberinfrastructures are very porous, leaving too much room for cyber-attackers to freely operate. In 2017, there were 3,500

successful cyber-attacks on Nigerian cyberspace, which led to the country losing an estimated 450 million dollars. These cybercrimes are hampering Nigeria’s digital economy, and also help to explain why many Nigerians remain skeptical about Internet marketing and online transactions. If sensitive conversations using digital devices are not well monitored, Nigeria will be vulnerable to cyber-warfare, and its digital economy, military intelligence, and related sensitive industries will also suffer. The Nigerian Army Cyber Warfare Command was established in 2018 in order to combat terrorism, banditry, and other attacks by criminal groups in Nigeria. However, there remains an urgent need to produce digital surveillance software to help law enforcement agencies in Nigeria to detect and prevent these digitally facilitated crimes. The monitoring of Nigeria’s cyberspace and cyberinfrastructure has become imperative, given that the rate of criminal activities using technology has increased tremendously. In this regard, digital surveillance includes both passive forensic investigations (where an attack has already occurred) and active forensic investigations (real-time investigations that track attackers). In addition to reviewing the latest mobile device forensics, this book covers natural laws (Benford’s Law and Zipf’s Law) for network traffic analysis, mobile forensic tools, and digital surveillance software (e.g., A-BOT). It offers valuable insights into how digital surveillance software can be used to detect and prevent digitally facilitated crimes in Nigeria, and highlights the benefits of adopting digital surveillance software in Nigeria and other countries facing the same issues.