International Conference on Information and Communication Technology and Its Applications (ICTA 2016)

Federal University of Technology, Minna, Nigeria

November 28 – 30, 2016

Cybercafés in Nigeria: Curse to the Internet?

Oluwafemi Osho[1] and Solomon A. Adepoju[2]
[1]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria
[2]Department of Computer Science, Federal University of Technology, Minna, Nigeria
{[1]femi.osho, [2]solo.adepoju}@futminna.edu.ng

***Abstract*—Cybercafés have grown in popularity since their emergence. This popularity is predicated on their capacity to offer relatively cheap, immediate and convenient access to the internet. Regrettably, cybercriminals, and even terrorists, have been exploiting them to perpetrate their unwholesome activities. This study evaluates the security posture of cybercafés in Nigeria. Using a combination of survey and observation, a total of ninety nine cybercafés, covering nine states, in five of the six geopolitical zones of the country, were covered. The findings suggest that most of the cybercafés have adequate capacity to prevent unauthorized access to their network, and the exploitation of the network to remotely perpetrate cybercrimes. However, within the physical confines of most of the internet cafes, cybercrimes are and could easily be carried out, and their networks exploited for other unethical uses of the internet. Security needs to be given more attention than it currently enjoys in the management of cybercafés by managers. On the other hand, government must ensure the regulation of the activities of the sector.**

Keywords-cybercafé; internet café; Nigeria; management, security; cybercrime

I. INTRODUCTION

Cybercafés, also known as internet cafes, are public places that provide commercial – paid or metered – access to the internet [1]–[5]. However, it is not unlikely to see other services including selling refreshments [2] being rendered. This is common in advanced countries where cybercafés offer not only internet access, but also beverages [1], [6] or food and other types of drinks [7]. Depending on the business model, types of cybercafé include traditional internet cafés, gaming, self-serve internet cafés, standalone internet kiosks, information and advertising-based kiosks, and wireless hotspots [3].

Since the emergence of internet cafes, they have grown in popularity. In Africa and most developing countries, internet access is largely through cybercafés [7]–[10]. A survey by [11] reveals that for up to 25% of students in Turkey cybercafé was the dominant place for accessing the internet. Li, Zhang, Lu, Zhang, & Wang [12] found out that while internet café was the 2nd most commonly used place for internet access among elementary and middle school students in China, it was the most used among those who were found to be internet addict. Internet cafes provide many advantages. They offer convenient [6], immediate, and relatively cheap access to internet. They have even been proposed as an essential component for social security [8].

However, similar to other information technology (IT) components, cybercafés are prone to abuse. Like all networks on the internet, their networks are exposed to security risks. In a study by [7], 80% of cybercafé operators identified malware, while 20% identified the users, as their biggest threat. A cybercafé network has to contend with risks from those within and outside the network. There are users whose intent is to exploit the systems in the café for unethical purposes. When appropriate security mechanisms are not in place, the network of such cybercafé could be used to perpetrate cybercrime, including installing a keylogger [13], spamming, fraud, hacking, to mention but few. On the other hand, there are malicious internet users, outside the network of the café, who intrude into vulnerable networks. There are many potential attacks that could be launched. One of these is remotely infecting vulnerable systems with malware that automatically adds them to a botnet operated by the attacker. The bots are used for criminal activities. Even terrorists use cybercafés [14]. The internet has become indispensable to terrorists for planning and coordinating their attacks [15]. Internet café offers a platform for the terrorist to veil their identities.

Apart from users who have malicious intents for using the café, another category of user that needs proper monitoring is children. Online attacks that target children are continually on the increase. Cybercafés have been discovered to be locations for different adolescent crimes [6] and social excesses [16].

Most internet café users have little or no knowledge of the security risks they are exposed to and how to mitigate the risks [2]. It therefore lies on the managers of the cybercafés to provide adequate security. To achieve the needed security, there are requirements that must be provided. Some of these include surveillance/security system, legal software [17], firewalls, antivirus software, making regular backup of data, and up-to-date updating of applications [1].

However, studies have shown that security is often not given due attention. Cybercafés engage staff who are unskilled, with little or no IT knowledge [18], [19].While many of the cafes have anti-malware applications, few regularly update them [2]. And in most cybercafés, articulated policies guiding activities of users are often not available [7]. In cases where there are they are often not comprehensive [2].

In Nigeria, internet cafes have contributed tremendously to digital inclusion. Since the deregulation of the telecommunication sector in 1999 [20], and the introduction of the Global System for Mobile (GSM) communication services in 2001 [21], [22], the adoption rate of mobile technology in the country has proliferated. This, unfortunately, has resulted in cybercafés losing their place as the primary platform used for accessing the internet. One of the effects is the demise of many of these cybercafés in the country [18]. This sharp drop in number and patronage notwithstanding, because not all users can afford internet access through mobile and other personal devices, existing and functioning cybercafés have continued to enjoy some measure of patronage. As is the case in other parts of the world, they are used for their traditional purposes of researching, sending and accessing emails, communicating, job search and application, to mention but few. In some academic environments cybercafés are the primary instrument for accessing the internet [7], [23], [24].

Regrettably, while internet cafes have improved the adoption of IT in the country, they have also helped to multiply its abuses. Teenagers use cybercafés as havens for accessing pornographic materials, scammers utilize them for their criminal activities, sending out scam emails [25]–[27]. Many cybercafés have been sealed off by security agencies due to the perpetration of cybercrimes using the café network [7]. And in some cases, the activities of criminal have led to their outright shutting down [18].

In the light of the foregoing realities, we pose some critical questions: Do internet cafes in Nigeria have the capacity to prevent unauthorized access to their network? Do they have the capacity to prevent their systems from being used locally or remotely to perpetrate cybercrimes? Are they likely locations for other unethical uses of the internet? This paper investigates management of cybercafés in Nigeria, with emphasis on security.

This study is significant in at least two ways. First, it exposes the security state of internet cafes in Nigeria. While there are laws that tend to relate indirectly to different activities that are associated with cybercafés in Nigeria, there are currently no known comprehensive guidelines on the establishment and operations of cybercafé. This study, secondly, would assist relevant policy and regulatory agencies of government in the development of regulatory framework for the operations and management of cybercafés in Nigeria.

The rest of the paper is sectionalized as follows: section two presents a summary of studies related to internet cafes. In section three, the methodology adopted is described. The findings are presented in section four. Subsequently, these findings are discussed is section five. The limitations of the study are highlighted and suggestions for further works given in section six. Lastly, in section seven, the study is concluded, and some recommendations suggested.

II. Related Works

Many literatures have focused on different aspects of internet café, including their management, use, effect of usage, and security.

On the management of cybercafés, [4] concentrated on the management of infrastructures, [7] on operational issues, controversies, and challenges, while discussion of management software was the focus of [28], [29].The objectives of other studies in the domain of cybercafé management include management of e-waste by cybercafés [30], factors that affect provision of quality services [31], evaluation of technical efficiency of internet access methods used in the cafes [32], and identification of factors responsible for closure of cybercafés [33].

Studies on cybercafé usage majorly center on rate, purposes and effects of, and factors that affect use. Very few of the studies have explored internet café usage effects. One of these is the work of [16] which investigated the effect of usage on cigarette smoking and alcohol use among Chinese adolescents and youth. Another, by [34], entails a survey on the consequences of internet café usage on students' social capital. And in [35], the effects of playing computer games in internet cafes on the flow experiences of adolescents was investigated.

On the other hand, studies on rate and purposes of usage have considered different countries. These include China [36], Indonesia [37], Malaysia [38], Nigeria [39], [40], Pakistan [10], Philippines [41], Tanzania [42], Tanzania and Indonesia [43], and Turkey [44]. On factors that affect use, [45] proposed a framework with perceived trust as antecedent of internet café continuance intention.

The issue of security of internet cafes is very crucial to their survival. It is therefore not surprising that this area has attracted the attention of some authors. Specifically, some of the studies discussed security issues related to cybercafé use and operation, highlighting sources and types of security risks, and proffering countermeasures [1], [2].The focus of [8] was the development of cybercafé security policy in Nigeria. This, the author argued, can enhance social security. Consequently, it was recommended that such policy should be integrated into the National Information Policy. Another similar study by [46] centered on the development of regulation of internet cafes in China. However, one study [47] departed from the traditional notion of the security of cybercafé being solely dependent on technological infrastructure. They proposed security measures that, in addition to technological mechanism, are also based on social and soft components of management. Other aspects of security explored in different literatures include malware detection and prevention [48], [49], security evaluation [50], cybercafés and cybercrimes [19], [51]–[54], and cybercafé and terrorism [14].

As far as research related to cybercafé is concerned security has not been given due attention [8]. Very few studies have centered on the state of security in internet cafes using empirical data. One of these is the study by [18]. The authors investigated physical and security issues faced by managers of cybercafés in Ibadan, and measures to tackle the challenges. They however recommended similar research across the country.

Our study examines security measures provided by internet café managers to prevent unauthorized access to their network, mitigate perpetration of cybercrimes via and other unethical uses of their networks.

III. Methodology

To achieve the aim of this study, descriptive research was adopted. Two methods were employed to collate data: survey and observation. To collect data that were considerably representative of the country, the stratified random sampling method was used. Nigeria is composed of geopolitical zones, with each composed of states which are essentially homogeneous. Consequently, this formed the basis for stratification. For each stratum, random samples were selected from at least one of the component states. The objective was to cover at least a state in each of the six geopolitical zones of the country. A total of ninety nine internet cafes, located in nine states, in five of the zones (with the exception of North East) were covered in the survey. The survey was conducted within 2013 and 2014. Table I presents the composition of cybercafés by state and zone.

The survey questions were administered through questionnaires. Observation was used to ascertain the correctness of the data supplied by the managers/operators. The questionnaire sought information on the number of systems used for browsing and café attendant, availability of wireless access technology, those permitted to use the cybercafé, availability of introductory class for novice users, permissions, security measures, and managers' observations and experiences. The ninety nine questionnaires were returned, found to be valid, and thus used for analysis. To identify relationships among variables, we performed some statistical tests, including chi-square, t-test, Fisher's exact test, and Pearson's correlations. All tests were conducted at 95% confidence interval.

IV. Analysis

The findings, presented in Table II, revealed that majority of the cybercafés, 61.6% operate with no more than 10 computers. Only 13.1% have above 15 systems. Most of the cybercafés (71.7%) did not have more than 3 café attendants. A positive linear correlation was found to exist between number of systems used for browsing and café attendants (r = 0.426, p< 0.001). This, expectedly, implies that the higher the number of browse-able systems the more the number of café attendants employed by the owners.

TABLE I. Number of cybercafés by state and geographical region

Zone	State	Frequency	Percent
North Central	Abuja	14	14.1
North Central	kogi	10	10.1
North Central	Niger	6	6.1
North West	Kaduna	15	15.2
South East	Abia	5	5.1
South East	Enugu	9	9.1
South South	Cross River	13	13.1
South West	Ekiti	8	8.1
South West	Lagos	19	19.2
		99	100.0

Other characteristics considered in the study revealed that 97.0% of the internet cafes surveyed allow any individual to access the internet using their network, regardless of age; 62.6% provide access via wireless, in addition to wired, technology; and about half of the cybercafés, 50.5%, offer introductory classes for novice users who need assistance in using the internet. The results are presented in Table III. The practice of offering this class to novice users was significantly dependent on the number of café attendants (p = 0.015). On average, 39.96% of internet cafes with a maximum of 3 attendants offered introductory classes for novice users. Conversely, among those with a minimum of 4 operators, an average of 77.93% offered introductory classes.

TABLE II. Number of systems used for browsing and café attendants

	Frequency	Percent
Number of systems used for browsing		
1 - 5	18	18.2
6 - 10	43	43.4
11 - 15	25	25.3
Above 15	13	13.1
Total	99	100.0
Number of café attendants		
1	19	19.2
2	32	32.3
3	20	20.2
4	17	17.2
5	4	4.0
Above 5	7	7.1
Total	99	100.0

A. *Permissions*

Table III also reveals the some basic activities a customer is permitted by managers to undertake in the cybercafé. 78.8% of the cafes permit saving on their computer memory, 79.8% allowed customers to use their personal external memory drive to save. Most of the cafes equally permit the use of their systems to make payment online (87.9%) and download from the internet (86.9%).

Perhaps, to mitigate downloading of malicious and illegal software documents, more than half, precisely 51.2%, of the cafés that allow downloading required customers to obtain authorization before actually downloading.

In order to secure their networks and systems cybercafé managers provide security measures. From Table III, other findings revealed that more than three-quarter of (76.8%) and almost all the cafes (97.0%) provide firewall and antivirus software respectively. However, many of them do not provide regulatory policy and measures to monitor power users. Specifically, only slightly more than half of the cafes have policy displayed to regulate the activities of their customers (53.5%) and have developed measures to monitor customers with expert knowledge in the use of the internet (58.6%).

B. *Security Measures*

Providing regulatory policy to curtail user activities was found to significantly influence putting measures to monitor power users ($\chi2(1) = 6.127, p = 0.013$). Those who had regulatory policy in place were found to be less interested in monitoring power users. While 71.7% of internet cafes without regulatory policy had measures to monitor users in place, only 47.2% of those with policy did have measures. Only about one-quarter (25.3%) of the cafes provide both policy and measures. And far fewer cafés, 11.1% ($\chi^2(1) = 12.01,\ p = 0.001$), provide both in addition to offering introductory classes for novice users.

More crucial are the availability of regulatory policy and monitoring measures to internet cafes that permit customers to use the cafe network to make online payments, download, and store on system's memory and their memory drive. Less than one-quarter, 24.1%, of cafes which allowed their network to be used for online payment provided both regulatory policy and measures to monitor power users ($\chi2(1) = 6.656, p = 0.010$). Among the cafes that allowed customers to save on the café system memory and their personal memory devices, only 24.4% and 22.8% ($\chi2(1) = 8.711, p = 0.003$) respectively provided both. And for internet cafes which expectedly permitted downloading via their networks, only 22.1% provide both policy and measures ($\chi2(1) = 5.883, p = 0.015$).

TABLE III. OTHER CHARACTERISTICS, PERMISSIONS, SECURITY MEASURES, EXPERIENCES AND OBSERVATIONS

	Frequency	Percent
Other Characteristics		
Café open to Everyone	96	97.0
Use of wireless LAN	62	62.6
Introductory class for novice users	50	50.5
Permissions		
Save on computer memory	78	78.8
Save on customer's USB drive	79	79.8
Systems Used for Online Payment	87	87.9
Download	86	86.9
Security Measures		
Availability of firewall	76	76.8
Availability of anti-virus	96	97.0
Availability of regulatory policy	53	53.5
Measures to monitor power users	58	58.6
Experiences and observations		
Computers in café formatted in the last one year	80	80.8
Noticed a customer who loves using a particular system	76	76.8
Someone successfully tampered with administrative settings	52	52.5

TABLE IV. LENGTH OF PASSWORD

	Frequency	Percent
More than 8	58	58.6
Less than 8	40	40.4
No password	1	1.0
Total	99	100.0

Cybercafés naturally are expected to make use of passwords to manage access to the internet via their network. However, the associated security issues lie with the strength of the password. From our survey, depicted in Table IV, there are internet cafes that actually do not use passwords. 1.0% of the cafes fell into category. In contrast, 40.4% use passwords but less than 8 characters long, while the rest reported they used passwords with length more than 8. Fisher's exact test revealed an evidence of relationship between cafés using wireless LAN and length of password (p = 0.006). Only 30.6% of internet cafes using both wired and wireless technology for providing internet access either did not provide password mechanism for accessing their systems or used passwords that are less than 8 characters.

C. *Managers' Observations and Experiences*

From Table III, 80.8% of the cybercafés had had to format their systems at least once in the last one year. Almost half of the population, precisely 48.7%, as presented in Table V, had formatted either twice or thrice. Providing wireless technology for accessing the internet significantly influenced the likelihood of formatting systems ($\chi2(1) = 4.230, p = 0.04$). Findings revealed that while 70.3% of internet cafes that provided internet access via wired network only formatted their systems in the last one year, 87.1% of those with wireless network, in addition to wired network, have formatted theirs.

In most of the cybercafés (76.8%), there have been instances where a customer was noticed to always prefer the use of a particular system. On administrative settings being changed by customers, more than half (52.5%) of the cafés confessed they had experience that. The study found significant evidence of association between customer who loves using a particular system and administrative setting being tampered ($\chi2(1) = 8.398, p = 0.004$). The occurrence of a customer being noticed to prefer the use of a particular system increased the likelihood of administrative settings of systems being tampered with. Specifically, 60.5% of cybercafés that reported noticing a customer who loved using particular system, compared with only 26.1% among those who did not notice any, had experienced their administrative settings being changed.

TABLE V. NUMBER OF TIMES COMPUTERS HAD BEEN FORMATTED

	Frequency	Percent
Once	21	26.2
Twice	25	31.2
Thrice	22	17.5
Four times	7	8.8
Five times	5	6.2
Total	80	100.0

V. DISCUSSION

This study sought to evaluate the security state of internet cafes in Nigeria. Results of keen observation and extensive survey of ninety-nine internet cafes located in five of the six geopolitical zones of the country revealed that most internet cafes in Nigeria are small enterprises, open to everyone, deploy both wired and wireless network for accessing the internet, and provide introductory class for novice users.

The decision by managers of internet cafes to open their businesses to all categories of users for accessing the internet is evidently geared towards expanding their customer base, which in turn can be expected to improve patronage. However, this poses some inherent risks. One of these is that children can easily take advantage of it. If not properly monitored, many of them might exploit the cafes for purposes unapproved of by their parents.

Offering introductory classes for rookie internet users by most managers of internet cafes is commendable. Novice users often lack the requisite knowledge to use computer systems appropriately. They can subject systems to physical abuse, unauthorized adjustment of setting. Thus, having introductory classes can be seen as a proactive measure to forestall possible misuse. It can also be considered a marketing strategy capable of attracting new customers, as well as a measure to attract customer loyalty. Nevertheless, providing necessary capacity for conducting introductory class for this category of users would require increased cost of management of the cybercafés. One of the findings of the study confirmed this fact. On average, most cafes offering introductory classes tend to have higher number of café attendants, when compared with those which did not.

Most internet cafes in Nigeria considerably seem capable of preventing unauthorized access to their network. Hackers located within a certain range of a cybercafé could gain internet access through the café's network without authorization if the wireless network is not properly secured. One defence mechanism is to deploy a firewall. Hackers will often exploit weak defence system and weak passwords, amongst other things, to penetrate network systems. Our findings revealed that the availability of firewall in most of the cafes. Also, most of the internet cafes using both wired and wireless technology for providing internet access implemented passwords that were more than 8 characters.

Regarding the capacity of internet cafes to prevent their networks from being used to perpetrate cybercrimes, the study suggest that while most cafes can avert cybercriminals from using their system remotely, only very few have put necessary mechanisms in place to prevent perpetration of cybercrimes by a criminal within the physical confines of the internet cafe. To commit crime via a cafe network remotely, the café must be operating, either partially or completely, on a wireless network, and a cyber criminal would need to gain access remotely to the network. The capacity to prevent this by most cafes has already been identified in the study.

However, on the issue of cybercrime being perpetrated locally, the study finds significant evidence to suggest that in most of the internet cafes in Nigeria cybercrimes are and could easily be carried out. In most of the cafes, administrative settings on computer systems had been altered. It was more common among cafes where some customers accessed the internet using particular systems. This raises the question of what could be special about the preferred system. It is possible that a customer might have developed a preference for a particular system due to the functionality it provides. This is because, in many cybercafés, it is common to find one or more components on most of the computer systems not functioning properly. From observation, many of the cafés often buy used and low-graded computer monitor and peripherals. A second factor is the position within the café where the preferred system is located. The physical space occupied by some cafés are so inadequate that a customer, for instance, may have to sit so close to the entrance/exit, and consequently have to endure brushings by those coming into or going out of the café. Any customer would therefore prefer systems located in positions that offer the least inconvenience, Notwithstanding, it is not impossible that the reason a customer would insist on using only a particular computer in the internet cafe is simply for illegal activities that constitute cybercrime. Cybercriminals would tweak the settings on computer systems in the cafe to permit certain tools to facilitate their criminal intentions. To minimize such occurrence, as basic, irreducible requirements, policy regulating users' activities and measures to monitor some categories of users are crucial. One of the most common cybercrimes in Nigeria is the advance fee fraud. One form of this crime is geared towards stealing or cloning online transaction cards. Cybercriminals purchase and pay for goods online using these cards. The implication of this is that a cybercafé which permit their network to be used for making online payments without measures to monitor power users is prone to becoming a platform through which this kind of criminal activities would be performed. Equally vulnerable are those without regulatory policies. Unfortunately, most of the cafes that had regulatory policy in place were less interested in monitoring power users. Findings also revealed that most of those that allowed online payments via their network did not provide both regulatory policy and monitoring measures.

There are other unethical uses of the internet. These include viewing, downloading, uploading, and spreading of illegal contents and software, including pornographic materials, and malware. There are basic functions a customer typically would expect the systems and network of an internet café to provide. A cybercafé that does not allow customers to save their documents, download, or, use their platform to make online payments would displease many customers. For instance, how would a customer (or tourist) book a hotel if he cannot conduct payments? No doubt, these activities, in most cases, are fundamental to other activities performed in the café. However, they also pose some potential threats. Being able to use memory drives and download without restraint can aid accessing, uploading and spreading of illegal contents and software. Permitting a malicious customer to save on the hard disk of the system being used potentially makes the system, if proper security measures are not put in place, vulnerable to, for example, be used to store malicious programs. Being able to use external drives on systems in cybercafés exposes the entire network of the café to serious risks like malware attack. Other malicious software can be easily transmitted via these drives. Regrettably, our findings suggest that most of the internet cafes in Nigeria are potential locations for other unethical uses of the internet. Most of the internet cafes had had to format their systems within a space of one year, despite their use of antimalware. The percentage was higher for cafes that used wireless technology partially or fully. In each case, less than a quarter of the cafes which permitted customers to save on the cafe systems, their personal systems, and download, provided both regulatory policy and measures to monitor power users.

Our study corroborates previous findings, including [6], [26], [25], that have identified cybercafés as locations for perpetration of cybercrimes and other unethical internet uses. It also agrees with [7] who identified users as one of the biggest threats faced by cybercafé operators.

VI. LIMITATIONS AND FUTURE STUDIES

Our study relied primarily on self-reported data. It is thus subject to the validity of the measures. Secondly, we cannot confidently generalize the findings as outrightly representative of the entire country, since the six geopolitical zones were not covered. Future studies could consider a more representative approach.

It can be expected that the security posture of internet cafes would differ in the different states/zones. For instance, in Nigeria, while some states/zones are predominantly urban, others are rural. This dichotomy, and other factors, could influence the prevalence of cybercrimes, and consequently the level of security risk internet cafes in those states/zones. A comparative security evaluation of cybercafés by state/zones can be investigated.

Our current study does not evaluate child online safety in the internet cafe. Considering the increasing online attacks specifically aimed at young internet users, more empirical studies that assess their security while online in different access locations, including internet cafes, are required.

Much attention has not been given by researchers to regulation of internet cafes, especially in Nigeria. This is another critical aspect that requires urgent attention.

VII. Conclusion and recommendations

Activities of cybercriminals have been and remain detrimental to the survival of internet cafes in Nigeria. Unfortunately, while many of the cafes possess the capacity to prevent unauthorized access to their network, and forestall their networks from being used remotely to perpetrate cybercrimes, in many of them, cybercriminals engage in criminal activities, and other unethical internet activities take place with relative ease.

The findings of this study underscore the need for necessary interventions by relevant stakeholders, including managers of cybercafés and the government. Internet cafe managers need to be more proactive in their management. From a business perspective, this is essential for their survival. They need to put in place necessary security mechanisms to safeguard their networks from being exploited for unethical purposes. Deploying basic security tools and mechanisms, including firewalls, antivirus, and ensuring effective monitoring, whilst not violating customers' privacy, can go a long way to ensuring the nation's cybercafés are not comfort zones for hackers, spammers, and other cyber offenders. On the other hand, government needs to devote more interest in cybercafé operations in the country. As is obtainable in most sectors of the country, there is need for regulation of their activities.

Acknowledgement

We wish to acknowledge the following individuals who served as research assistants, assisting with collection of the survey data: Andrew Eyo, Christopher I. Onuoha, Eliab S. Ilemobayo, Godwin Abenege, Joel N. Ugwu, Sefiyat O. Ohida, and Temidayo H. Ajisola

References

[1] O. B. Adogbeji, "Computer Security in Cybercafes," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 18–29.

[2] L. A. Mohammed, "Cybercafe Systems Security," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 1–17.

[3] R. C. Hendrix, "A guide to starting an Internet Cafe Business," 2013.

[4] K. A. Sodiq, "Assessment of the Management of Information and Communication Technology (ICT) Infrastructure of Selected Cybercafes in Lagos State," in *Journal of Educational and Social Research*, vol. 2, no. 9, 2012, pp. 181–188.

[5] N. Rangaswamy, "Telecenters and Internet cafés: the case of ICTs in small businesses," *Asian J. Commun.*, vol. 18, no. 4, pp. 365–378, 2008.

[6] S. M. Mutula, "Cyber Security of Children: Implications for Sub-Saharan Africa," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 46–61.

[7] H. O. C. Otokunefor and H. K. Kari, "Issues, Controversies, and Problems of Cybercafés Located in a University Campus," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 62–83.

[8] S. C. A. Utulu, "Enhancing Social Security through Appropriate Cybercafé Security Policy in Nigeria," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 30–45.

[9] O. O. Bola and O. O. Ogunlade, "Accessibility and Utilization of Internet Service by Graduate Students in University of Lagos, Nigeria," *Eur. Res.*, vol. 25, no. 7, pp. 1092–1098, 2012.

[10] S. H. Batool and K. Mahmood, "Entertainment, communication or academic use? A survey of Internet cafe users in Lahore, Pakistan," *Inf. Dev.*, vol. 26, no. 2, pp. 141–147, 2010.

[11] S. L. Gencer and M. Koc, "Internet Abuse among Teenagers and Its Relations to Internet Usage Patterns and Demographics," *Educ. Technol. Soc.*, vol. 15, no. 2, pp. 25–36, 2012.

[12] Y. Li, X. Zhang, F. Lu, Q. Zhang, and Y. Wang, "Internet addiction among elementary and middle school students in China: a nationally representative sample study," *Cyberpsychol Behav Soc Netw*, vol. 17, no. 2, pp. 111–116, 2014.

[13] C. Herley and D. Florencio, "How to login from an Internet café without worrying about keyloggers," in *2nd Symposium. on Usable Privacy and Security (SOUPS), July 12-14, Cornegie Melon University*, 2006, pp. 1–2.

[14] E. E. Adomi and W. P. Akpochafo, "Cybercafés and Prevention of Terrorist Activities," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 270–282.

[15] O. Oluwafemi, F. A. Adesuyi, and S. M. Abdulhamid, "Combating Terrorism with Cybersecurity : The Nigerian Perspective," vol. 1, no. 4, pp. 103–109, 2013.

[16] L. Wu and J. Delva, "The effect of computer usage in internet cafe on cigarette smoking and alcohol use among Chinese adolescents and youth: A longitudinal study," *Int. J. Environ. Res. Public Health*, vol. 9, pp. 496–510, 2012.

[17] CCAOI, "Guide for Cyber Café , CSC and eCommerce Service Retailer."

[18] A. A. Oyelude and C. O. B. Adewumi, "Cybercafé Physical and Electronic Security Issues," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 84–94.

[19] P. A. Tiemo and C. U. Charles-Iyoha, "Cybercafés and Cyber Crime in Nigeria," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 295–306.

[20] F. C. Chidozie, L. P. Odunayo, and A. O. Olutosin, "Deregulation of the Nigerian Telecommunication Sector : Interrogating the Nexus Between Imperialism and Development," *Acad. J. Interdiscip. Stud.*, vol. 4, no. 1, pp. 173–184, 2015.

[21] NCC, "The Nation (2nd November , 2011) - What makes telecom business tick ?"

[22] S. K. Mamah, "The Prospects and Problems of Deregulation of the Nigerian Economy," University of Nigeria, Nsukka, 2012.

[23] P. Udende and A. L. Azeez, "Internet access and use among students of the University of Ilorin , Nigeria," *J. Commun. Media Res.*, vol. 2, no. 1, pp. 33–42, 2010.

[24] F. Osang, "Internet Access in Nigeria: Perception of National Open University of Nigeria (Noun) Students," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 2, no. 10, pp. 492–497, 2012.

[25] S. Ifedigbo, "Tribute to the Cyber Café," *Daily Times*, pp. 1–3, 2012.

[26] M. Chawki, "Nigeria Tackles Advance Fee Fraud," *J. Inf. Law Technol.*, no. 1, pp. 1–20, 2009.

[27] H. Chiroma, M. Abdulhamid, A. Ya, A. Muhammad Usman, and T. Umar Maigari, "Academic Community Cyber Cafés -A Perpetration Point for Cyber Crimes in Nigeria," *Inf. Sci. Comput. Eng.*, vol. 2, no. 2, pp. 7–13, 2011.

[28] A. O. Obuh, "Cybercafé Management Software," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 113–124.

[29] A. I. Ajewole, "Software Requirements for Cybercafés," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 125–146.

[30] E. M. Mwathi, "Factors influencing effective management of electronic waste: A case study of Cybercafes in Nairabi Central

Business District, Kenya," Project Planning and Management of the University of Nairobi 2014, 2014.

[31] M. M. Marwa, "Technology Barriers to Quality of Service Offered by Cyber Cafes: A Case Study of Cyber Cafes in the Nairobi CBD," United States International University, 2013.

[32] S. Magaji and C. I. Eke, "Measuring Technical Efficiency of Wireless and Wired Technologies in Nigeria Cyber Cafés," vol. 4, no. 1, pp. 15–34, 2013.

[33] O. B. Adogbeji and M. N. Mabi, "Cybercafes operations and its incessant closure in Delta State, Nigeria," *J. Internet Inf. Syst.*, vol. 5, no. 1, pp. 1–8, 2015.

[34] M. Koç and K. A. Ferneding, "The Consequences of Internet Café Use on Turkish College Students ' Social Capital," *Turkish Online J. Educ. Technol.*, vol. 6, no. 3, pp. 88–97, 2007.

[35] N. Kara and K. Cagiltay, "Flow Experiences of Adolescents in Terms of Internet Café Environment and Computer Game Play Characteristics," *Procedia - Soc. Behav. Sci.*, vol. 89, pp. 298–307, 2013.

[36] W. Shang, G. Li, O. Arogundade, and X. Jiang, "Understanding Cybercafés Users behavior in Mainland China : An Exploratory Study," in *Proceedings of IPID Postgraduate Strand at ICTD 2010*, 2010, pp. 1–4.

[37] B. Furuholt, S. Kristiansen, and F. Wahid, "Information Dissemination in a Developing Society: Internet Cafe Users in Indonesia," *Electron. J. Inf. Syst. Dev. Ctries.*, vol. 22, no. 3, pp. 1–16, 2005.

[38] S. S. Alam, Z. Abdullah, and N. Ahsan, "Cyber Café Usage in Malaysia : An Exploratory Study," *J. Internet Bank. Commer.*, vol. 14, no. 1–13, 2009.

[39] M. Y. Abdulkareem, "Characteristics and information-seeking behaviour of cybercafé users in some Nigerian cities," *Int. J. Libr. Inf. Sci.*, vol. 2, no. 5, pp. 95–101, 2010.

[40] E. E. Adomi, "Overnight Internet Browsing Among Cybercafe Users in Abraka , Nigeria," *J. Community Informatics*, vol. 3, no. 2, pp. 1–8, 2007.

[41] R. P. Bringula, J. Bonifacio, A. Natanauan, M. Manuel, and K. Panganiban, "Pattern of Internet Usage in Cyber Cafés in Manila: an Exploratory Study," *Int. J. cyber Soc. Educ.*, vol. 5, no. 2, pp. 149–163, 2012.

[42] A. S. Sife, "Internet use behaviour of cybercaf?? users in Morogoro Municipality, Tanzania," *Ann. Libr. Inf. Stud.*, vol. 60, no. 1, pp. 41–50, 2013.

[43] B. Furuholt and S. Kristiansen, "Internet cafés in Asia and Africa – Venues for education and learning?," *J. Community Informatics*, vol. 3, no. 2, pp. 1–12, 2007.

[44] M. Gurol and T. Sevindik, "Profile of Internet Cafe users in Turkey," *Telemat. Informatics*, vol. 24, pp. 59–68, 2006.

[45] A. Lawan, B. S. Galadanci, and A. A. Abdallah, "A Modified Expectation Confirmation Theory with Perceived Trust on Internet Cafes Use Continuance: A Conceptual Framework," in *IT4InDev 2015*, 2015, pp. 134–140.

[46] J. L. Qiu and Z. Liuning, "Through the Prism of the Internet Cafe: Managing Access in an Ecology of Games," *China Inf.*, vol. 19, no. 2, pp. 261–297, 2005.

[47] D. Onojaefe and M. Leaning, "Managing Cybercafés: Achieving Mutual Benefit through Partnership," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 95–111.

[48] [48] A. O. Obuh, "Viruses and Virus Protection in Cybercafés," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 170–185.

[49] A. R. Garuba, "Computer Virus Phenomena in Cybercafé," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 186–204.

[50] A. A. Paul and C. Zhang, "Evaluate Security on the Internet-Cafe," 2013.

[51] Y. Dina, "Cyber Laws and Cybercafés: Analysis of Operational Legislation in some Commonwealth Jurisdictions and the United States," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 221–238.

[52] O. T. Emiri, "Prevention of Cyber Crime in Cybercafés," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 239–252.

[53] D. Rauniar, "Cybercafés of Nepal: Passage to Cyber Crime?," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 253–269.

[54] S. E. Igun, "Cyber Crime Control in Developing Countries' Cybercafés," in *Security and Software for Cybercafes*, E. E. Adomi, Ed. Hershey PA: IGI Global, 2008, pp. 283–294.