Universal Journal of Educational Research 8(6): 2710-2716, 2020 http://www.hrpub.org
DOI: 10.13189/ujer.2020.080656

School-based Cybersecurity Education Programme for Schoolchildren in South Africa! A Timely Call from Bloemfontein

Olugbenga Adedayo Ige

School of Social Sciences and Language Education, University of the Free State QwaQwa Campus, Republic of South Africa

Received February 15, 2020; Revised April 6, 2020; Accepted April 19, 2020

Abstract The interconnection of many countries of the world today is hugely tied to the overwhelming improvements in the Internet. However, the improved Internet connectivity is not without diverse security risks such as bullying, scamming, hate speech, and identity theft especially for minors. It is unfortunate that the security risks attached to the use of the Internet are often ignored in the rush to log online by schoolchildren in South Africa. The cyber insecurities in South Africa became more precarious as schools do not teach cybersecurity as a subject in South Africa at present. Consequently, it behooves the researcher to unveil how the agents of education in South Africa learning ecologies can use the school-based cyber security education programme to protect schoolchildren against cyber scammers, and propose a blue-print on developing a school-based cybersecurity education programme for South African schoolchildren. In this paper, the space transition theory is used to explain the causation of insecurities confronting cyber savvy schoolchildren in South Africa. This paper methodically explicated related scientific papers that were published from 2005 to 2019 on cybercrimes, cybersecurity, and school-based participatory research. The community-driven model developed by Lavery et al. (2005) was used to design the school-based cybersecurity educational programme. This paper exhaustively explained the operations of the school-based cybersecurity educational programme and illustrated how teachers can use the informal cybersecurity educational programme to teach cybersecurity in South African schools.

Keywords Bloemfontein, Cybersecurity, Cybercrime, Schoolchildren, School-based Approach, South Africa

1. Introduction

The incidences of crimes were limited to the physical spaces in the pre-Internet era. At the dawn of the nineteenth century, most crimes that were hitherto the preserve of physical spaces were imported into cyberspace which was made possible by the escalation in the use of the Internet and other ancillary devices. From this period, the physical mails sent via the post offices gave way to electronic mails, terrorism in the physical spaces turned to cyber terrorism, pornography moved to the Internet, and physically organized crime translated to cyber organized crime. These criminal activities that were carried out via the Internet have resulted in $7.45 billion monetary losses which emanated from 1,509,679 people's complaints between 2014 and 2018 (National White Collar Crime Center, 2018). The victims of these monetary losses were from different countries of the world and usually under the age of 20 while the other victims ages ranged from 20 to over 60. These victims were resident in India, the United Kingdom, Canada, Australia, Georgia, Germany, Brazil, Mexico, Greece, Philippines, Russian Federation, France, South Africa, Italy, Hong Kong, Switzerland, China, Spain, Portugal, and Japan. The report that featured these nations excluded the data from the United States, while only South Africa featured in the African continent. It is likely a reader of this article would ask what the police or security agencies in these nations were doing that law-abiding citizens, including school children would lose $7.45billion in four years (National White Collar Crime Center, 2018). The police or security agencies in the countries where these victims resided were trained to function in the analog era, and as such lack of the capacity for cyberspace policing. Furthermore, the anonymity associated with the evolution of the Internet makes the investigation of incidences of cybercrime difficult especially with the change of the

Internet protocol addresses by the perpetrators who are in different countries of the world.

This article examines the incidences of cybercrimes involving schoolchildren in South Africa and it is motivated by the 2018 Internet crime report that shows that children under the age of twenty are at risk in South Africa while interacting in the cyber space. The space transition theory is used to explain the vulnerability of schoolchildren in South Africa to incidences of cyber lawlessness, while the school-based cyber security education is represented as a panacea to the vulnerability. This review answers this question:

1. How can the agents of education in South Africa learning ecologies use the school-based cyber security education programme to protect schoolchildren against cyber scammers?

2. Conceptual Framework

2.1. What Is Cybercrime?

Crimes committed in the cyber space are termed 'Cybercrimes'. Moid (2018) stated that cybercrimes comprise any criminal conduct carried out via information technological devices such as cyber hacking, identity theft, spamming social engineering, programming attacks, online fraud, and data alteration. The definition ascribed to cybercrime by Moid (2018) seems to focus on technical cybercrimes and excludes the social related cybercrimes that are endemic among schoolchildren. Cassim (2011) declared that 'cybercrime' has thriven on the African continent and affirmed that cybercrime otherwise called 'computer crime' has no clear out definition. Cassim (2011), in furtherance of this assertion, cited Brener and Clarke (2005) that when a computer is used as an instrument to perpetrate analog-aged crimes such as fraud, theft, extortion, denial of service attacks and malware, child pornography etc, the computer is taken as an object crime. It might be pertinent to add that such a computer must have a live Internet connection for such a crime to qualify as a 'cybercrime'.

Ige (2008) shifted from the definitions of scholars in core science disciplines and defined 'cybercrime' which is otherwise referred to as 'Yahoo Yahoo' in the context this scholar researched as a crime committed on the Internet, using the Internet and by means of the Internet. Amosun and Ige (2009) went further to highlight eighteen different crimes committed in the cyberspace especially among schoolchildren and discovered that identity theft was the most common cybercrime.

On the appropriate definition of cybercrime, Jaishankar (2012) stated that several definitions of cybercrime were evolved in the pre and post millennial era, with these definitions focusing on the crimes committed in the cyberspace, or the victims as well as the offender. Halder and Jaishankar (2011) defined cybercrimes as offences that are committed against individuals or groups of individuals with a criminal motive to deliberately damage the reputation of the victim directly or indirectly, using present-time telecommunication networks such as the Internet. The definition of Halder and Jaishankar (2011) marked a shift from machine-based to human focused definition (see Jaishankar, 2012). It is evident from this definition that the internet is central to the use of computer and other ancillary devices (i.e. provides necessary support to the primary activities of the Internet) to commit crime in the cyberspace. The realities of the current age make it impossible to have a globally accepted definition of crimes committed in the cyberspace. At present, crimes committed in the cyberspace are evolving. Some of these crimes are known, while others would emerge as the world becomes more interconnected.

2.2. Incidences of Cybercrime Involving Schoolchildren in South Africa

A recent data released by the South African Banking Risk Information Centre reported that South Africa ranked third globally with regards to cybercrime victims and accumulated losses of about 2.2 billion South African Rands (USD119850500,00.) These are some of the incidences of cybercrimes involving children in South Africa in recent times.

2.3. The Porn Pastor at Cape Town

This occurrence involved a man named 'Kent Locke' who disguised as a scantily cladded female to entice a minimum of forty-seven teenage boys to send explicit photographs to him (Chambers, 30 October 2019). Kent Locke was re-arrested after a collaborative investigation involving the South African Police Service and Department of Homeland Security in the United States. Chambers (2019) reported that Kent was jailed for fifteen years and his name was added to the sexual offenders' register. However, five of these fifteen years sentence was suspended after a plea bargain by Kent.

2.4. The Serial Paedophile

Another interesting incidence was the case involving Bret Allen Steven who was jailed by the Port Sheptsone Regional Court for ten years for possessing child pornographic materials (Naidoo, 2019). Five of the ten years was suspended because he pleaded guilty to possessing child pornographic materials. Naidoo (2019) reported that this offender had earlier been sentenced to eight years jail term at East London in 2006 for possessing child pornographic materials, and seven years imprisonment in 2011 for possessing more than three thousand pornographic images of children. Three of

Steven's second eight years in jail was suspended as well.

2.5. Implications of the 2018 Internet Crime Report for Schoolchildren in South Africa

The Internet fraud Complaint Center (IFCC) which later changed to Internet Crime Complaint Center was established by the United States government. The Centre started operations on 8 May 2000, a partnership involving the National White Collar Crime Center and Federal Bureau of Investigation, and had received 4,415,970 complaints till 31 December 2018 (The National White Collar Crime Center & Federal Bureau of Investigation, 2018).

Table 1 Presents the 2018 victims of cybercrimes by age in the first twenty countries of the world which are targets of cyber-scammers

Table 1. 2018 Cybercrime victims by Age Group Worldwide

Age Range	Total Count	Total Loss
Under 20	9,129	$12,553,082
20-29	40,924	$134,485,965
30-39	46,342	$305,699,977
40-49	50,545	$405,612,455
50-59	48,642	$494,926,300
Over 60	62,085	$649,227,724

Source: 1C3 2018 Internet Crime report (1 January 2018-31 December 2018).

Table 1 shows that victims above the age of 60 had the highest monetary losses to cyber-scammers while the victims below the age of 20 lost the least amount of money. However, it should be noted that the group under age 20 represents the schoolchildren in South Africa which are the focus of this article. The victims below age 20 would have experienced more severe monetary losses to cyber predators if they were the working class in South Africa and the other nineteen nations in the top twenty mark. It is in the light of South Africa's rating as thirteen among the top twenty countries whose citizens were victims of cybercrime that this article designs a school-based cybersecurity education programme in South Africa.

3. Theoretical Framework

3.1. Space Transition Theory

The Space transition theory was propounded by Karuppannan Jaishankar, a foremost criminologist at Rasksha Shakti University, India in 2008. Jaishankar (2008) posited that the movement of people from one space to another i.e physical space to cyber space would cause the exhibition of conforming and non-conforming behaviours in these spaces. In this article, it is appropriate to state that a space which is a continuous zone that is free or unoccupied would readily be occupied by legal or illegal means. Unfortunately, the cyber space has evolved in a manner that makes it difficult for daily users of the Internet to identify legal or illegal occupants of the cyber space until an evil that warrants investigations is committed. In the physical space, it is possible for the law enforcement agencies to spot a person with non-conforming behaviours at checkpoints or during neighbourhood patrols. The situation is different in the cyberspace because as soon as the anti-virus programs, firewalls, internet encryptions, or cryptographic protocols are breached by an impostor, there will be nothing that hinders such an impersonator from scamming unsuspecting victims. The second proposition of space transition theory by Jaishankar (2008) stated that *'identity flexibility, dissociative anonymity and lack of deterrence factor in the cyberspace provide the offenders with the choice to commit cybercrime', which* is relevant to the focus of this discourse. For instance, if an investigator would ask any of the under 20 age range that lost money to cyber scammers in the trends reported by the National White Collar Crime Center and Federal Bureau of Investigation in 2018, the response by the victim on the identity of whom they wired money to would be different from the identity of the scammers in real life. Another recent event was reported in the United States which involved a Japanese woman and a United State Army Captain in Syria (Crime & Justice News, 2019). Both were engaged in intense internet romance for more than ten months which left the Japanese woman two hundred thousand dollars poorer, and unfulfilled promises from Captain Terry Garcia to sneak diamonds out of Syria (*See http//www.thecrimereport.org*). Eventually, it was an investigation that was initiated by a Federal Bureau of Investigation agent in the United States in 2016 that revealed in 2019 that Captain Terry Garcia was non-existent, but another person who was a part of international circuit of cyber scammers that operated from Nigeria and Los Angeles. The instances cited in this article clearly provide information on the nature of flexibility, (i.e. I can change to who I want users to believe I am in the cyberspace), and dissociative anonymity (i.e. I can make people not to know me in the cyberspace). These two instances that were cited to explain the second proposition of space transition theory were corroborated by Jaishankar and Chandra (2018) that an individual (F^1) can assume false identity and continually communicate with another individual (F^2) for varied number of days or months before that individual (F^1) would discover that the person he has been electronically conversing with is not who he claimed to be.

Despite the general acceptability of Jaishankar's (2008) space transition theory, it would be worthwhile to point out that conforming behaviours in a society might be non-conforming behaviours in a nation. Given these possibilities in the light of the realities of globalization, it

might be necessary to review this aspect of space transition theory. The relevance of space transition theory to the issues of cyber insecurities discussed in this article is the explanation it offers on the loss of money experienced by under 20s (i.e. schoolchildren) in South Africa and other countries. People in the age-range of 20 that were swindled by cyber scammers were accessed via identity flexibility, dissociative anonymity, and lack of deterrence factor.

4. Methodology

The researcher carried out electronic researches on reputable sources such as the repositories of Internet Crime Complaint Center in the United States of America, International periodicals, sage publications, Emerald Group Publishing, and other journals that were published on cybercrimes such as International Journal of Cyber Criminology. Keywords such as cybercrime, cybersecurity, action research, action curriculum models, school-based intervention, cybercrime reports were used to search these scholarly repositories. In addition to these, manual searches were conducted on scholarly journal repositories such as *International Journal of Cyber Criminology, Journal of Work-Applied Management, Journal of Emotional and Behavioral Disorder, The American Journal of Public Health, The Journal of the Fiji Institute of Accountants, The African Symposium: An Online Journal of African Educational Research Network, Victims and Offenders, and The Comparative and International Law Journal of Southern Africa.*

The articles selected from these journals were included in the current research because they were published from 2005 to 2019. The selected articles published during this period were selected because educational research on cybercrimes gathered momentum from early 2000s (See Yar, 2005; Wall, 2005). Additionally, the articles published in the selected journals focused on cybercrimes, action research, and community capacity.

5. Discussion

5.1. The South African School-based Cybersecurity Education Programme

Consequent on the presence of South Africa as the only African nation with cybercrime victims in the Top 20 rank, and the loss of $12,553,082 by people under the age of 20 in South Africa and other countries reported by the National White Collar Crime Center and Federal Bureau of Investigation in 2018, this research article presents a model (Figure 1) for preventing cybercrimes among school children in South Africa using the action community model by Lavery, Smith, Esporza, Hrushow, Moore, and Reed (2005).

Source: Lavery, S.H, Smith, M.L., Esporza, A.A., Hrushow. A., Moore, M., & Reed, D.F. (2005). The community action model: A community-driven model designed to address disparities in health. Am J Public Health, 95(4), 611-616.

Figure 1. Community Action Model

Step 1: Train Participants

To initiate the action to tackle cybercrime, the teacher gives action training to develop the skills of schoolchildren for collaborative endeavours. McLaughlin, Leone, Meisel, and Henderson (1997) premised the need for building the capacity of school children on the need to train students who are habitually non-complaint and unresponsive to school authority, and who pose a danger to themselves and other students.

The teacher is expected to build the capacity of schoolchildren through seminars, and workshops to initiate the process of developing the school-based cybersecurity education programme.

Step 2: The school children define, design, and do community diagnosis

In this step, Lavery et al. (2005) suggested the use of action research by the advocates to define, design, and conduct a community diagnosis. The participatory action research (see Ige, 2018) is preferable to adopt by schoolchildren to define, design and conduct a community diagnosis because the context of the cyber security education programme is situated in school ecologies. The action research frame suggested by Lavery et al. (2005) might be connected to the context in which these scholars developed and evaluated the programme. Alternately, the schoolchildren might consider using Action Research Action Learning (ARAL) (Coghlan & Brannick, 2005; McAlinden, 2015) which comprises diagnosis, planning action, taking action, and evaluating action.

Lavery et al. (2005) stated that this step is necessary to ascertain the primary causes of a social issue and list the resources to overcome it. Therefore, the school children will ascertain the roots of cyber insecurities confronting schoolchildren in South Africa and outline the resources that are available in the school to deal with it. The participants of Lavery et al. (2005) used key informant interviews to achieve this step. Consequent on the nature of cybercrime, in-depth focus group discussions that will last from two to three weeks are recommended to enable the selected schoolchildren to attain these objectives.

Step 3: Analyse Results of Community Diagnosis

The school children present the outcomes of the in-depth focus group discussions and identify recurring themes across each group. Ige (2018) stated that teacher/researcher and focus group leaders prepare findings, and propose the action means of implementing the results.

Step 4: Select Action or Activity and implement

The schoolchildren utilize the outcomes of the focus group discussion to propose solutions to cybercrimes affecting schoolchildren in South Africa. Lavery et al. (2005) stated that the 'action' specified at this stage connotes the desired policy outcome for the research projects, and it must meet three criteria such as achievability, potential for sustainability and compelling members of groups (i.e. schoolchildren) to change their community cyberspace for the well-being of the entire users. Lavery et al (2005) further posited that activities are the educational and organizational interventions that develop and support the outcomes. Ige (2018) stated that the participants may establish a club (i.e. Cybersecurity Education Club), draw a constitution for the club, suggest participatory activities such as drama, public campaigns, public jingles, seminars, workshops and implement these participatory activities.

Step 5: Maintain and Enforce Action or Activity

The schoolchildren sustain the cyber security educational activities by advocating for popular policies regarding cyber insecurities and conclusion.

The article is a timely call from Bloemfontein due to the escalating trends in the cyber victimization of South Africans which has culminated into $7.45bllion monetary losses. The demographical information of people that experienced these financial losses reflected that of the school-aged children in South Africa. The call made to schools in South Africa is timely because South Africa did not feature in the 2015 data released by the National White Collar Crime Center on countries by victims location. However, three hundred and thirty-seven victims were reported to have been scammed in South Africa in 2016, while the country was ranked 12 among the top 20 countries where the victims were residents. Despite the 13th position of South Africa in the data released by 1C3, 349 and 409 victims were reportedly swindled in 2017 and 2018 respectively. These figures showed the increasing trends that portend great dangers for safety of schoolchildren in South Africa when they communicate in the cyberspace.

6. Conclusions

This is the current scenario that reflects the safety of schoolchildren in South Africa:

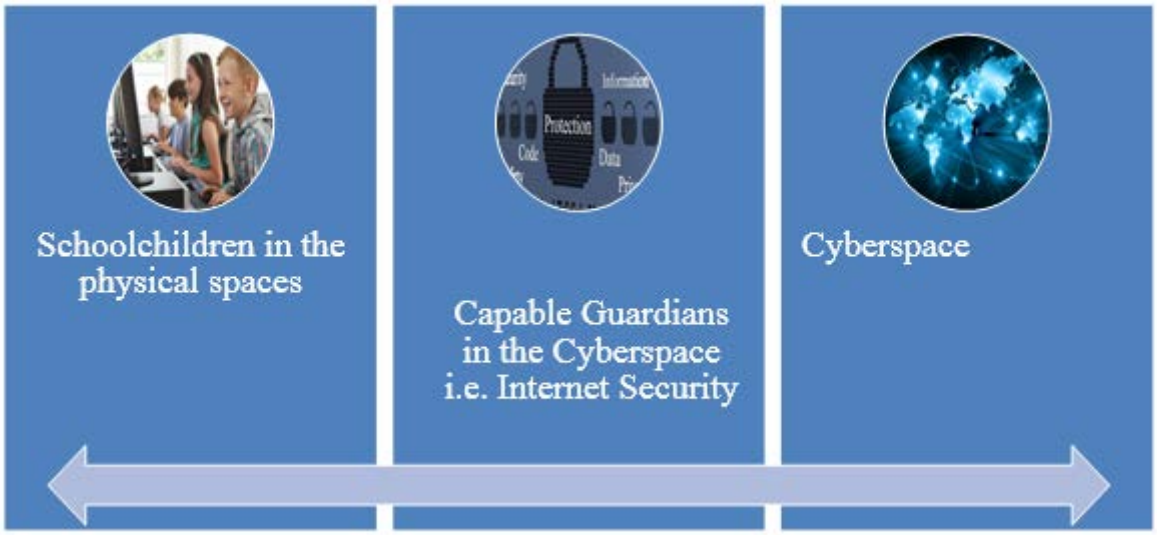

Figure 2. Ecological scenario of Internet security programs for schoolchildren in South Africa

The implication of this structure in figure 2 is that schoolchildren become immediately vulnerable cyber scammers who overpower the technical guardians such as Internet encryption, Internet security programs, firewalls etc.

It is consequent on the vulnerability of school children in the prevalent security arrangement in the cyberspace that this article presents this new programme, which is illustrated in figure 3:

Figure 3. Cyber ecological scenario of School-based cybersecurity education programme

The conclusion I wish to make is that Internet security programs cannot singlehandedly protect schoolchildren from victimization in the cyberspace. Rather education should be introduced to complement the technical programs developed by computer scientists and engineers to end the menace of cybercrimes in South Africa.

Ethical Considerations

The details of the school-based cybersecurity programme provided in this article was approved and reviewed by the General/Human Research Ethics committee (GHREC) at the University of the Free State, South Africa. The ethical clearance number is UFS-HSD2019/1832.

Acknowledgements

I humbly wish to express my heartfelt appreciation to Dr. Daniel Ajayi at Technische Universitat Chemnitz, Germany who edited the draft of this article at no cost.

REFERENCES

[1] Amosun, P.A. & Ige, O.A. (2009). Internet crime: A new breed of crime among in-school aged children in Nigeria. *The African Symposium: An Online Journal of African Educational Research Network, 9*(2), 90-98.

[2] Cassim, F. (2011). Addressing the growing spectre of cyber crime in Africa: Evaluating measures adopted by Africa and other regional players. *The Comparative and International Law Journal of Southern Africa, 44*(1), 123-138.

[3] Chambers, D. (30 October 2019). 'Porn Pastor' gets 15years for sexually abusing boys in Cape Town. Sunday Times, Times Lives. Retrieved 12 November 2019 from https://www.timeslive.co.za/news/south-africa/2019-10-30-porn-pastor-gets-15-years-for-sexually-abusing-boys-in-cape-town/.

[4] Coghlan, D. and Brannick, T. (2005). *Doing Action Research in Your Own Organisation*. Sage Publications, London.

[5] Crime and Justice News (23 August 2019). Feds charge 80 in $46m Nigerian cybercrime scheme. The Crime Report, Retrieved from https://thecrimereport.org/2019/08/23/feds-charge-80-in-46m-nigerian-cybercrime-scheme/.

[6] Finau, G., Samuwai, J., & Prasad, A. (2013). Cybercrime and its implications to the pacific. *The Journal of the Fiji Institute of Accountants*, June, 15-16.

[7] Halder, D., & Jaishankar, K. (2011). Cyber gender harassment and secondary victimization: A comparative analysis of the United States, the UK, and India. *Victims and Offenders, 6*(4), 386-398.

[8] Ige, O.A. (2008). *Secondary school students' perceptions of incidences of internet crimes among school age children in Oyo and Ondo states, Nigeria*. An unpublished Master's dissertation submitted to University of Ibadan, Ibadan, Nigeria.

[9] Ige, O.A. (2018). Effects of gender and technological fluency on learners' attitude to cyber crime prevention in urban learning ecologies. *International Journal of Cyber Criminology, 12*(1), 143-163. http://www.cybercrimejournal.com/IgeVol12Issue1IJCC2018.pdf

[10] Jaishankar, K. (2008). Space transition theory of cyber crimes. In Schmallager, F. & Pittaro, M. (Eds), *Crimes of the Internet* (pp. 283-301). Upper Saddle River, NJ:Prentice Hall.

[11] Jaishankar, K. (2012). *Victimization in the cyberspace: Patterns and trends*. In Manacorda, S., Flor, R. & Jang, J.O. (Eds.). *Cybercriminality: Finding a balance between freedom and security*, 91-106, Milano, Italy: International Scientific and Professional ISP C Advisory Council. ISBN 978-88-96410-02-8.

[12] Jaishankar, K., & Chandra, R.R. (2018). *Cyber criminology and cyber forensics*: Module 23: Space transition theory of cyber crimes. Retrieved 12 November 2019 from https://www.researchgate.net/publication/321716315_Space_Transition_Theory_of_Cyber_Crimes.

[13] Lavery, S. H., Smith, M. L., Esporza, A. A., Hrushow. A., Moore, M., & Reed, D. F. (2005). The community action model: A community-driven model designed to address disparities in health. *Am J Public Health*, *95*(4), 611-616.

[14] McAlinden, F. (2015). Using Action Research and Action Learning (ARAL) to develop a response to the abuse of older people in a healthcare context. *Journal of Work-Applied Management, 7*(1), pp. 38-51,https://doi.org/10.1108/JWAM-10-2015-004

[15] McLaughlin, M.J., Leone, P.E., Meisel, S., & Henderson, K. (1997). Strengthen school and community capacity. *Journal of Emotional and Behavioral Disorder, 5*(1), 15-23.

[16] Naidoo, S. (4 November 2019). Paedophile jailed for third time. *South Coast Herald*. Retrieved 12 November 2019 from https://southcoastherald.co.za/381576/paedophile-jailed-again-2/.

[17] The Federal Bureau of Investigation and Internet Crime Complaint Center. (2018). 2018 Internet Crime Report. Retrieved 13 November 2019 from https://www.ic3.gov/media/annualreports.aspx.

[18] Wall, D. 2005. The Internet as a Conduit for Criminals. In A. Pattavina (Ed.). Information Technology and The Criminal Justice System. London: Sage.

[19] Criminal Justice System. London: Sage.Yar, M. 2005. The Novelty of Cyber Crime: An assessment in Light of Routine Activity Theory. European Journal of Criminology. 2: 407-427.