Copyright © 2018 International Journal of Cyber Criminology – ISSN: 0973-5089
January – June 2018. Vol. 12(1): 151–170. DOI: 10.5281/zenodo.1467888
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Effects of Gender and Technological Fluency on Learners' Attitude to Cyber Crime Prevention in Urban Learning Ecologies: Lessons for Swedish Gymnasiums

Olugbenga A. Ige[1]
University of the Free State, South Africa

Abstract

The technology age has produced new kinds of 'yakuza' called 'cyber bandits'. Unfortunately, the laws that could curb these new loci of criminal activities were promulgated in the analog era in Nigeria and Sweden. The rise of Internet use among children in secondary schools in Nigeria and Sweden has influenced the increase in the rate of cyber scams in these countries. This study showcases the use of a participatory action research paradigm to develop a cybercrime prevention programme. The action programme was evaluated using the quasi experimental design of a pretest-posttest type. The confounding effects of gender, technological fluency, and the action programme were tried out on 218 students to test their attitude to crime prevention in the cyber space. The analysis gave a disordinal interaction, as the sex difference was evident for the low, medium and high technologically fluent students. Additionally, the students' perceptions of the action program were positive. The implications of these findings are discussed, while a blue print is given on replicating the participatory cybercrime prevention programme with upper secondary education students in Sweden.

Keywords: Gender, Technological fluency, Learners' attitude to cybercrime prevention, Urban learning ecologies, Swedish gymnasiums.

Introduction

The Internet has transformed into an integral platform such that research on globalization has affirmed the Internet's advancement on the integrative tides of the modern world (Townes, 2012, p. 43). Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts, and Wolff (1997, p. 3) state that the Internet evolved from Licklider's August 1962 discussion of 'Galactic Network' concept which was the earliest recorded account of social interactions that was possible through networking. Leiner et al. explain that 'In late 1966, Roberts went to the Defense Advanced Research Projects Agency

[1] Postdoctoral Research Fellow, SANRAL Chair in Science, Mathematics and Technology Education: Office of the Dean, Faculty: Education, PO Box 339, Bloemfontein 9300, Republic of South Africa. Email: IgeOA@ufs.ac.za

(DARPA) to develop the computer network concept and quickly put together his plan for the 'ARPANET', which was published in 1967' (1997, p. 3).

Ren, Kwan, and Schwanen (2013, p. 187) confirm that in the previous fifteen years, the use of Internet has attracted significant attention in media studies, sociology, geography, and other related disciplines. Leiner et al. (1997, p. 5) declare that the 'ARPANET' developed into the 'Internet', which was founded on the idea that there would be multiple independent networks of rather arbitrary design which started with the 'ARPANET' as the first packet switching network, and later included packet satellite networks, ground-based packet radio networks, and other networks.

A famous survey on the incidences of Internet crimes among school-aged children in Nigeria (Ige, 2008) reveals that cybercrime is popularly known as 'Yahoo Yahoo' or 'Yahoo Plus' (street name for scammers using 'Mayehun' (voodoo power/magic) for their targets). Ige (2008) explains that the 'use of another person's name and social security number to obtain goods and services, otherwise known as 'Identity Theft' is the most common cybercrime among school-aged children in Nigeria.

Educational researchers were celebrating the transformation the Internet had brought to education, when the criminal behaviors aided by the anonymity offered by the Internet were confounding the many users across the globe. It should be noted that the Defense Advanced Research Projects Agency (DARPA) expanded ARPANET that enabled multiple computers to communicate on a single network purely on societal development grounds. Brunton (2013) states that the expansion of the 'ARPANET' to 'Internet' ushered in the era of high-margin Nigerian wire scams which have 'ponzi' features. The use of the Internet to affect criminal enterprise emanated as an external shock to educational researchers in developed nations of the world.

One of the earliest researches that blew the whistle on cyber crime was Esen (2002) who states that the concept has no globally accepted definition. Esen (2002) subsequently defines this new locus of criminal activity as illegal activities performed principally using a computer that is connected to the Internet. Liang and Liu (2010) state that cyber crimes are in two broad categories: criminal activities targeting information networks and computer systems as well as other crimes carried out using computer-related networks. The operational categories highlighted by Liang & Liu (2010, pp. 111-112) derived from the crimes committed in the cyber landscape of China. The crimes committed in the cyber context of other nations might have accounted for scholars' definitions of cyber crime.

Why Develop Learners' Attitude to Cyber Crime Prevention through Education?

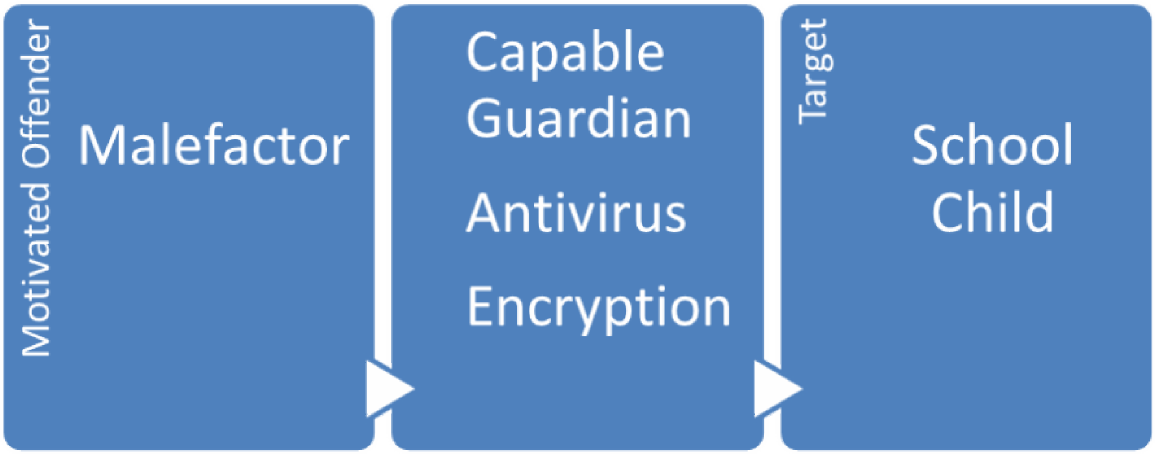
1. Routine Activities Theory

Many theories have striven to unearth the causes of crime in cyber space. One of these is the routine activities theory propounded by Cohen and Felson (1979). Wick et al. (2017, p. 27) explain that routine activities theory proposes that crimes occur at the interchange of three circumstances namely:

- A reachable, striking and suitable target,
- The availability of a motivated malefactor (proximity),

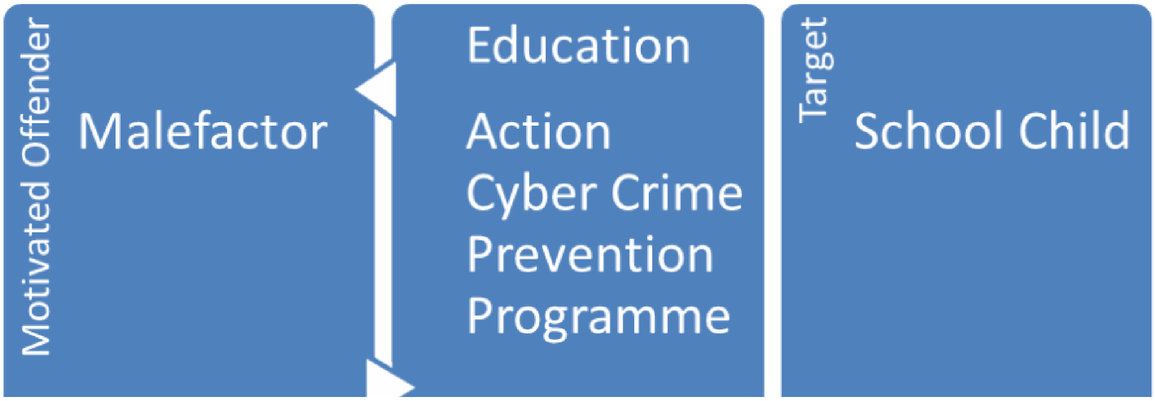
- And the non-existence of a competent guardian. The implication of these conditions for the occurrence of crime in cyberspace is illustrated in figure 1.

Figure 1. Cyber ecological scenario described by Routine Activity Theory



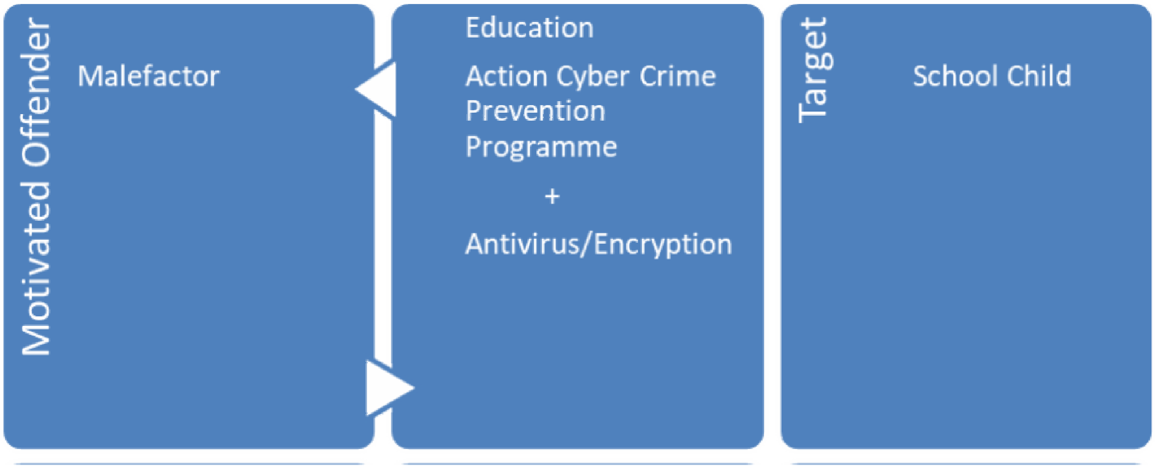
This illustration implies that the failure of an antivirus or internet security programme will make a child vulnerable to cyber scammers when surfing the Internet. It is this lacuna that has been observed in the use of technical solutions proffered by scientists to the amelioration of the occurrence of crime in cyberspace that led to the development of action cyber crime protective scheme education by the researcher (see figure 2). To the researcher, education seemed a more capable guardian than encryption and antivirus programs.

Figure 2. Cyber ecological scenario created by the action cyber crime prevention programme



While the motivated offender may have access to the child in the ecological scenario depicted in figure 2, the cyber-attack will be unsuccessful because the child has been educated on techniques of handling anonymous interaction in cyber space. However, it is recommended that the action cyber crime prevention programme be complemented with technically capable guardians like an antivirus program and encryption (see figure 3).

Figure 3. Possible cyber ecological scenario of combination of education and computer security programme



The routine activity theory is relevant to this research project because school-aged children are not only reachable, but striking and suitable for adult predators or pedophiles that are ravaging children operating personalized accounts on the Facebook in Nigeria, and other countries of the world. These adult predators or pedophiles are the motivated malefactors that are regularly available on the social networking websites. These social networking platforms enabled the adult predators or pedophiles to operate near female school children active on the Facebook, 2go.com, Whatsapp etc. The absence of a competent guardian posited by Cohen and Felson (1979) is evident in the story reported by a national tabloid in Nigeria of a Lagos printer that abducted and raped a pupil he met on Facebook.[2] In figure 3, it is believed that guardians like antivirus, internet security program, and encryption will take care of technical insecurity confronting learners in cyber space, while an action cyber crime prevention programme will take care of cyber social issues.

3. Space Transition Theory

Another theory that evolved at the dawn of the twenty-first century is the space transition theory which was developed by Jaishankar (2008, p. 27). The second and fifth postulates of the space transition theory are relevant to the causation of cyber crimes among school children. The first postulate states that identity flexibility, dissociative anonymity and lack of deterrence factors in cyberspace present the offenders the choice to execute cyber crime. Students in Nigeria use addresses that are not name-specific to open emails and social media accounts which give them a flexible identity in cyberspace. These pseudo-names afforded by email service providers make students believe they are not known to other users of cyberspace. The absence of a teacher-student relationship in cyberspace like the physical classroom, could spur a student to commit crimes in this space.

The fifth postulate states that 'strangers are likely to unite together in cyberspace to commit crime in the physical space' while the second part of the postulate reads that

[2] See http://punchng.com/lagos-printer-abducts-rapes-pupil-he-met-on-facebook.

'associates of physical space are likely to unite to commit crime in cyber space. The realities of the computer age are such that students can liaise with strangers in the anonymity and speed provided by cyberspace which have made it easier to meet new people at a freakish rate. They can befriend people they have never met physically in the nooks and crannies of the world. Lenhart et al. (August, 2015) report that teenagers' ability to make friends is no longer confined to the school yard, neighborhood or playground, but extends online. The researcher discovered that fifty-seven percent of teenagers aged thirteen to seventeen had made a new friend online, while only twenty percent of these teenagers had met their friends in person. Students have more virtual or digital friends than the friends they see physically.

Acar (2016, p. 110) corroborates the findings of Lenhart et al. (August, 2015). The structure of the schools utilized for this study in Nigeria was such that students could come together in their school compounds (i.e. physically) to launch assault on perceived foes in cyberspace. The action cybercrime prevention programme showcases the benefits of using education to reorient students on best practices in the cyberspace. The failure of technical solutions provided by computer scientists and information security experts has led to this try-out of education, which is believed to be the missing link in repetitive efforts at securing cyberspace.

3. Urban Learning Ecologies

Despite earlier claims regarding the concept of learning ecologies originating from the works of Looi (2001, p. 14) and Barron (2006, p. 195) by Hlalele (2013, p. 564), Alberti (2008, p. 626) states that the concept of learning ecology featured in the works of Lynch (1981). Lynch (1981, p. 115) recommends that a learning ecology is more suitable for human settlement since some of its players are at least conscious, adept to remold themselves and thus altering the canons of the game. Building on the works of these scholars, Ige (2017 p. 311) defines urban learning ecologies as spaces (schools) in which learning occurs in urban geographical locations. Hlalele (2013, p. 564), drawing on earlier definitions of Looi (2001, p. 14) and Barron (2006, p. 195), highlights the characteristics of a learning ecology as an agglomeration of overlapping communities of interest, cross-fertilizing each other, dynamic and mainly self-organizing. In this study, urban learning ecologies connote secondary schools in urban spaces that supply or give opportunities for acquisition of knowledge, skills and attitudes through study. The schools in urban learning ecologies were selected for this study consequent on the availability of the Internet in the urban spaces which makes them vulnerable to incidences of crime in the cyberspace.

4. Gender and Technological Literacy

Igbo, Onu and Obiyo (2015, p. 1) establish that gender is related to how people perceive themselves in such a way that those of the same sex view themselves with distinct attributes. Previous studies suggest that several factors like usage of social networks, and interactions with families and peers (Ryabov, 2011; Othman & Leng, 2011; Khan, 2012; Ige, 2008) could influence students' attitude. Technological fluency connotes student's interaction with the computer at low, medium and high levels. It is believed that students' usage of technological devices could influence the outcome of this study. Consequent on this, the technological fluency test was used to evaluate the ability of the students to use computers. The low, medium and high technological fluency were randomly distributed to promote group learning during the programme. The focus group discussion also reflects the gender of the participants. The study answers a research question 'What are secondary students' perceptions of the action cyber crime prevention programme?' and tested two hypotheses at 0.05 level. These hypotheses are: 'There is no significant interaction effect of gender and technological fluency on students' attitude to cybercrime prevention', and 'There is no significant effect of treatment, gender and technological fluency on students' attitude to cybercrime prevention.

5. Gymnasiums in Sweden

Scholars have resounded the transformation of the Swedish education system resulting from the alignment of education more closely to the dictates of knowledge capitalism, also known as 'knowledge economy' (Lundahl & Olson, 2013; Ball, 2007). Dovermark and Arreman (2017) explain that the Swedish education system was transformed with the broader aim of increasing economic productivity of the citizens. These transformations culminated in a school market which is closer to the logic of the market than many global school systems (see Chubb, 2007). Gymnasiums in Sweden connote upper secondary or high schools. Arreman (2014) affirm the upper secondary education as the platform for citizens' social and economic self-sustenance. This scholar notes that the new policies for upper secondary education in Sweden include a new curriculum and education act implemented on 1 July 2011 which bolstered the requirements for entry into this level of education. This new policy guaranteed equal standards among Swedish education service providers and raised the level of teaching as well as student's performance (Arreman, 2014; Lundahl, Arreman, Lundstrom, & Ronnberg, 2010; Ministry of Education, 2008).

Prior to the 1990's, Lund (2008) remarked that it was not possible for learners to select any upper secondary school of their choices because the central government educational policies controlled and shaped learners' admission into the twenty-six school programmes through the Country Board of Education. Lund (2008) further explained that the education reformations of 1994 in Sweden led to the evolution of a new curriculum and grading system. The scholar stated that there were seventeen academic programmes of three years duration which included compulsory subjects like social studies, religion, Swedish, physical education, general science, English, mathematics and the arts. This reformation made it possible for learners to select a field of study in their first year in upper secondary education. The outcome of the current study is relevant to the upper secondary schools in Sweden because the 1994 education reformations transformed these schools to a citadel of social order which preserves law and legal order. These reformations empowered schools to file police reports on actions that contravened school rules and regulations (see Ring 2010; Lund, 2008). The action cyber crime prevention programme developed through the social studies and civic education subjects in this study is applicable to the Swedish upper secondary schools because social studies is offered in these 'gymnasiums'.

Methods and Data

a. Design

The participatory action research (PAR) frame was used to put together the cyber crime prevention programme to test the efficacy of the developed programme, which utilizes the experimental design of pretest, post-test, control group of quasi-experimental type. The subjects were selected from intact classes in the experimental and control schools. In the experimental ecologies, teachers who were research assistants were trained on techniques of moderating focus group discussion. A resource person was invited from - University of Ibadan to train the subjects on broad team skills for group activities and collaborative interpersonal dispositions. The training was done to educate the students on the benefits of solving problems in groups' i.e. group learning or cooperative learning. The students were provided with the curricular for civic education and social studies at secondary school level. The themes relevant to cybercrime, and methods of prevention were selected through focus group discussions. The subjects agreed that the programme for preventing crimes in cyberspace among secondary school students should contain societal problems and issues, information and communication technology and its attendant problems, values and non-positive behaviors.

The objectives of the cyber crime prevention programme were defined by the subjects in the experimental ecologies. These are to equip students with the knowledge of information and communication technology as well as cyber security concepts, to orientate students on the ills of crimes committed in cyberspace, to empower students to demonstrate their citizenship duties and obligations when utilizing the Internet or interacting in cyberspace, to equip students with the requisite skills necessary for preventing crimes in cyberspace and develop civic virtues like team work, empathy, etc.

The subjects went on to establish clubs in the experimental learning ecologies to prevent crimes committed in cyberspace by students, drafted a constitution to regulate the conduct of members, held executive meetings, invited academics, a court judge, a lawyer, law enforcement officials, and used staged drama and debate to actualize the contents of the cyber crime prevention programme. During the focus group discussion, the subjects agreed to put up a notice board for displaying initiatives to prevent crimes in cyberspace, hoisted banners and got a public-address system. The research assistants harmonized the suggestions of the focus group in the experimental schools through voting or consensus.

The teachers teaching social studies as well as civic education in the experimental schools were interviewed on the method used to teach the themes selected by the subjects for preventing crimes in cyberspace. Their responses showed that the conventional lecture method was the mode of teaching used to teach the selected concepts for cybercrime prevention. This led to the preparation of lecture modules on the concepts selected by the experimental groups and given to teachers in three secondary schools in other geographical locations to teach learners offering social studies and civic education in the common level of schooling i.e. junior secondary school level 2. These three schools were used as the control for the experimental schools.

b. Participants Selection and Sample

The subjects were 218 junior secondary school students in level two; 426 students commenced the study, but only 218 subjects attended all the weekly experimental activities. 75 of these students were in the experimental group, while 143 were in the control group that utilized the conventional lecture method. 108 were male while 110 were female. 98 were of low technological fluency, 86 were of moderate technological fluency, while 34 were of high technological fluency.

c. Ethical Considerations

The management of the selected schools approved the conduct of this research project after receiving adequate information from the researcher. The participating students got the permission of their parents to participate in the study following the after-school period of the experimental activities which lasted for ten weeks. The schools and students selected for the study offered social studies and civic education at the Junior School level. The students were assured that they were free to disengage from the experimental activities at any time they so wished before the completion of the research project.

d. Questionnaire and Measures

Three of the instruments used to evaluate the variables of interest in the study were developed by the researcher; one was developed by the students; while one was adapted from the North American Division of Seventh-Day Adventists (2009). The instruments developed by the researcher were: the focus group discussion guide, conventional lecture method guide, students' perception of the action cyber crime prevention programme questionnaire, and students' attitude to the cybercrime prevention questionnaire. The subjects developed the action cyber crime prevention programme while the technological literacy and competency test was adapted from the North American Division of the Seventh Day Adventists Office of Education.

The focus group discussion outline was put together to aid the subjects to determine the contents of the cybercrime prevention programme. The guide was tried out using students in junior secondary schools that were not part of the study. The content that the students found unclear was reworked before the commencement of the study. The test was designed in 2005 but reviewed in 2009. The first part has sixty questions while the second part has ten. The questions were administered among the students that were not part of the study for reliability. Only thirty-eight questions were used for the study after determining the difficulty index of the questions. The reliability co-efficient was 0.78 using KR-20.

The students' perceptions of the action cybercrime prevention programme questionnaire, a 4-point likert type instrument elicited the subjects' perceptions of the developed programme. The instrument was used to evaluate the perceived benefits of the developed programme by the subjects. The students' attitude to the cyber-crime prevention programme questionnaire was designed to evaluate the dispositions of the subjects to prevention of crimes in cyber space. The 4-point likert-type instrument has twenty-two items that were evaluated. The achievement of basic cyber security attitudes, appropriate skills and values for active cyber security, and cyber policing in subjects' environment were attained. The reliability coefficient was 0.76 after trying it out on students that were not part of the study. The action programme was put together by the subject through experiment activities that lasted for ten weeks. The contents were societal problems and issues, information and communication technology and its attendant problems, values, and non-positive behaviors. The process used by the subjects to develop the action programme was derived from Roberts (2007). The planning of the programme began with the training of the focus group moderators and interviewing of the subjects established the contents of the prevention program using action strategies. This was done collaboratively during focus discussion (Ige, 2012). The subjects validated the contents of the action cybercrime prevention programme through the establishment of a club, use of a resource person for cybercrime prevention lectures, drama and debate.

The conventional lecture method module guided the teachers in the control group. The module was written on each of the concepts in the contents of the action cyber crime prevention programme. The teachers in the control group taught these concepts for eight weeks while pretest and post-test look place, before the commencement of teaching and at the completion of teaching activities. The module empowered teachers in the three selected schools to introduce the selected concepts, discuss the concepts in sequence, write notes on the concepts, ask questions and elicit answers, and give homework to the subjects in the control group.

e. Variables in the Study

These variables are in the study: Gender was a variable which described the societal beliefs about the effect of sex stereotype on learning outcome of male and female children. Technological fluency connoted subjects' abilities to deploy technological tools and constructively utilize them significantly. Technological fluency was manipulated at three levels namely low technological fluency, average technological fluency and high technological fluency which were the moderator variables that the researcher controlled in the study. The independent variable was manipulated at two levels namely: action cyber crime prevention programme and conventional lecture method. The dependent variable was students' attitude to cybercrime prevention which connotes the subjects' disposition to the prevention of crime occurrence in cyber space.

f. Data Analysis

Descriptive statistics such as percentage, frequency counts, mean and standard deviation were used to analyze the data collected on students' perceptions. I further used a 2x3x2 full factorial ANCOVA model to test the hypothesis. Analysis of covariance enabled the researcher to explore the effect of the categorical independent variables (action cyber crime prevention programme and conventional lecture method) and a metric dependent variable, especially the interaction effect between the moderator and dependent variables. The model used a statistical test that parceled out the initial disparities in the pretest scores. The significant p values of the test enabled the researcher to reject the null hypothesis that the means of the dependent variables were the same across groups. Assumptions for conducting analysis of covariance were met as there were no statistically significant differences at base line between the treatment and control group for the statistical analysis; the alpha level was put at $p<0.05$, while the partial eta square (η^2) indicated the effect size (Richardson, 2011; Piwowar et al., 2013; Ige & Hlalele, 2017). Scholars have affirmed that the effect size is adjusted to be large at 0.14, moderate at 0.06, and small at 0.01 (Cohen, 1988; Piwowar et al., 2013; Ige & Tsotetsi, 2017)

Results

The results and discussion sections are organized to show the perceptions of subjects about the action cyber crime prevention programme, pre-test and post-test, showing the effectiveness of the action cyber crime prevention programme, and the graphical illustration of the interaction effect.

Research Question: What are secondary students' perceptions of the action cyber crime prevention programme?

Table 1. Students' Perceptions of Action Cyber Crime Prevention Programme (N= 75)

S/N		Strongly Agree		Agree		Disagree		Strongly Disagree		Mean	Std. Dev
		F	%	F	%	F	%	F	%	X	S.D
1	Action cyber crime prevention programme will help students to stop obtaining goods and services without paying on the Internet.	60	80.0	7	9.3	1	1.3	7	9.3	3.60	0.92
2	Action cyber crime prevention programme will help students to stop accessing sex websites.	68	90.7	6	8.0	-	-	1	1.3	3.88	0.43
3	Action cyber crime prevention programme will enable students to understand the dangers of using another person's name and social security number to obtain goods and services on the Internet.	64	85.3	6	8.0	2	2.7	3	4.0	3.75	0.69
4	Action cyber crime prevention programme can help students doing 'Yahoo Yahoo' to turn a new leaf.	52	69.3	6	8.0	1	1.3	16	21.3	3.25	1.23
5	Action cyber crime prevention programme can educate students to turn down terrorists who use Internet to further their agenda.	57	76.0	9	12.0	2	2.7	7	9.3	3.55	0.93
6	Action cyber crime prevention programme can educate students to stop sending electronic mails to solicit for money in Dollars ($), Pounds (£) and Euro (€) from people abroad.	63	84.0	10	13.3	2	2.7	-	-	3.81	0.46
7	Action cyber crime prevention programme will educate students who leave school for Internet Café to do ('Yahoo Yahoo') to stay in school	55	73.3	4	5.3	5	6.7	11	14.7	3.37	1.12
8	Action cyber crime prevention programme will educate students from poor homes not to engage in 'Yahoo Yahoo'.	63	84.0	3	4.0	1	1.3	8	10.7	3.61	0.96
9	Action cyber crime prevention programme will educate students to stop the act of sending an email to internet users falsely claiming to be established legitimate enterprises to scam the users	57	76.0	11	14.7	1	1.3	6	8.0	3.59	0.87

	into surrendering private information that will be used for identity theft.										
10	Action cyber crime prevention programme will educate students on the dangers inherent in buying goods and services on the Internet without paying.	57	76.0	9	12.0	2	2.7	7	9.3	3.55	0.93
11	Action cyber crime prevention programme will help students to know that 'Yahoo Yahoo' amounts to stealing from other people.	54	72.0	7	9.3	2	2.7	12	16.0	3.37	1.12
12	Action cyber crime prevention programme will educate students not to use special hacking software that could record the sequences of key strokes that computer user makes on their key boards or infiltrate internet banking	54	72.0	10	13.3	4	5.3	7	9.3	3.48	0.96
13	Action cyber crime prevention programme is another waste of time that will not prevent students from doing 'Yahoo Yahoo'.	57	76.0	6	8.0	2	2.7	10	13.3	3.47	1.06
14	Action cyber crime prevention programme will not stop students from accessing sex websites.	59	78.7	8	10.7	-	-	8	10.7	3.57	0.95
15	Action cyber crime prevention programme will not stop students from persuading people to invest relatively small amounts of money with the promise of giving a larger amount of money later on the Internet.	32	42.7	6	8.0	5	6.7	32	42.7	2.51	1.41
16	Action cyber crime prevention programme will educate students not to join 'Yahoo Boys' Club	60	80.0	6	8.0	-	-	9	12.0	3.56	0.99
17	Action cyber crime prevention programme will educate students to dissociate from friends who do 'Yahoo Yahoo'	61	81.3	6	8.0	1	1.3	7	9.3	3.61	0.91
18	Action Cyber Crime Prevention Club cannot end the menace of 'Yahoo Yahoo' in Nigerian secondary schools	54	72.0	6	8.0	3	4.0	12	16.0	3.36	1.13
Weighted Average= 3.49											

Table 1 shows that the perceptions of the students yielded high mean scores for all the 18 items. The lowest score is 2.51 (item 15) while another mean scores ranged from 3.25 (item 4) to 3.88 (item 2). These high mean scores show that the students' perceptions of the Action cyber crime prevention programme are quite positive. The high weighted average of 3.49 also lends credence to this finding.

Table 2. Summary of ANCOVA of Posttest Attitude Scores by Treatment, Gender and Computer Literacy

Source of Variance		Hierarchical Method				
		Sum of Squares	Df	Mean Square	F	Sig
Covariates	PREATT	8029.586	1	8029.586	109.949	.000
Main Effects	(Combined)	12021.196	4	3005.299	41.151	.000
	TREATMENT	11618.533	1	11618.533	159.092	.000*
	GENDER	8.055	1	8.055	.110	.740
	TECH. FLUENCY	394.609	2	197.304	2.702	.069
2-Way Interactions	(Combined)	711.911	5	142.382	1.950	.088
	TRTMENT *	4.283	1	4.283	.059	.809
GENDER		151.950	2	75.975	1.040	.355
	TRTMENT *	465.427	2	232.713	3.187	.043
TECHFLU		81.894	2	40.947	.561	.572
	GENDER *					
TECHFLU		20844.587	12	1737.049	23.785	.000
3-Way Interactions		14971.193	205	73.030		
TRTMENT*GENDER*		35815.780	217	165.050		
	TECHFLUENCY					
Model						
Residual						
Total						

* Significant at $p < 0.05$

Table 2 reveals that there is a significant two-way interaction effect of gender and technological fluency on students' attitude to cyber crime prevention ($F_{(2,217)} = 3.187$; $p<.05$). This made for the decision to reject the null hypothesis. This significant interaction effect is explained in figure 4.

Figure 4. Interaction Effect of Gender and Technological Fluency on Students' Attitude to Cyber crime Prevention

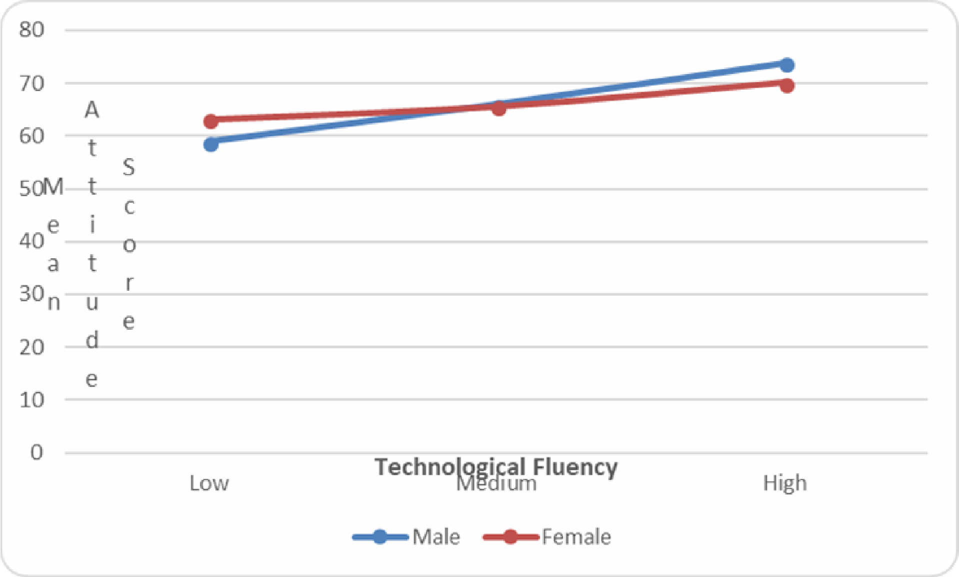


Figure 4 reveals that in the group of students with low technological fluency, female students' attitude scores were higher than male students attitude score. The male students performed better than female students with moderate and high technological fluency. The interaction presented on Figure 4 is disordinal because the difference observed in for male and female is different for the low technologically fluent students compared to the average and high technologically fluent students. Despite these differences, the gaps between male and female students across the low, average, and high technological levels were contiguous.

Table 2 shows that the three-way interaction effect of treatment, gender and technological fluency on students' attitude to cyber crime prevention is not significant ($F_{(2,217)} = .561$; $p > .05$). On this basis, hypothesis two is not rejected.

Discussion and Conclusion

The outcomes of this participatory intervention show that:

i. The perceptions of the students yielded high means scores for the eighteen statements that evaluated students' perceptions of the intervention programme.
ii. The two-way interaction effect of gender and technological fluency on students' attitude to cyber crime prevention was significant.
iii. The three-way interaction effect of treatment, gender and technological fluency on students' attitude to cyber crime prevention was not significant.

The current study developed and evaluated a humanistic programme for protecting students in cyberspace. To achieve this purpose, the researcher utilized a participatory curriculum model in active collaboration with students to achieve responses to cyber security issues. It was unlike other cyber security programmes developed by computer scientists and information security professionals, which omitted attitudes necessary for cyber security. The positive effects of gender and technological fluency on students' attitude to cyber crime prevention recorded in this study may be due to these reasons: First, the repetitive ranking of Nigeria, the country where this study was conducted, as a cyber scam hub (National White Collar Crime Center, 2010). The students conceived the study as a channel to remake the image of Nigeria as a cyber-lawful country in the comity of nations. The report that seventy-six percent of internet scam perpetrators were males might have accounted for the dedication observed from the male subjects during the study (National White Collar Crime Center, 2010). The Internet security programmes currently used are handed to end users without participation in the development process. The action programme developed in this study was evaluated by learners to ascertain their perceptions of the new programme. The need to evaluate the subjects' perceptions of the prevention programme was premised on Huey, Nhan and Broll (2012) that the distributive style of the fourth revolution in education (i.e., Internet, see Ige, 2012) demanded that safety issues be tackled through participatory/cooperative efforts by public and private users. The participatory nature of this study aims to equip students with the requisite attitudes necessary to handle cyber security issues when using the Internet.

Another noteworthy outcome of this study is the significant influence of gender and technological fluency on students' disposition to prevent crimes in cyberspace. The performance across gender boundaries shows that the quasi-experimental design enabled male subjects to have a higher attitude adjustment than female subjects. Further, subjects with technological fluency had advantage over moderately fluent and lower technologically fluent subjects. Despite the action nature of the prevention programme, the ability of the subjects to maneuver the computer technology greatly accounted for the development of collaboration.

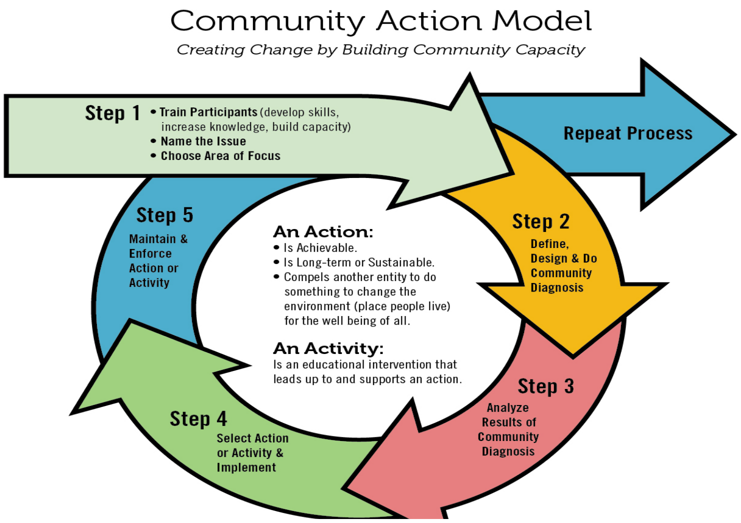
The Federal Bureau of Investigation on the gender dimensions of incidences of cybercrimes confirmed the findings of Adu and Ige (2016) that male school-aged children engaged more in cyber lawless activities than female school-aged children. Despite the observed influence of gender and technological fluency on students' attitude to the prevention of cyber crimes in this study, the interaction effect of treatment, gender and technological fluency had no consequential impact on the dependent variable. Previous studies related to action intervention programmes were inconclusive on the interaction effects of such programmes alongside the accompanied confounding variables. Reidel (2002) states that many schools have adopted action service programmes to promote citizenship as a means of collective action to address social quandaries. Riedel's study indicates that self-selection appears to play a paramount role in determining what students benefit from action service programmes. Another study conducted by health service professionals which combined a service learning programme with a university course in gerontology emerged with conflicting findings (Yamashita, Kinney, & Lokon, 2011). The outcome of this study indicates significant changes in the behavioral domains of subjects. Subjects who completed the gerontology course as well as subjects who concluded the service learning programme in addition to the gerontology had a higher post-attitude change than subjects in other social science courses. From the experiment conducted by Yamashita et al. (2011), it seems the interaction effect of the intervention programmes and moderator variables in this study would have been different if a third experimental group has been put together to use the programmes interchangeably with conventional lecture method, i.e. blending.

Lessons for Swedish Upper Secondary Schools

Mjomark (November, 2016) reports that internet use among Swedish children is on the rise. Mjomark reports that fifty percent of girls aged eleven have been discovered to be more occupied on the social networking websites than males. It was also discovered that girls aged 12 to 15 years get into trouble especially bullying more often when communicating in cyberspace. Researchers should note that the age group specified by Mjomark (November, 2016) is peculiar to upper secondary school students in Sweden. The scenario pointed out by this reporter is similar to the situation in Nigeria, which was not given attention and it thereby escalated. Recent estimates show that mobile internet user penetration rate in Sweden would hit 91.52% of the total population in 2021.[3] This increase of 23% from the 73.57% internet user penetration rate in Sweden makes the upper secondary school students, especially females, more vulnerable to cyber bullying and other ills perpetrated using the Internet

The Local (October, 2012) reports that cyber attacks rarely results in convictions in Sweden, because the regulations promulgated in Sweden are for the analog era. The rate of incidences of cyber crime in Sweden oscillated between eleven and fifteen thousand crimes per 100,000 of the residents in the previous two decades, the Swedish government said in response to attacks' on the Swedish national police and other government websites attacks. Cyber attackers found culpable might get two to ten years behind bars (secure64, 2006).

Figure 5.


Community Action Model
Creating Change by Building Community Capacity
Step 1
• Train Participants (develop skills, increase knowledge, build capacity)
• Name the Issue
• Choose Area of Focus
Repeat Process
Step 2
Define, Design & Do Community Diagnosis
Step 3
Analyze Results of Community Diagnosis
Step 4
Select Action or Activity & Implement
Step 5
Maintain & Enforce Action or Activity
An Action:
• Is Achievable.
• Is Long-term or Sustainable.
• Compels another entity to do something to change the environment (place people live) for the well being of all.
An Activity:
Is an educational intervention that leads up to and supports an action.

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.

[3] See https://www.statista.com/statistical567967/predicted-mobile-internet-user-penetration-rate-in-sweden).

The new laws promulgated by Sweden are aimed at ameliorating the incidences of cyber crime. While this is a step in the right direction, research (Ige, 2013) has however shown that the law only cannot serve as a brake to the incidences of cyber crimes emanating from the nooks and crannies of the world. It is on this premise that this study is proposing the use of education to complement the new laws promulgated to tackle the incidence of cyber crimes in Sweden. The proposed prevention model for Sweden is illustrated in Figure 5.

The model shows that while the criminal might initiate his/her cyber attacks, prior education of an upper secondary school students will keep him/her safe, and not vulnerable to the cyber scammer. The community action model designed by Lavery, Smith, Esporza, Hurshow, Moore and Reed (2005), as against the Roberts (2007) model used to develop the contents of the cyber crime prevention educational programme in this study, is proposed for designing the intervention for upper secondary school students' in Sweden.

The model is illustrated below:

To use the model among upper secondary school students in Sweden, the sequential steps are recommended.

Action i

Train the students on collaborative learning and endeavors. The expert facilitator will need to develop the collaborative skills of the students to build capacity and upgrade the knowledge of the participating students. The students should collaboratively name the issue e.g. cyber security education and choose an area of focus e.g. cyber bullying.

Action ii

The participating students should engage in focus group discussion to establish the primary causes of cyber lawlessness in Sweden and outline the stratagem to overcome the menace.

Action iii

The researcher and focus group discussion leaders note and prepare findings.

Action iv

The focus group leaders disseminate the findings to the students. The focus group discussants select, plan and implement participatory activities to address cyber lawlessness in Sweden. Lavery et al. (2005) added that the action activities should be achievable, sustainable, and compel the group of students to change their community (Sweden) for the well-being of all.

Action v

The participating students maintain and enforce the participatory cyber security education programme through the establishment of a school club e.g. cyber security education club.

The findings of this study strongly reinforce the need for educational intervention to ameliorate the incidence of cyber crimes across the globe. As sterling as these findings are, the sample of two hundred and eighteen students that survived during the period of the study lasted is limited to six secondary schools in Nigeria. For the generalization of the findings of this study to a developed nation, the term cyber security education is more appropriate than cyber crime prevention which is peculiar to the developing and less developed nations. It was evident from previous incidence of cyber crimes that the less developed nations were the perpetrating countries, while the countries with good and robust economy wellbeing or health were the target or marked countries.

Acknowledgements and Disclaimer

I sincerely appreciate 'Olusayo' my wife of 'five happy years' who burnt the midnight lamp to type this research work. I also sincerely thank The SANRAL Chair in Science, Mathematics and Technology Education at the University of the Free State that funded my Postdoctoral Research Fellowship, on which this study is based. Some components of my post doctoral research have been presented at conferences and published by a leading journal in the field of education and information technologies.[4] *The aspect documenting gender and technological fluency in this study have not been presented in any conference or submitted for publication elsewhere. The funding university was not involved in the design of the research, analysis of data as well submission of the research article. The author bears sole responsibility for the opinions expressed and any errors that accompany them in this research article.*

References

Acar, K. V. (2016). Sexual extortion of children in cyberspace. *International Journal of Cyber Criminology*, *10*(2), 110-126.

Alberti, M. (2008). *Advances in urban ecology: Integrating humans and ecological processes in urban ecosystems*. Springer Science+Business Media, LLC. ISBN 978-0-387-75509-0.

Arreman, I. E. (2014). Student perception of new differentiation policies in Swedish post-16 education. *European Education Research Journal*, *13*(6) 616-631.

Ball, S.J. (2007). *Education plc: understanding private sector participation in public sector.* Abingdon, Oxon, New York: Routledge.

Barron, B. (2006), Interest and self-sustained learning as catalysts of development: A learning ecology perspective. *Human Development Paper*, *49*,193-224.

Brunton, F. (2013). *Spam: A Shadow History of the Internet.* Cambridge, MA: MIT Press, 2013. pp. 1-296.

Chubb, J. E. (2007). *Kommentar: Att få ut det mesta möjliga av marknaden [Comment: How to gain the most possible from the market]*, in A. Lindbom (Ed.) Friskolorna och framtiden: segregation, kostnader och effektivitet [Free schools and the future: segregation, costs and efficiency], pp. 51-57. Stockholm: Institutet för framtidsstudier.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588-608.

Dovemark, M., & Arreman, I. E. (2017). The implication of school marketisation for students enrolled on introductory programs in Swedish upper secondary education. *Education, Citizenship and Social Justice*, *12*(1), 49-62.

EC-Council. (2017). *Sweden. Information security landscape.* Retrieved from

[4] See www.eujournal.orh/index.phplesj/article/download, https://library.iated.org/view/AMOSUN2014NIG, and https://link,springer.com/article/10,1007/s10639-013-9298-0.

https://eccouncil.org/international-cyber security/Sweden.

Esen, R. (2002). Cybercrime: A growing problem. *The Journal of Criminal Law*, *66*(3), 269-283.

Folarin, S. (25 May 2018). Lagos printer abducts, rapes pupil he met on Facebook. Retrieved from http://punchng.com/lagos-printer-abducts-rapes-pupil-he-met-on-facebook.

Hlalele, D. (2013). Sustainable rural learning ecologies-a prolegomenon transversing transcendence of discursive notions of sustainability, social justice, development, and food sovereignty. *TD The Journal for Transdisciplinary Research in Southern Africa*, 9(3), 561-580.

Huey, L., Nhan, J & Broll, R. (2012). 'Uppity civilians and cyber-vigilantes'. The role of the general public in policing. *Criminology & Criminal Justice*, *13*(1), 81-97.

Adu, O. E., & Ige, O. A. (2016). *Secondary school teachers' perceptions of incidences of cyber crimes among school-aged children in Lagos State, Nigeria*. In Van Niekerk, J. F. (eds)., Proceedings of the African Cyber Citizenship Conference 2016 (ACCC 2016). Nelson Mandela Metropolitan University, 61-84.

Igbo, J. N, Onu, V. C., & Obiyo, N. O. (2015). Impact of gender stereotype on secondary school students' self-concept and academic achievement. SAGE Open, January-March, 21-10.

Ige, O. A., & Hlalele, D. J. (2017). Effects of computer-aided and blended teaching strategies on students' achievements in civic education concepts in mountain learning ecologies. *Educ Inf Technol*, *22*(6), 2693-2709.

Ige, O. A., & Tsotetsi, C. T. (2017). Effects of computer aided and blended teaching strategies on students' civic attitudes in rural learning ecologies: A model for South Korea rural schools. *The Anthropologist*, *29*(2), 170-177.

Ige, O. A. (2012). *Action cybercrime prevention programme in civics and social studies: the Nigeria experience*. Lambert Academic Publishing, Germany. ISBN 978-3-659-14758.

Ige, O. A. (2017). Rethinking students' dispositions towards civic duties in urban learning ecologies. *International Journal of Instruction*, *10*(4), 1308-1470.

Ige, O. A. (2008). *Secondary School Students' Perceptions of Incidences of Internet Crimes among School Age Children in Oyo and Ondo States, Nigeria*. A Master dissertation in the Department of Teacher Education, University of Ibadan, Nigeria.

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.

Khan, A (2012). Sex difference in educational encouragement and academic achievement. *Psychological Reports: Mental & Physical Health*, *111*(1), 149-155.

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.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel J., Roberts, L. G., & Wolff, S. (2003). A brief history of the Internet. Retrieved from https://cdn.prod.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf.

Lenhart, A., Smith, A., Anderson, M., Duggan, M. & Perrin, A. (August, 2015). Teens, Technology, and Friendships. Pew Research Center. Retrieved from http://www.pewinternet.org/2015/08/06/teens-technology-and-friendships.

Liang, B., & Liu, H. (2010). Internet development, censorship, and cyber crimes in China. *Journal of Contemporary Criminal Justice*, *26*(1), 103-120.

Looi, C. K. (2001). Enhancing learning ecology on the Internet. *Journal of Computer Assisted Learning*, *17*(1), 13-20.

Lund, S. (2008). Choice paths in the Swedish upper secondary education- a critical discourse analysis of recent reforms. *Journal of Education Policy*, *23*(16), 633-648.

Lundahl, L., & Olson, M. (2013). Democracy lessons in market-oriented schools; the case of Swedish upper secondary education. *Education, Citizenship, and Social Justice*, *8*(2), 201-213.

Lundahl, L., Arreman I. E., Lundström, U., & Ronnberg, L. (2010). Setting things right? Swedish upper secondary school reform in a 40-year perspective. *European Journal of Education*, *45*(1), 46–59.

Lynch, K. (1981). *A theory of good city form*. Cambridge, MA: MIT press.

Metcalf, L.C. (1971). *Values education: Rationale, strategies and procedure*. Washington, B.C. National Council for Council for Social Studies.

Ministry of Education (2008a). Government bill 2008/09:199. Högre krav och kvalitet i nya gymnasieskolan. Retrieved from http://www.riksdagen.se/sv/Dokument-Lagar/Forslag/Propositioner-och-skrivelser/Hogre-krav-ochkvalitet-i-den-_GW03199/?text=true. Stockholm: Ministry of Education.

Mjomark, P (November, 2016). The Swedes and the Internet 2016. The Internet foundation in Sweden, Stockholm. Retrieved from https://www.iis.se/english/blog/the-swedes and the internet-2016.

North American Division of Seventh-Day Adventists (2009). Computer literacy and competency test. Retrieved from http://www.nadventist.orglartide/1073742477/ministries/education.

Othman, N., & Leng, K. B. (2011). The relationship between self-concept, intrinsic motivation, self-determination and academic achievement among Chinese primary school students. *International Journal of Psychological Studies*, *3*(1), 90-98.

Reidel, E. (2002). The impact of high school community service programs on students' feelings of civic obligation. *American Politics Research*, *30*(5), 499-527.

Ren, F., Kwan, M., & Schwanen, T. (2013). Investigating the temporal dynamics of Internet activities. *Time & Society*, *22*(2), 186-215.

Richardson, J. (2011). Eta squared and partial eta squared as measures of effect size in educational research. *Educational Research Review*, *6*(2), 135-147.

Ring J. (2010). *Brott bland ungdomar i a˚rskurs nio: resultat fra˚n skolunderso¨kningen om brott a˚ren 1995– 2008* (Crime among young people in grade nine: Results from the national survey of crime 1995– 2008). Stockholm: Brottsfo¨rebyggande ra˚det.

Roberts, M.R. (2007). *Curriculum Development Process*. Northern Arizona, CTE 592.

Ryabov, I. (2011). Peer networks, generational status, and achievement of American adolescents. *Journal of Educational and Developmental Psychology*, *1*(1), 105-117.

Secure64 Software Corporation (November, 2006). Really old news-UK and Sweden enact laws against cyber crimes. Retrieved 29 July 2017 from https://secure64.com /really-old-news-uk- sweden-enact-laws-cyber-crimes.

Statista. (2017). Forecast of the mobile internet user penetration rate in Sweden from 2014 to 2021. Retrieved from https://www.statista.com/statistics/567967/ predicted-mobile internet-user-penetration-rate-in-sweden.

The Local. (October, 2012). Sweden seeks tougher penalties for hacking. Retrieved from https://www.The local.se/20121010/43722.

The National White Collar Crime Center (2010). 2009 Internet crime report. Retrieved from https://pdf.ic3.gov/2010-ic3Report.pdf

The National White Collar Crime Center (2016). 2010 Internet crime report. Retrieved 27 July 2017 from https://pdf.ic3.gov/2010-ic3Report.pdf.

Townes, M. (2012). The spread of TCP/IP: How the Internet became Internet? *Millenium: Journal of International Studies*, *41*(1), 43-64.

Wick, S. E., Nagoshi, C., Basam, R., Jordan, C., Kim, Y. K., Nguyen, A. P., & Lehman, P. (2017). Patterns of cyber harassment and perpetration among college students in the United States: A test of routine activities theory. *International Journal of Cyber Criminology*, *11*(1), 24-38.

Yamashita, T., Kinney, J. M., & Lokon, E. J. (2011). The impact of a gerontology course and a service learning program on college students' attitudes towards people with dementia. *Journal of Applied Gerontology*, *32*(2), 139-163.