A Review of Application Challenges of Digital Forensics

Kenneth Okereafor [1], Rania Djehaiche [2]

[1] *Department of Information and Communications Technology*, Database Security Division,
National Health Insurance Scheme (NHIS) Abuja, Nigeria.
nitelken@yahoo.com

[2] *Department of Electronics*, Faculty of Sciences and Technology,
Mohamed El Bachir El Ibrahimi University of Bordj Bou Arreridj, Algeria.
rania.djehaiche@univ-bba.dz

***Abstract* - The growing preference of automation and digital transformation over semi manual operations in the corporate world has led to an exponential rise in the applications of computer technology, internet and web assets for everyday living, resulting in significant behavioural adjustments, particularly how humans communicate with each other and interact with the environment. Unfortunately, digital growth has also given rise to different forms of cyber criminalities in industry, government and academia. With many cyberattacks becoming more and more sophisticated, it is equally becoming increasingly difficult to trace cybersecurity breaches without first establishing an accurate mechanism for data collection and analysis offered by digital forensics. In the absence of reliable data analysis, the scope of digital forensic operations required to respond to modern cybersecurity breaches could become significantly challenging, costly and open-ended. This paper reviews the major challenges faced by organizations in performing effective digital forensic operations.**

Keywords - ***Analysis, breach, cyberattack, cybersecurity, data, digital forensics, evidence, organization.***

I. INTRODUCTION

Concerns over cybersecurity are becoming a recurring event in everyday life. From theft of banking information, and unauthorized modification of mobile subscriber data, to unethical privacy infringements, the spate of cyberattacks cuts across all sectors of human endeavour, costing organizations and governments huge losses in revenue and reputation. There is an increasingly widespread use of personal computers and other digital assets in businesses and homes, as a result of which organizations are now exchanging information online more than ever before [1] [2] and this has increased high-tech crimes to significant proportions. The rising incidents of cyberattacks and the attendant consequences all together provide the justification to embrace systematic incident response mechanisms. Responding to high-tech crimes and performing effective incident response operations must follow a systematic approach based on a credible forensic exercise. This paper identifies the challenges encountered while using forensic techniques to implement cybersecurity countermeasures particularly to assist with computer incident response.

The rest of the paper is organized as follows: Section II explores the cybersecurity landscape that justifies everyday concerns over cyberspace safety. Section III discusses selected high profile cyberattacks of global proportion. Section IV reviews digital forensics processes and sources of digital evidence, highlighting their industrial and commercial applications. Section V discusses current challenges to performing effective digital forensic operations. Section VI concludes the paper and summarizes the key points.

II. CURRENT CYBERSECURITY LANDSCAPE

We live in a highly connected world of data moving in many forms, as a result of which the society relies on their effective analysis and management across various types of digital networks. Hence network security is constantly evolving owing to traffic growth, usage trends and the ever-changing threat landscape [3]. Cybersecurity, as a broad range of domains dealing with the defence of digital assets and preservation of data, covers the protection of computing systems that process data as well as safeguards to human resources and material assets that manage the computing environment where data is processed. It also involves the design, development, implementation and maintenance of various policies, frameworks and strategies that guide the protection of data against unauthorised access and illegal modifications.

Respective domains of cybersecurity focus on specific areas of data and system protection including web application security [4] [5], operations security, telecommunications security, cloud security, software security, network security [3], database security [6] [7] [8], and lately home-automation security, IoT security [9] [10] [11], big data security [12] [13], etc. Although the nomenclature used across cybersecurity domains can be quite descriptive, each domain presents a unique set of

potential breaches with peculiarities and exclusivity, for example:

- web application security focuses on the protection of online applications and web-based resources from misuse and corruption of data,
- network security ensures that connectivity systems and transmission channels are safe and adequate for secure exchange of data,
- database security guarantees the protection of corporate data stored in local and remote digital repositories against unauthorized access, illegal modification and other forms of cyber breaches.

Cyber breaches and exploits occur everywhere on the cyberspace so long as humans continue to rely on technology to interact with the environment, rather inevitably. Most cyber breaches [14] [15] associated with unauthorized data manipulation or denial of service occur using a malicious software (malware) as an accessory. A malicious software is operationally designed with malicious intents including to cause undesirable effects [16], privacy infringements, damage to system or other security breaches. Depending on whether active or passive [17] consequences are triggered, a high impact breach can potentially lead to a total collapse of the entire security architecture through various propagation malwares particularly viruses and ransomware.

III. THE GROWTH IN CYBERATTACKS INCIDENTS

Credit card thefts have made daily headlines in major cities around the world, while spear phishing email scams are on the increase. Widespread virus attacks [18], [19] have continued to infect porous systems and networks with devastating consequences. Also not spared are the stand-alone Supervisory Control and Data Acquisition (SCADA) systems [20], [21], [22], [23] which are the Industrial Control System (ICS) [24] facilities used for remote monitoring of a variety of stand-alone industrial processes including wind turbines, nuclear plants, rail systems, power utilities, refineries, water flow, dams, industrial processes, and air/water pollution; they are also targets of cyberattacks. Three high profile cyberattacks have been reviewed below to buttress the necessity for an effective digital forensic culture in organizations across the globe.

A. Stuxnet Computer Virus Attack

In January 2010, the Iranian nuclear programme was hit by the Stuxnet computer virus [25] a sophisticated cyber weapon which disabled about 96% of Iran's nuclear facility's capacity. According to the Lloyds "Business Blackout" report, the Stuxnet computer virus caused an estimated financial damage of between about US$243 Billion in immediate and tangential economic loss, up to US$1 Trillion [26]. Stuxnet became the first known computer virus to disable a stand-alone physical equipment, the Iran's uranium enrichment facility at Natanz. Although it was sophisticated in nature, its scope was limited due to prompt isolation [27] in line with digital forensic ethics. It was widely speculated that Stuxnet was a targeted cyberwarfare against Iran as the country recorded 58.85% [25] of all infected systems globally.

B. WannaCry Ransomware Attack

In May 2017, the WannaCry ransomware capitalized on a vulnerability in the structure of Microsoft Windows operating systems [28] and attacked more than 200,000 computer systems in over 150 countries with majority of its UK victims falling within the healthcare sector. As a typical ransomware it prevented users from accessing infected systems and files by blocking login capabilities and encrypting files, while demanding that a ransom be paid [29] within a very tight deadline. Unfortunately in most ransomware cases, ransom payment does not guarantee instant release of encrypted files [30], neither does release of decrypted files assure that malware has been totally removed from the infected system; WannaCry was not any different. The four most affected countries were Russia, Ukraine, India and Taiwan [31] [32], resulting in an estimated global revenue loss of about US$4 billion with the UK's National Health Service (NHS) alone losing over US$100 million [33] [34]. WannaCry crippled many business operations, causing fear and panic. The ransomware caused leak of confidential data belonging to individuals and corporate organizations, led to privacy-related litigations, pushed many businesses into liquidation, and created massive unemployment.

C. NotPetya Ransomware Attack

In June 2017 the NotPetya crypto ransomware [35], [36] surfaced in Ukraine, hitting the Ukrainian nuclear power plant in Chernobyl near the city of Pripyat. Soon the malware spread rapidly to about 64 countries, including Belgium, Brazil, Germany, Russia, India, and the United States, exploiting the same Windows SMBv1 vulnerability as its predecessor WannaCry Ransomware and used the same EternalBlue Exploit payload [35]. It also utilized the Advanced Encryption Standard (AES) 128-bit to encrypt information [37] in the infected computer. Beyond modifying the infected system's Master Boot Record (MBR) causing it to crash, it also demanded a ransom of about US$300 in bitcoin from its victims in exchange to obtaining the supposed decryption code [35] [38].

It was later proven that NotPetya functioned more as a destructive wiper-like tool rather than an actual ransomware [39]. Critical systems belonging to organizations, airports, banks, government departments, retail, and power facilities in the affected countries were crippled. The advertising

giant WPP and the Pharmaceutical Lab Merck were said to have suffered losses exceeding US$300 Million, and had to rebuild entire infrastructure, including about 4,000 new servers, 45,000 new computers, and 2,500 new applications [40]. FedEx the courier giant also recorded huge losses in the wake of NotPetya attack [41]. Some French companies were equally impacted including Saint-Gobain Manufacturing Company and the state-owned railway company SNCF [42] with combined losses in excess of €220 Million. Some of the organizations undertook massive manpower cuts as a major part of their recovery strategy. Ultimately the primary and ancillary losses to the digital economy were significant and the harm to critical services and infrastructures took months to recover from [40].

D. Unreported Cyber Incidents

Unlike the Stuxnet, WannaCry and NotPetya cyberattack incidents, many unreported cases of cyber breaches of huge magnitude befall organizations on a frequent basis with devastating impacts, leading to far-reaching recovery measures and corporate response decisions. Reasons for unreported cyberattacks include apprehension over possible client backlash, deliberate aversion of fines and penalties, fear of culpability by data security regulatory authorities, etc. Unreported cases jeopardize response efforts by making adequate mitigation plans grossly uncertain.

Since cybersecurity deals with all the measures and techniques required to prevent, detect and respond to cyber breaches; incident response therefore forms an indispensable component of everyday digital protection. Unreported cyber breaches frustrate effective response actions that could ordinarily aid in determining, reproducing and analysing what events have occurred within a system or network, including the extent of exposures of sensitive data [43].

IV. OVERVIEW OF DIGITAL FORENSICS

Digital forensics, also referred to as computer forensics is the application of scientific methods and techniques to recover data from electronic and digital media [44]. Since total eradication of cyberattacks is not feasible, it is very important to deploy measures to detect cyber breaches where complete prevention is unrealistic. Digital forensics bridges that gap between cyberattack *prevention* and *response* procedures by aligning with the universal steps for carrying out the standard incident response namely preparation, identification, containment, eradication, recovery and lessons learnt. Computer forensics uses computer investigation and analysis techniques to collect evidence regarding what may have happened on a computer in a manner that qualifies the evidence to be admissible in a court of law [1]. Essentially the digital forensics process involves collection, preservation, analysis and presentation of evidence from digital sources [45]. Each of the standard steps involved in the digital forensic process is briefly described below.

A. Digital Forensic Processes

A1. Collection: Data is required to carry out a forensic exercise and is mostly obtained through a collection process. The *collection* is the step of identifying, labelling, recording, and acquiring data from sources identified as containing possible relevant digital evidence, while following procedures that preserve the integrity of the data and maintain a credible chain of custody. The data collection process is essential to the trustworthiness of the outcome of the entire process and usually follows standard mechanisms to check for exactness and to ensure that the primary data being used for the forensic investigation is not subjected to unethical modifications that could question its integrity.

A2. Examination: The data so collected requires proper examination and close attention. The *examination* phase deals with forensically processing collected data using a combination of automated and manual methods. During examination, data of interest is assessed and extracted methodically while preserving its integrity throughout the entire process. Examination of data of interest includes looking for deletion history, abnormal login sequence, irregular file operations, unconventional file naming and extensions, exceptional data traffic statistics, unidentifiable user accounts, etc. The focus of the examination stage is simply to look out for events of interest showing anomalies, variances, deviations and other signs of abnormal occurrences that could indicate a pattern or profile of a cyber breach. Under proper examination, these signs of abnormal and irregular occurrences would essentially appear as patterns and the examination phase produces a documentation of the patterns in addition to the operations and actions carried out.

A3. Analysis: After examining data of interest, a detailed scrutiny follows next. The *analysis* phase focuses on using legally justifiable methods and techniques to scrutinize or analyse the results of the examination, in order to derive useful trends and information that addresses the objectives of performing the collection and examination in the first place. The analysis phase interprets the examination process, deduces an explanation and infers credible intelligence based on methodical observation of the trends. Essentially the analysis phase is used to derive a meaning through the examination of the collected data.

A4. Reporting: At the end of a proper analysis, the *reporting* stage generates the results and outcome of the analysis, including a clear description of the methods adopted and actions carried out. Reporting also provides

detailed justification explaining choice of tools and procedures adopted; and determines any other follow-up action(s) that may be required including lessons learnt (e.g. forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls, etc). To forestall future occurrence, the reporting phase includes recommendations for system improvement covering policies, procedures, tools, and other identified areas that could strengthen future forensic tasks.

B. Sources of Digital Evidence

With today's proliferation of computing devices, software applications and web resources, there are several potential sources of digital evidence around which data collection can take place for forensic purposes. Although sources can vary from scenario to scenario, they all have one thing in common: they present the foundation upon which data examination and analysis can take place. A partial listing of sources of digital evidence includes electronic files, operating systems, storage media (CDs, removable/flash drives, cloud, etc), network traffic statistics, software applications, memory modules, Hard Disk Drives (HDD), email trail, supercomputers, servers, event logs files, distributed client-server networks, websites, cookies, application cache, laptops, handheld devices, smart phones, digital cameras, Local and Wide Area Network (LANs and WANs), databases, etc. Each of these sources presents peculiar avenue to extract huge evidence that can support the entire forensic process under strict chain of custody.

C. Applications of Digital Forensics

Since computer forensics involves recovery and investigation of materials found in digital devices, it is applied in all circumstances where the inquiry involves computing assets, software applications, web facilities, data processing and transmission systems, as well as other sources of digital evidence. Computer forensics therefore finds application in the following areas:

C1. Crime Investigation and Law Enforcement: Digital forensics is applied in the tracking, recovery and reconstruction of suspected criminal's travel history, internet transactions, GPS location and mobility, phone conversations and overall digital footprints in order to produce a detailed report containing reliable evidence of either guilt or exoneration. The forensics report is usually admissible in a court of law, provided that there is a proof that credible chain of custody has been followed throughout the data collection, examination, analysis and reporting steps.

C2. Audit of Computer Violations: It is also applied in computer-based internal policy violations to provide a methodical audit of systems usage with a focus on identifying abnormal operations in software, electronic systems, and other digital infrastructure in line with existing ICT policies.

C3. Investigation of Banking and Related Frauds: It finds usefulness in computer-based banking and other related financial frauds focussing on collection and analysis of a subject's banking and eCommerce records for possible clues that could lead to evidence of scam.

C4. Cyberattack Investigations: Digital forensics facilitates investigation of corporate cyberattack incidents involving virus and ransomware attack, denial of service, website session high-jacking and many more forms of cyber-criminalities. Application of digital forensics in the investigation of cyberattacks focuses on the systematic reconstruction of incidents by gathering potential evidences from numerous internal and external sources including a review of computer configurations, appraisal of network topologies, scrutiny of login credentials, audit of previous log files, confirmation of status of antivirus software, review of the effectiveness of Intrusion Detection and Prevention Systems (IDS and IPS), insider collusion, social engineering violations etc. Additionally, it helps to find out the root cause and impacts of incidents involving electronic data recovered from local or remote digital assets.

C5. Computer Helpdesk: Computer forensics supports technical troubleshooting of operational computing problems, giving system administrators the tools to perform password reset, CCTV review, backend file recovery, biometric access report audit, recovery from accidental system damage [43], incident response, etc.

Irrespective of area of application, digital forensics follows a universal standard procedure consisting of data collection, examination, analysis, and reporting under a strict chain of custody. The end product of digital forensics is usually a systematically documented evidence derived from digital sources for addressing disputes, inquiries and other issues involving storage devices, data communication systems, software applications, and online resources.

V. CHALLENGES TO EFFECTIVE DIGITAL FORENSICS

The benefits of digital forensics [46] in sanitizing the cyberspace cut across multiple domains of human interaction with the environment, yet its popularity is not at par with its practical applications in many spheres. The reasons for the low embrace of digital forensics are identified as follows:

A. Poor Awareness

In some organizations, the seeming lack of awareness of global standards and best practices in cybersecurity especially where corporate policies are required to direct action, is a major drawback to carrying out a successful forensic exercise. Poor awareness of basic incident response practices leads to ignorance of the consequences of digital forensics resulting in varying degrees of impacts when cyber breaches occur. E.g. employees who are unaware of the consequences of reusing old passwords run the risk of exposing critical servers to password hacking attacks resulting in avoidable identity theft and significant loss of corporate data. Furthermore, where basic understanding of digital forensics is lacking, it is difficult to detect when critical system files have been modified in an unauthorized manner e.g. by a virus, or to recognize when data storage thresholds have been exceeded in a data backup system. Unfortunately, in all these scenarios, only a total system failure or huge data loss would ignite reactive actions leading to disruption of normal operations, scandal, and possible loss of revenue, in addition to corporate reputational damage.

B. Denial Syndrome

A lot of organizations are in denial over the reality and scope of cybercrimes and this gives such organizations a false sense of confidence to relax their security approaches leading to heavy consequences. A corporate attitude of denial also pushes the organization to compromise on its security investment, often resulting to a reactive rather than proactive cybersecurity strategy.

C. Defective and Unsupportive Policies

An organization's adopted ICT strategy is expected to be total in scope in the sense that it should cover every aspect of the organization's digital operation. A selective approach to ICT strategy, comprising only of basic components often leaves exploitable loopholes that place the organization at great risk of future targeted cyberattacks. All organizational policies that fail to recognize and make provisions for future forensic needs run the risk of being taken unawares by sophisticated cyber threats particularly the Advanced Persistent Threat (APT) [47] [48], a family of exploits which tracks digital assets in target organization consistently over a long period of time varying from 1 month to 28 months or more, giving the threat enough time to study and adapt to the security measures [49] of the environment and keeping it undetected by the target's weak security controls.

D. Visionlessness

Lack of a clear organization vision as it relates to cybersecurity is partly responsible for the cluelessness exhibited by some organizations in the face of a cyberattack especially during wide-scale or global cyber breach incidents such as the 2010 Stuxnet computer virus, and the 2017 WannaCry ransomware and NotPetya episodes. Making cybersecurity an organizational concern should ordinarily be derived from the overall corporate objectives, mission statement and vision. Where the vision is lacking, weak or not well defined based on the quality of corporate leadership, vital structures of corporate management such as ICT strategies and cybersecurity policies become sources of threat, worry and potential targets.

VI. CONCLUSION

As the popularity and use of digital technologies gain more grounds, the inevitability of cybersecurity incidents becomes more and more obvious given that the advancement of Information and Communications Technologies (ICT) opens fresh avenues for cybercriminals [2]. This justifies the need for effective digital forensics involving the identification, collection, preservation, examination, and analysis of digital information. Digital forensics has shown to be a vital tool to responding to cybersecurity incidents procedurally.

This paper has reviewed the procedural steps of digital forensics alongside the many challenges faced by organizations in performing digital forensics. Poor capacity and inefficient ICT policies have been identified as major barriers, resulting in organizational cluelessness in the face of high profile cyberattacks. It is therefore hoped that the review made in this paper will stimulate the consciousness of organizations to identify cybersecurity pitfalls and to surmount the challenges, phobia and apathy against their digital forensic components.

ACKNOWLEDGMENT

Kenneth Okereafor thanks the National Health Insurance Scheme (NHIS), Nigeria; the Computer Forensics Institute, Nigeria (CFIN); and the Mohamed El Bachir El Ibrahimi University of Bordj Bou Arreridj, Algeria for supporting this work.

Conflict of Interest: None declared.

About the Authors

Kenneth Okereafor is Deputy General Manager and a United Nations trained Cybersecurity and Biometric expert with over two decades of Cybersecurity experience and special skills in managing and teaching Cyber Threat Intelligence & Mitigation Technologies in industry,

government, and academia. He is a member of the International Organization for Standardization's Technical Committee on Health Informatics (ISO-TC-215), and he chairs the ISO's Security and Privacy Working Group-4 in Nigeria where he supports the development and adoption of Cybersecurity standards for Nigeria's digital health ecosystem. He holds a PhD in Cybersecurity & Biometrics from Azteca University, Mexico; and has research interests in, and publications on, Cybersecurity Incident Response, Multi-biometric Liveness Detection, Electronic Health Security, Telemedicine, Automation Management, and Digital Identities.

Rania Djehaiche is a PhD student in Electronics and Telecommunications Systems at the Mohamed El Bachir El Ibrahimi University of Bordj Bou Arreridj, Algeria. She has developed mobile applications in transport technology, electronic health, and home automation, and has research interests in Network Security, Mobile Applications, M2M Communications, and Internet of Things.

REFERENCES

[1] R. Bassett, L. Bass and P. O'Brien, "Computer Forensics: An Essential Ingredient for Cyber Security," Journal of Information Science and Technology, vol. 3, no. 1, pp. 22 - 32, 2006.

[2] "Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria," Internation Journal of Cybersecurity Intelligence and Cybercrime, vol. 2, no. 1, pp. 56 - 63, 2019.

[3] M. S. Gaigole and M. A. Kalyankar, "The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms," International Journal of Computer Science and Mobile Computing, vol. 4, no. 5, pp. 728-735, 2015.

[4] S. Kumar, R. Mahajan, N. Kumar and S. K. Khatri, "A study on web application security and detecting security vulnerabilities," in 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, 2017.

[5] S. Rafique, M. Humayun, Z. Gul, A. Abbas and H. Javed, "Systematic Review of Web Application Security Vulnerabilities Detection Methods," Journal of Computer and Communications, vol. 3, no. 9, pp. 28-40 (DOI: 10.4236/jcc.2015.39004), 2016.

[6] Sukhdev Singh Ghuman, "Database Security," International Journal of Computer Science and Mobile Computing, vol. 2, no. 2, pp. 102-105, 2013.

[7] I. Basharat and F. Azam, "Database Security and Encryption: A Survey Study," International Journal of Computer Applications, vol. 47, no. 2012, pp. 28-34, 2012.

[8] T. R. Gaikwad and A. B. Raut, "A Review on Database Security," International Journal of Science and Research (IJSR), vol. 3, no. 4, pp. 372-374, 2014.

[9] M. A. Iqbal, O. G. Olaleye and M. A. Bayoum, "A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches," Global Journal of Computer Science and Technology: E Network, Web & Security, vol. 16, no. 7, pp. 1-10, 2016.

[10] T. Siddiqui and S. S. B. Alazzawi, "Security of Internet of Things," International Journal of Applied Science - Research and Review, vol. 5, no. 2:8, pp. 1-3, 2018.

[11] R. S. M. Joshitta and L. Arockiam, "Security in IoT Environment: A Survey," International Journal of Information Technology & Mechanical Engineering - (IJITME), vol. 2, no. 7, pp. 1-8, 2016.

[12] R. Toshniwal, K. G. Dastidar and A. Nath , "Big Data Security Issues and Challenges," International Journal of Innovative Research in Advanced Engineering (IJIRAE) , vol. 2, no. 2, pp. 15-20, 2015.

[13] Gang Zeng, "Big Data and Information Security," International Journal of Computational Engineering Research (IJCER), vol. 5, no. 6, pp. 17-21, 2015.

[14] A. Juma'h and Y. Alnsour, "The Effect of Data Breaches on Company Performance," International Journal of Accounting and Information Management, vol. 28, no. 2, 2020.

[15] L. A. Gordon, M. P. Loeb and L. Zhou, "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?," Journal of Computer Security, vol. 19, no. 1, pp. 33-56, 2011.

[16] K. U. Okereafor and O. Adebola, "TACKLING THE CYBERSECURITY IMPACTS OF THE CORONAVIRUS OUTBREAK AS A CHALLENGE TO INTERNET SAFETY," International Journal in IT and Engineering (IJITE), vol. 8, no. 2, pp. 1-14, 2020.

[17] A. S. Kumar, N. R. S. Kumar and A. Das, "Monitoring Cyber Attacks and Analysis of Breaches," International Journal of Recent Technology and Engineering (IJRTE), vol. 7, no. 5S3, pp. 222-225, 2019.

[18] M. Joshi and B. V. Patil, "Computer Virus: Their Problems & Major at-tacks in Real Life," International Journal of P2P Network Trends and Technology (IJPTT), vol. 3, no. 4, pp. 206-209, 2012.

[19] A. Ray and A. Nath, "Introduction to Malware and Malware Analysis: A brief overview," International Journal of Advance Research in Computer Science and Management Studies, vol. 4, no. 10, pp. 22-30, 2016.

[20] Shubhada S. Warke, "A Review on Applications of Supervisory Control and Data Acquisition (SCADA) Systems," Journal of Emerging Technologies and Innovative Research, vol. 3, no. 8, pp. 73-74, 2016.

[21] S. Hopkins and E. Kalaimannan, "Towards establishing a security engineered SCADA framework," Journal of Cybersecurity Technology, vol. 3, no. 1, pp. 47-59, 2019.

[22] P. W. Singer, "Stuxnet and its hidden lessons on the ethics of cyberweapons," Case Western Reserve Journal of International Law, vol. 47, no. 1, pp. 79-86, 2015.

[23] S. Collins and S. McCombie, "Stuxnet: the emergence of a new cyber weapon and its implications," Journal of Policing, Intelligence and Counter Terrorism, vol. 7, no. 1, pp. 80-91, 2012.

[24] Hindawi Publishing Corporation, "Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2012, no. 268478, pp. 1-10, 2012.

[25] Siddharth Prakash Rao, "Stuxnet , A new Cyberwar weapon : Analysis from a technical point of view," Aalto University, 2014.

[26] T. Maynard and N. Beecroft , "The insurance implications of a cyber attack on the US power grid," University of Cambridge Judge Business School, Centre for Risk Studies, UK, 2015.

[27] James Moos, "Cyber Forensics in a Post Stuxnet World," ITNOW, vol. 57, no. 4, pp. 32-32, 2015.

[28] M. Mago and F. F. Madyira, "Ransomware Software: Case of WannaCry," International Research Journal of Advanced Engineering and Science, vol. 3, no. 1, pp. 258-261, 2018.

[29] M. Akbanov, V. G. Vassilakis and M. D. Logothetis, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms," Journal of Telecomminucations and Information Technology, vol. 1, no. 2019, pp. 113-124, 2019.

[30] S. K. Sahi, "A Study of WannaCry Ransomware Attack," International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), vol. 4, no. 9, pp. 5-7, 2017.

[31] Financial Times, "Global alert to prepare for fresh cyber attacks," 14 May 2017. [Online]. Available: https://www.ft.com/content/bb4dda38-389f-11e7-821a-6027b8a20f23. [Accessed 04 April 2020].

[32] The One Brief, "4 Lessons And 7 Questions From The WannaCry Ransomware Attack," June 2017. [Online]. Available:

https://theonebrief.com/lessons-learned-questions-posed-by-wannacry-ransomware-attack/. [Accessed April 2020].

[33] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi and P. Aylin , "A retrospective impact analysis of the WannaCry cyberattack on the NHS," NPJ Digital Medicine, vol. 2, no. 98, pp. https://doi.org/10.1038/s41746-019-0161-6, 2019.

[34] CHRIS BRUNAU, "Ransomware News: WannaCry Attack Costs NHS Over $100 Million," 18 October 2018. [Online]. Available: https://www.datto.com/blog/ransomware-news-wannacry-attack-costs-nhs-over-100-million. [Accessed April 2020].

[35] CERT-MU , THE PETYA CYBER ATTACK, June 2017 .

[36] E. Kovacs, "U.S., Canada, Australia Attribute NotPetya Attack to Russia," SECURITYWEEK, 16 2 2018. [Online]. Available: https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia. [Accessed 23 4 2020].

[37] Reyner Aranta Lika, "NotPetya: Cyber Attack Prevention through Awareness via Gamification," IEEE, 2018.

[38] G. KALLENBORN, "Six questions pour tout comprendre sur la cyberattaque mondiale NotPetya," 28/06/2017.

[39] LogRhythm Labs, "NOTPETYA TECHNICAL ANALYSIS," LogRhythm Labs, 2017.

[40] M. Hathaway, MANAGING NATIONAL-CYBER RISK, 2018.

[41] Z. Shoorbajee, "FedEx attributes $300 million loss to NotPetya ransomware attack," Cyberscoop, [Online]. Available: https://www.cyberscoop.com/fedex-attributes-300-million-loss-notpetya-attack/. [Accessed 23 4 2020].

[42] HISCOX, "Les 10 cyberattaques qui ont marqué l'année 2017," le 21 décembre 2017 .

[43] K. Kent, S. Chevalier, T. Grance and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," National Institute of Standards and Technology (NIST) Special Publication 800-86, Maryland, 2006.

[44] W. S. Tonye, "Cyber Forensic and Data Collection Challenges in Nigeria," Global Journal of Computer Science and Technology: G Interdisciplinary, vol. 18, no. 3, pp. 1 - 5, 2018.

[45] F. N. Dezfoli, A. Dehghantanha, R. Mahmoud, N. F. Binti, M. Sani and F. Daryabar, "Digital Forensic Trends and Future," International Journal of Cyber-Security and Digital Forensics (IJCSDF) , vol. 2, no. 2, pp. 48 - 76, 2014.

[46] Whyte Stella Tonye, "Cyber Forensic and Data Collection Challenges in Nigeria," Global Journal of Computer Science and Technology: G Interdisciplinary, vol. 18, no. 3, 2018.

[47] M. Bere, F. Bhunu-Shava, A. Gamundani and . I. Nhamu, "How Advanced Persistent Threats Exploit Humans," International Journal of Computer Science Issues (IJCSI), vol. 12, no. 6, pp. 170-174, 2015.

[48] M. A. SIDDIQI, A. A. MUGHERI and A. OAD , "Advanced Persistent Threats Defense Techniques: A Review," Pakistan Journal of Computer and Information Systems, vol. 2, no. 2, 2017.

[49] M. A. Siddiqi and N. Ghani, "Critical Analysis on Advanced Persistent Threats," International Journal of Computer Applications (0975 – 8887), vol. 141, no. 13, pp. 46-50, 2016.