# IMPACT OF AN ACTION CYBER CRIME PREVENTION PROGRAMME ON IN-SCHOOL AGED CHILDREN'S ATTITUDE TO CRIME PREVENTION CONCEPTS IN CIVIC EDUCATION AND SOCIAL STUDIES

Peter Adewale Amosun
University of Ibadan, Ibadan
Olugbenga Adedayo Ige
Adekunle Ajasin University, Akungba Akoko

#### **Abstract:**

This study evaluated the impact of a participatory cyber crime prevention programme on inschool aged children's attitude to cyber crime prevention in Nigeria, consequent on the global annual ranking of Nigeria as one of the most cyber lawless countries by The National White Collar Crime Center and Federal Bureau of Investigation in the United States of America. The study used the participatory action research paradigm to develop an informal cyber crime prevention programme, and further utilized pretest-posttest quasi experimental design to evaluate the impact of the action cyber crime prevention programme on secondary school students' attitude in Civic Education and Social Studies. The sample of the study comprised two hundred and eighteen students purposefully selected from intact classes in six secondary schools in Nigeria. Percentages, Mean, Standard Deviation and Analysis of Covariance (ANCOVA) were used to analyze the data. Multiple Classification Analysis aspect of ANCOVA was used to determine the magnitude of performances across the groups, while line graph was used to disentangle significant the interaction effects. Results showed that there is significant main effect of treatment on in-school aged children's attitude to cyber crime prevention in civic education and social studies. Consequent on these, the study recommended the use of Action Cyber Crime Prevention Programme for developing countries experiencing the menace of cyber crimes perpetrated by school-age children.

**Key Words:** Impact, Action Cyber Crime Prevention Programme, In-School Aged Children, Learning Outcomes, Social Studies, Civic Education

# Introduction

The new Social Studies and Civic Education curriculum that was put together in year 2007 reflect depth, appropriateness and interrelatedness of the contents of the curriculum. Emerging issues which covered value reorientation, peace and dialogue including human rights education, family life HIV/AIDS education, entrepreneurial skills, crime prevention themes and Information and Communication Technology (ICT) were infused into the relevant contents of the new 9-year basic education curriculum (NERDC, 2007). Adesina and Adeyemi (2007) stated that the field of Social Studies has come to stay in Nigerian primary and secondary schools, as such the importance attached to its study cannot be exaggerated. It is believed to be the correct drug that can be used to heal the ailment of moral decadence (Cyber Crime) and instill in the youth a sense of decent behaviour (Cyber Crime Prevention). To this end, the objectives of Social Studies specifically are to enable the children develop an understanding of their immediate surroundings; develop certain skills which will enable the children to deal with and manage the forces of the world in which they live; and learn how to live harmoniously where many different groups co-exist (Obidoa, 1991). Adesina and Adeyemi (2007) further clarify that Social Studies can be seen as a programme of study in Nigerian secondary schools which is used to inculcate in learners the knowledge, skills, attitude and actions considered important in human relationship in society. These are reasons why Action Cyber Crime Prevention Programme will best be taught through Social Studies and Civic Education. Comparative Education Study and Adaptation Centre (1993) defines Social Studies as a subject concerned with the way man lives in and

interacts with his social and physical environments and how science and technology, for instance, computer, help him to live well in those environments.

In addition to these, the Internet Crime Reports of year 2001 to 2010 published by the National White Collar Crime Center and the Federal Bureau of Investigation in the United States of America show the extent to which Nigerians perpetrate cyber crimes. Table 1 show the top ten countries in the world whose citizens are enmeshed in cyber crimes from year 2001 to 2010.

Segments  Segments  Segments  Segments  Segments  Segments  Segments	5. 2.75: 2.25: 0.85:	2-4 2-4	2.7%	2 m2	2.0%	1-0	56		56		56		56						1010 02.8%	
Rigeria orada formania initiad Konglian	5. 2.75: 2.25: 0.85:	2-4 2-4	2.1% 2.2% 1.7%	2 m2	2.0%	1-0	56		56		56		56							
Regards Smalls Smalls Small Kingdown	2.7% 2.2% 0.8%	and one	1.2% 1.7%	2+0	115		2.27%	2-0	7.8%	7-0	-		-							
Comments Sectional Recognition	0.0%	enn	2.7%								2.8%	200	2.7%	3+0	7.2%	3-0	2.0%	1-0	22%	2140
interd Kongdom				9530													2.0%	enn	2.4%	10
	0.8%	enn			3.2%	7700	0.00%	7100	0.756	220	3.000	200	3.2%	200	0.3%	<b>BCD</b>	-		-	
Control of the last			-		1.8%	210	2.82%	enn	0.2%	1-0	2.0%	enn	200	1-0	10.3%	1-0	1.15	2	10.6%	100
	0.3%	ecn			3.1.	ecn.	-		1.0%	210	0.0%	1010	0.00	710	0.7%	ocn	0.7%	200		П
indicate	0.6%	710	0.8%	pen	-				-		-		-		-		0.3%	3,000	0.3%	10
of contract of	DAS:	220	0.3%	3,000	-		-		-		-		-		-		-		-	
Sep. 1	D.B.S.	men.	D.756	2100	-		-		-		-		-		-		-		-	
unada (	0.1%	1000	1.1%	200	-				0.7%	220	1.1%	220	0.2%		-		-		-	
	-		0.0%		1.4%		0.0%				-		0.000	219	0.0%	2-	0.7%	200	0.2%	100
	-		D.D/b	2230	0.8%				-		2.2%				-		-		-	
_	-						2.01%						1.1%	acn	0.3%	ecn.	-		-	
	-				113	220					0.7%	ecn.	-		-		-		-	
	-				-		0.00%			1000	-		-		-		-		-	
	-				-		0.20%				-		-		-		-		-	
-	-		-		-		0.38%	n	1.1%	acn.	-				1.0%					**
The same of the sa	-				-				-		-		0.756	1000	0.0%	220			0.7	2.0
diagnia P	-				-				-		-		-		-		0.7%	200	0.2%	1.5

Source: 103 2001 – 2009 internet Grime Reports (January 1, 2001 to December 31 2010) prepared by the National White Coller Crime Center and the Federal Bureau of Investigation.

Table 1 show that Nigeria was second in year 2001 among the top ten countries noted for cyber crimes with 2.7%. In year 2002, Nigeria retained the second position with 5.1% while Nigeria was third with 2.9% in year 2003. In year 2004, Nigeria still maintained the third position with 2.87% even though this year recorded the lowest perpetration of internet crimes involving Nigerians. In year 2005 Nigeria moved to second position with 7.9%, and third repeatedly in years 2006, 2007, 2008 and 2009 with 5.9%, 5.7%, 7.5% and 8.0% respectively. In year 2010, Nigeria retains the third position with 5.8%, Table 1 shows a downward trend in the perpetration of scamming activities by Nigerians in 2010. This decline may not be unconnected with austere conditions caused by the global economic meltdown. Internet fraudsters could only thrive when the economic conditions of the target (mark) countries are in good condition. However, it should be noted that the Internet Crime Reports only shows the ten most cyber lawless countries and leaves out the remaining countries below the global top ten mark.

For educational researchers, the need to protect children from the dangers posed by cyber crimes has become imperative. It is most unfortunate that over ninety percent (90%) of 8 to 16years old in the category mentioned earlier viewed pornography online while doing home work (Chiemeke and Longe, 2007). Although empirical data about cyber crimes and its impact on the life of the teeming youth and children are not readily available, fears are already very rife in some sectors about the possible negative consequences obnoxious and uncensored Internet contents will have on the psycho-social wellbeing of varying categories of users, especially school-age children in Nigeria.

The Internet is both a source of prospect for school-age children in Nigeria and a source of concern. The prospect is that the Internet offers such an enormous range of positive educational experiences and materials. Yet, children online may not only be vulnerable to harm through exposure to sexually explicit materials, adult predators and peddlers of hate, but also perpetrate any of these crimes while on the Internet. The technical nature of the Internet has not evolved in a way that makes control over content easy to achieve (Dick and Herbert, 2003). It has become imperative for educational researchers to evolve protective schemes like Action Cyber Crime Prevention Programme for Internet savvy children and teenagers in a country where the struggle for survival keeps parents at work while having little or no time to monitor what their children do with the Internet at home, in their schools and other Internet access points.

# **Theoretical Framework**

This study is based on the constructivist theory of learning which provides the theoretical base for the participatory action research paradigm adopted for this study, space transition theory, which is a criminological theory that take cognizance of the milieu in which cyber crime is committed, Lombrosso theory of atavism, which has been described as the most notorious of the evolution approaches to deviant behaviour and Routine Activity Theory, formerly applied to aggregate level crimes has been considered appropriate for cybercrimes .

The concept of constructivism has roots in classical antiquity, going back to Socrates's dialogues with his followers, in which he asked directed questions that led his students to realize for themselves the weaknesses in their thinking. The Socratic dialogue is still an important tool in the way constructivist educators assess their students' learning and plan new learning experiences. Jean Piaget and John Dewey developed theories of childhood development and education, what is now called 'Progressive Education' that led to the evolution of constructivism. Piaget believed that humans learn through the construction of one logical structure after another. He also concluded that the logic of children and their modes of thinking are initially entirely different from those of adults. The implications of this theory and how he applied them have shaped the foundation for constructivist education. Dewey called for education to be grounded in real experience. He wrote, "If you have doubts about how learning happens, engage in sustained inquiry: study, ponder, consider alternative possibilities and arrive at your belief grounded in evidence." To Dewey, inquiry is a key part of constructivist learning. Among the educators, philosophers, psychologists, and sociologists that added new perspectives to constructivist learning theory and practice are Lev Vygotsky' Jerome Bruner and David Ausubel. This philosophy of constructivism underlies the methodology of action research and they are achievable under collaborative endeavours. The constructivist theory of learning is only relevant to the process of developing the Action Cyber Crime Prevention Programme.

Gagnon and Collay (2006) stated that there are four epistemological assumptions at the heart of constructivist learning. These are:

- I. Knowledge is physically constructed by learners who are involved in active learning;
- II. Knowledge is symbolically constructed by learners who are making their own representations of action;
- III. Knowledge is socially constructed by learners who convey their meaning and making to others:
- IV. Knowledge is theoretically constructed by learners who try to explain things they do not completely understand.

The scholars further maintained that these epistemological assumptions can be seen in the works of Dewey, Montessori, Piaget, Bruner and Vygotsky, and that constructivism represents a paradigm shift from education based on behaviourism to education based on cognitive theory. Fosnot (1996) maintains that behaviourist epistemology focuses on intelligence, domains of objectives, level of knowledge and reinforcement, while the constructivist epistemology assumes that learners construct their own knowledge on the basis of interaction with their environment. One of the major arguments of the constructivist is that effective learning involves action or active participation of the learners which involves participatory activities where groups of students interact and help one another to learn. Participatory action model is not having students talk to one another, either face to face or in a conference while they do individual assignments; rather it involves working together to achieve a common purpose. For instance, students can be assisted to work together in a participatory mode, form a club, and elect officers. By learning to vote, they are learning the concept of democracy and at the same time acquiring the values of fairplay, tolerance and teamwork. From the constructivist point of view, there are some shifts in learning today. These shifts are:

- from instruction to construction and discovery;
- from teacher-centered to learners centered education;
- from absorbing learning materials to learning how to navigate and how to learn;
- from school learning to life long learning;
- from learning as torture to learning as fun;
- from the teacher as a transmitter to the teacher as a facilitator,

This philosophy of constructivism underlies the methodology of action research and they are achievable under collaborative endeavours. The constructivist theory of learning is only relevant to

the process of developing the Action Cyber Crime Prevention Programme, consequent on the selected students active participation in the development of the Action Cyber Crime Prevention Programme.

However, it may be necessary to examine some criminological theories that are relevant to the milieu in which cyber crimes are committed. Jaishankar (2008) propounded that there is a need for a separate theory of cyber crime because the general theoretical explanations were found to be inadequate as an overall explanation of the phenomenon of cyber crime. Consequent on these inadequacies, Jaishankar (2008) developed space transition theory in order to explain the causation of crime in the cyberspace. Space transition theory is an explanation of the nature of the behaviour of the person who brings out his/her conforming space and non-conforming behaviour in the physical space to cyber space. Space transition involves the movement of person from one space to another (e. g from physical space to cyberspace and vice versa). The theory argues that, people behave differently when they move from one space to another. The positions of the theory are:

- I. Persons, with repressed criminal behaviour (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.
- II. Identity flexibility, dissociative anonymity and lack of deterrence factor in the cyberspace provide the offenders the choice to commit cyber crime.
- III. Criminal behaviour of offenders in cyberspace is likely to be imported to physical space which, in physical space may be exported to cyber space as well.
- IV. Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the channel to escape.
- V. (a) strangers are likely to unite together in cyberspace to commit crime in the physical space.
  - (b) associates of physical space are likely to unite to commit crime in cyber space.
- VI. Persons from closed society are more likely to commit crime in cyberspace than person from open society.
- VII. The conflict of norms and values of cyber space may lead to cyber crimes.

The space transition theory views the emergence of cyber space as a new locus of criminal activity. This theory shows that secondary school students, if, not educated on the ills of cyber crimes can physically unite in their school premises to perpetrate acts that are criminal which they would not ordinarily commit on their school compounds.

Another criminological theory relevant to this study is the theory of atavism which Fulcher and Scott (2007) described as the most notorious of the evolutionary approaches to deviant behaviours. The theory was propounded by Cesare Lombroso, who holds that many criminals were born with atavistic features. Lombroso found out that criminals have definite biological failings that prevent them from developing to a fully human level. The criminals showed certain ape—like characteristics or sometimes merely saving features that gave them the distinct anatomical characteristics from which they could easily be identified: large jaws, long arms, thick skulls, and large monkey-like ears and so on. These atavistic features, Lombroso argues, also lead them to prefer forms of behaviour that are normal among apes and savages, but are criminal in human societies. He claims that about forty percent of all criminals are born criminals of this kind, and are driven into criminality by their biology. Other law breakers are simply occasional, circumstantial offenders and do not have the atavistic characteristics of the born criminal.

The excesses of Lombroso's theory and the racial assumptions that underpinned it have long been discarded. However, many people still see criminality as resulting from innate characteristics. Violence and aggression, for example, are often seen not only as specifically male characteristic, but in their extreme forms as being due to genetic peculiarities. It has been proposed, for example, that many violent criminals have an extra Y chromosome in their cells. Thornhill and Palmer (2000) suggested that rape can be explained as a consequence of normal, genetically determined male behaviour. In the 1990s, the success of the Human Genome project led to many strong claims about the genetic basis of crime. The idea of the born criminal was supported in a report that pimping and petty theft appear to be genetically conditioned, but a person's genes have little influence on their propensity for committing crime of violence (Independent, 15 February 1994), violence was reported to be due to a mild brain dysfunction in early life health care for pregnant women could reduce violent crime by over twenty percent (Independent, 8 March 1994). The link between biology basis to violent behaviour, the ways in which this is expressed and the consequence that flow from it depend upon the

meanings that are attached to it and the particular social situation in which it occurs (Fulcher & Scott, 2007). Though, the excesses of Lombroso's theory and the racial assumptions that underpinned it have long been discarded, his findings led other researchers to study specific traits that could make human beings to commit crimes. One of the biological factors discovered by scholars is the presence of extra Y chromosomes in 1-3% of violent criminals in prison cells. This may be the factor responsible for males involvement in cyber crimes than their female colleagues across the globe. Action Cyber Crime Prevention Programme is proposed consequent on educational researchers that education could be used to tame the excess 'Y' chromosome responsible for male students cyber lawless behaviour in Nigeria.

In addition to these, Routine Activity Theory (RAT) propounded by Lawrence Cohen and Marcus Felson in 1979 to fill the shortcomings in existing models that failed to adequately address crime rate trends since the end of World War II and formerly applied to aggregate level crimes has been considered appropriate for cybercrimes (Pease, 2001; Yar, 2005). Kigerl (2011) saw Routine Activity Theory (RAT) as an ecological approach to crime causation, the accessibility, location, and presence or absence of environmental characteristics, and certain types of people are what prove predictive of criminal behaviour. Cohen and Felson (1979) posited that Routine Activity Theory requires three situations to be true and meet in space for there to be a crime that is committed. These include: a motivated offender, a suitable target, the absence of a capable guardian.

Akers and Sellers (2004) went further to explain that a motivated offender must be someone willing to commit a crime should he or she have the opportunity. Felson and Clarke (1998) further stated that a suitable target is one of the motivated offender values (credit card information). The motivated offender would have observed that the suitable target is visible, accessible, and able to be misappropriated by the offender. In addition to these, anything that obstructs the offender's ability to acquire the target (for example, antivirus, encryption) i.e. a capable guardian must be absent. Kigerl (2011) stated that research has discovered some support for the three Routine Activity theory conditions whether a crime occurs in cyberspace. Actions such as time spent online, more use of internet banking, making more online purchases and risky online behaviours make people more suitable to offenders. Research have shown that people with these actions are likely to be recipients of cyber bullying (Holt & Bossler, 2009), receive more phishing attacks (Hutchings & Hayes, 2009), are more often targeted by internet fraud (Pratt, Holtfreter, & Reisig, 2010) as well as other forms of fraud (Holtfreter, Reisig, & Pratt, 2008) and lost time due to malware infection (Bossler & Holt, 2007). Choo (2008) stated that lack of antivirus, antispyware, and firewalls (capable guardians) are associated with more malware victimizations. Consequent on these, there appears to be some support for Routine Activity Theory in explaining the likelihood of being the target or victim of a cyber crime attack. However, it is not easy to predict whether a country will more likely be the source of a cyber attack or be the place of residence for a disproportionate number of cyber criminals. Some countries are known to be more problematic than others in terms of cyber crime activity (Kigerl, 2011). This theory shows that the failure of the capable guardians like encryption, anti-virus and internet security programme that computer scientists entrusted secondary school students to, is responsible for their exploitation of the anonymity afforded them by the Internet to defraud unsuspecting people in the cyber space. Consequent on this discovery, we feel 'Education' through the Action Cyber Crime Prevention Programme would be a more capable guardian to students than encryption, anti-virus and internet security programs in the cyber space.

#### Purpose of the Study

Consequent on the annual rankings of Nigeria by the National White Collar Crime Center and the Federal Bureau of Investigation as the most notorious country whose citizens perpetrate cyber crimes in Africa and third most notorious country noted for cyber crime acts in the world, it is expedient to find a means of changing this orientation. The median age of the cyber crime offenders is found to be less than thirteen years, which is an age range peculiar to secondary school students in Nigeria. The absence of enabling laws coupled with the fact that laws sometimes do not serve as a deterrent, education is the key factor that could be used to change long-established attitudes and habits to end the menace of cyber crimes. And in the absence of any formal specific programme targeting secondary school students' crime prevention knowledge and attitude in Civics and Social Studies, this study, therefore, determined the impact of an informal Cyber Crime Prevention Programme (CCPP)

through the action or participatory approach. The study further determined the moderating effects of gender and computer literacy on the dependent measures.

# **Hypothesis**

There is no significant main effect of treatment on students' attitude to cyber crime prevention

# Methodology

This study adopted a participatory action research paradigm to develop an informal Cyber Crime Prevention Programme as research have shown that participatory action research paradigm could foster value acquisition among students (Koshy, Koshy and Waterman, 2010). The study further adopted the pretest-posttest, control group quasi experimental design (Shadish, Cook and Campbell, 2002) to determine the impact of the Action Cyber Crime Prevention Programme on secondary school students' learning outcomes in Civics and Social Studies in Ondo State.

# **Selection of Participants**

The target population of this study comprises secondary school students in Ondo State. Six secondary schools were purposefully selected and assigned three a piece to the experimental and control groups for the purpose of this study in Akure, the capital city of Ondo State. The state capital is purposefully selected for this study because it has all the modern social amenities especially electricity, Internet Service Providers and cafes. Intact JSS 2 classes sample were selected in each of the six secondary schools that permitted their students' to partake in the study. Four hundred and twenty-six students started the study, but only two hundred and eighteen students were regular during the period the study lasted. The students dropped off consequent on their non residence on school compound. JSS 2 students were used for this study because, Civic Education and Social Studies are being taught at JSS level in Nigerian secondary schools, the students were not preparing for the external Junior Secondary School Examination, and as such they were more available to participate in the development of ACCPP. In addition to these, the students will be able to provide the initial leadership for the Cyber Crime Prevention Club, as the students have four more years in the secondary level of education; this would enable them to continue the Cyber Crime Prevention Clubs in their respective schools.

# **Research Instruments**

Five instruments were used for the study. These were:

- 1. Students' Attitude to Cyber Crime Prevention Scale (SACCPS)
- 2. Computer Literacy Test (CLT)
- 3. Conventional (Class) Lecture Method Guide (CLMG)
- 4. The Focus Group Discussion Guide (FGDG)
- 5. Action Cyber Crime Prevention Programme for Experimental Group

# **Students' Attitude to Cyber Crime Prevention Scale (SACCPS)**

This is a 22 item scale developed by the researcher to measure the attitudes of selected secondary school students to Cyber Crime Prevention. The scale is made up of two sections; Section A elicits responses on personal details like name, sex, school and membership of any Cyber Crime Prevention Club. Section B contains 22 scaled questions which consist of modified likert 4-point scale of Strongly Agree (SA), Agree (A), Disagree (D) and Strongly Agree (SA). The scale was designed to measure the following:

- a. Attainment of requisite crime prevention attitudes for identifying crime related problems and issues in the immediate environment.
- b. Inculcation of the right values and skills that will enable students to actively participate in the cyber crime prevention process.
- c. Development of a sense of moral responsibility in preventing incidences of cyber crime in the immediate environment.

The items will be scored by allotting 4 points to SA, 3 to A, 2 to D and 1 to SD for positively worded statements. This will be reversed for negatively worded statements.

An initial 22 items were drawn and subjected to peer and expert review to determine their appropriateness with reference to the targeted learners. This was also used to establish its content validity. Based on their inputs, modifications were effected and the 22 items were then tried out on a sample of JSS 2 students that will not be part of the main study. For reliability, copies of the draft

questionnaire administered were subjected to Cronbach Alpha method and a reliability coefficient of 0.76 was obtained.

# **Computer Literacy Test (CLT)**

The CLT was designed by the Office of Education, North American Division of Seventh Day Adventists in 2005 and revised in 2009. The test has two sections; section A has 60 questions which evaluates literacy, while section B has 10 questions, which tests competency. The 60 questions in section A are in 6 parts with 10 questions each. There are 13 options lettered A to M, with a correct option matching each question. Section B has 10 objective test items with options A – D which include only one correct option. The initial 70 questions were subjected to peer and expert review to ensure the construct and content validity of the test as well as its appropriateness for the target learners. The test items were thereafter reduced from 70 to 38 based on too high or too low difficulty indices, the results of the analysis were used to pick items that have discriminating index of 0.4 to 0.7. For reliability and average item difficulty, the final draft of the test was subjected to KR-20 which yielded 0.78.

# The Conventional (Class) Lecture Method Guide (CLMG)

The CLMG was designed by the researcher to guide teachers in the control group. This was to ensure uniformity. The CLMG was prepared on each of the concepts selected for the study. The Conventional (Class) Lecture Method Guide is made up of five steps; these are:

- The teacher introduces the concept
- The teacher discusses facts or ideas on the concepts in steps
- The teacher gives notes on the concept
- The teacher asks questions
- The teacher gives assignment to students.

# The Focus Group Discussion Guide (FGDG)

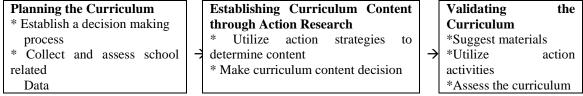
The researcher constructed the Focus Group Discussion Guide (FGDG). The instrument was constructed to enable secondary school students make decisions and develop the Action Cyber Crime Prevention Programme. The FGDG has 14 items and is made up of four (4) sections. To ascertain the validity of this instrument, the researcher made use of twenty-five (25) students from a co-educational school that were not involved in the study. Each item was discussed and any item that the students found difficult was amended. To ascertain the validity of the FGDG, the researcher made use of 20 JSS 2 students from a co-educational school that will not be involved in the study. Each item was discussed and the two items that the students find difficult was amended.

# **Development of the Action Cyber Crime Prevention Programme**

The Roberts (2007) curriculum model was adapted for the development of the Action Cyber Crime Prevention Programme. The model comprises 3 stages, namely:

- I. Planning the curriculum.
- II. Establishing curriculum content through action approach
- III. Validating the curriculum

The model is presented in the Figure I:



**Fig. I:** Curriculum model for the study (Adapted from Roberts, 2007)

#### Planning the Action Cyber Crime Prevention Programme

Focus Group Discussion Moderators (the selected teachers and research assistants) were selected and trained. The focus group discussion moderators moderated the group activities and led discussion towards making decisions in each discussion group. A training format was used to train the Focus Group Discussion Moderators. They were trained to achieve action means of reaching decision among group members and engage in participatory efforts toward solving problems.

The Junior Secondary School (JSS) Social Studies and Civic Education Syllabi was obtained, the crime prevention concepts were identified. The concepts that were identified are: citizenship, ICT,

problems of ICT, social issues and problems, negative behaviours, and values. JSS II Social Studies and Civic teachers were interviewed in each of the experimental schools to discover the method used to teach Crime Prevention concepts in the consulted syllabi. Some of the students in the experimental groups were selected randomly and interviewed.

# Establishing the Objectives and Contents of the Cyber Crime Prevention Programme through Action Approach

The objectives and contents of the Action Cyber Crime Prevention Programme were developed collaboratively during the focus groups discussion. The selected JSS 2 students in the experimental schools engaged in the focus group discussion.

# **Focus Group Discussion**

The focus group discussion was used to establish the objectives and contents of the Action Cyber Crime Prevention Programme. The focus group discussion took place in each of the three schools in the experimental group. Each focus group was made up of eight to ten participants. All the focus groups in each school had their discussion sessions simultaneously. The duration of the focus group discussion was two weeks. The outline for the focus group discussion was: introduction, setting the ground rules, overview of the topic, questions, discussion, and summary.

# **Validation of the Action Cyber Crime Prevention Programme**

The developed Action Cyber Crime Prevention Programme was validated in each experimental school with the establishment of Cyber Crime Prevention Club. The validation involves the following steps:

# **Drafting the Cyber Crime Prevention Club's Constitution**

The research assistants and the cooperating teachers educated the participants on the importance of drafting a constitution to guide the activities of the Cyber Crime Prevention Club. In each experimental school, copies of draft constitution prepared by the researcher were given to the participants, who grouped themselves and review every item in the draft constitution with the assistance of the participating teacher. The President of each review group later presented the positions of each group to all the participants. The participants harmonized the positions of each group on each item by consensus or voting. The participating teacher collected the harmonized constitution and read out the contents and called for motion to adopt the reviewed draft of the constitution, which the participants did. It could be observed that some marked differences exist in the contents of the constitution of each school, consequent on the peculiarities of each experimental school.

# **Election of Club Executives and Executive Meetings**

The participants elected one to two students as electoral officer/officers in each school who conducted the election with the assistance of the researcher, participating teachers and research assistant students were asked to nominate candidates for each post, while the nominated candidates were given a day to campaign and sell their manifestos to their colleagues. The election took place a day after campaign in each experimental school, the electoral officers counted the votes, collated the results and announced immediately. The electoral officers in consultation with the participating teacher nullified elections into some positions in two of the three experimental schools where the number of votes casted, exceeded the accredited voters. The electoral officers re-conducted such elections, counted, re-collated and announced the results immediately.

The elected club executives were presented to the participants in each experimental school. In each school, the executives met, deliberated and decided on inauguration of the club, and inaugural meeting of the club.

# **Inauguration of the Action Cyber Crime Prevention Club**

The Cyber Crime Prevention club was formally inaugurated in each school with the participating teacher who became the club staff Adviser, and Principal, who became the patron in attendance or represented by the Vice Principal. During the inauguration ceremony, the researcher mentioned the benefits that the participants and their schools could derive from selfless participation in the activities of the club such as acquisition of knowledge for effective crime prevention in the cyber space. The researcher presented a notice board, files, and banners to the club in each school, to enable the club take-up effectively.

# **Inaugural Meeting of the Cyber Crime Prevention Club**

After the inauguration of the Cyber Crime Prevention Club in each experimental school, the clubs conveyed the inaugural meetings to discuss programmes the club would carry out and strategies to adopt in encouraging other students to join the club next academic session.

#### Lecture

Two lectures were organized for the Cyber Crime Prevention Club in each experimental school. The first lecture examined communication, ICT and Problems of ICT'. A lecturer from Adekunle Ajasin University, Akungba who was invited to 'IT Security Conferences for the Next Generation' in Malaysia and Germany to present his research on cyber crime prevention delivered the lecture in each experimental school. The students were grouped, each group had at least two laptops connected to the internet throughout the duration the lecture lasted. It was observed during the first lecture that participants with high computer literacy and competency helped their low and moderate computer literate colleagues to navigate through difficult computer tasks.

The second lecture centred on citizenship and negative behaviours. A High Court Magistrate and Legal practitioner delegated by Ondo State Judiciary spoke on 'What the Nigerian Judiciary, Police force, and Nigeria Prisons' does to Cyber Crime offenders. The legal practitioner taught for twelve years in the secondary school cadre before joining the bar, this enable him to sequence the lecture he gave to the students.

#### Drama

The Cyber Crime Prevention Club in each school staged a drama titled 'Food by Deceit' to educate the students who were non-club members and teachers on cyber crime prevention. The drama chronicled the life of Raymond, a young promising chap that got entangled in web of 'Yahoo Yahoo' (Cyber Crimes) syndrome which ultimately sent him to the abysmal dungeon of cul-de-sac. Students in one of the experimental schools composed a song titled 'E ma Yahoo' meaning 'do not involve in Yahoo Yahoo'.

#### Debate

The participants in each experimental school had debate on the topic 'ICT has done more harm than good to humanity'. In each school, the President, vice-President and Editor-In-Chief debated on the topic with three non-executive members of the Cyber Crime Prevention Club.

#### Post Test

The treatment lasted for ten weeks in the experimental schools. The researcher subsequently administered the instruments on the participants in the experimental and control schools.

# **Method of Data Analysis**

The quantitative data was collated, coded and analyzed using Analysis of Covariance (ANCOVA). The Multiple Classification Analysis was employed to determine the magnitude of performances across the groups. A line graph was used to disentangle significant interaction effects.

#### Results

**Hypothesis:** There is no significant main effect of treatment on students' attitude to cyber crime prevention.

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

Source	Hierarchical Method								
				Mean	F	Sig			
	Squares		Square						
Covariates	Covariates PREATT		1	8029.586	109.949	.000			
Main Effects	Main Effects (Combined)		12021.196 4		41.151	.000			
	TREATMENT		1	11618.533	159.092	*000			
GENDER COMPTLIT		8.055	1	8.055	.110	.740			
		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			
GEND	151.950	2	75.975	1.040	.355				
	465.427	2	232.713	3.187	.043				
COMPT	81.894	2	40.947	.561	.572				
COMPT	20844.587	12	1737.049	23.785	.000				
3-Way Inte	14971.193	205	73.030						

TRTMENT*GENDER*	35815.780	217	165.050	
COMPTLIT				
Model				
Residual				
Total				

<sup>\*</sup> Significant at p < 0.05

Table 4.4 shows that there is significant main effect of treatment on students' attitude to cyber crime prevention ( $F_{(1;205)} = 159.092$ ; p<.05). This means that the difference in the attitude of students exposed to Action Cyber Crime Prevention Programme and their control group counterparts is significant. Hypothesis 1b is, therefore, rejected.

**Table 3:** MCA of Posttest Attitude Scores by Treatment, Gender and Computer Literacy Grand Mean = 64.89

			Grand M	ean = 04.89					
Variable + Category		N	Predic	ted Mean	Deviatio	n			Bet
			Unadju	Adjus	Unadju	Adjust	Eta	a	
			sted	ted for	sted	ed for			
				factors		factors			
				and		and			
				covariates		covariates			
TREATMENT	Cyber		77.09	75.19	12.19	10.29			
Crime		75							.58
	Prevention						689	2	
Prog			58.50	59.49	-6.39	-5.40			
		1							
	Control	43							
GENDER	Male	1	65.03	64.45	.13	45			.03
	Female	08	64.77	65.34	13	.44	010	5	
		1							
		10							
COMPUTER	Low		61.46	63.39	-3.44	1.51			
LITERACY	Moderate	98	65.81	65.82	.91	.92			.11
	High		72.50	66.93	7.60	2.03	299	0	
		86							
		34							
<u> </u>	R= .748								
R	Squared= .560	)							

Table 4.5 shows that students exposed to the Action Cyber Crime Prevention Programme had higher adjusted posttest attitude mean score ( $\bar{x}$  =75.19; Dev. =10.29) than their control group counterparts ( $\bar{x}$  =59.49; Dev. = 5.40). To this end, the Action Cyber Crime Prevention Programme was more effective than the conventional teaching.

## Discussion

Results obtained shows that the students' exposed to the Action Cyber Crime Prevention Programme obtained higher adjusted posttest attitude mean scores. The programme proved effective to the conventional lecture method, consequent on the relevance of the programme and retention of the participatory activities that allowed students to hear their views, learn from their colleagues and the support of the school and teachers for the programme. The Action Cyber Crime Prevention Programme was more effective because the learners were at the centre of the action activities; hence prevention attitudes were developed effectively.

# Conclusion

This study has established that the action Cyber Crime Prevention Programme is effective at enhancing students' knowledge of crime prevention and attitude to cyber crime prevention. The programme can be used to not only foster the learning of cyber crime prevention concepts, but attitude to cyber crime prevention irrespective of students' gender and computer literacy level. Consequent on the findings of the study, it could be concluded that the Action Cyber Crime Prevention Programme have great potentials at enhancing students' attainment in crime prevention concepts and attitude to

cyber crime prevention. The participatory action research paradigm adopted to develop the Action Cyber Crime Prevention Programme changed the learning landscape of the students not only from torture to fun but from instruction to discovery which developed in the students civic values and skills that would enable them to shun on-line activities that may project the image of Nigeria in a bad light. The formation of the Cyber Crime Prevention Clubs to sensitive members of the school community and public at large on dangers inherent in cyber crimes developed in the students civic values and skills like cooperation, unity, love, sympathy, consideration of others welfare, selflessness, hardwork, positive use of knowledge, honesty, obedience, respect, fair play, patience and loyalty. In this case, Civic Education and social studies teachers should make conscious efforts to utilize the Action Cyber Crime Prevention Programme when teaching crime prevention concepts in Civic Education and Social Studies. Also, the government and relevant agencies and professional associations should organize regular workshops and in-service teacher education programmes for social studies and civil education through which emerging issues could be discussed. Schools should also put in place facilities that can encourage students to participate in non formal research activities.

# **Implications for Teacher Education**

This study developed and validated an Action Cyber Crime Prevention Programme for secondary school students in Ondo-State, Nigeria, consequent on the growing concern at finding solutions to the incidences of cyber crime among school – age children in Nigeria. The students were encouraged to develop a Cyber Crime Prevention Programme through the bottom-up approach that could be used to educate students' against involvement in cyber crimes. The findings of the study show that the sustained implementation of the programme would enable the students to inculcate good values while roaming the cyber space through the internet.

Another major implication of this study is the acquiring of the values and traits of group roles like positive use of knowledge, patience, consideration of others, cooperation, love, unity and loyalty by the students. The action approach adopted helped the students to acquire these values, thus showing the importance of participatory approach in equipping learners with values and traits requisite for effective cyber crime prevention. This finding shows the need to adopt to adopt the participatory approach to complement the conventional method used to teach Civic Education and Social Studies in Nigerian secondary schools.

In addition to these, curriculum planners could adopt the participatory approach used in this study for curriculum development in order to involve students, who would benefit from such educational programme to participate in designing the programme. The 'Bottom-up' approach, rather than the top-down approach should not only be used to develop Civic Education and Social Studies curriculum, but to teach the subjects consequent on the trans-disciplinary nature of Civic Education and Social Studies.

The Action Cyber Crime Prevention Programme is recommended to teachers for educating secondary school students in Nigeria on Cyber Crime prevention. Students should be encouraged by the teachers to construct personal ideas, identify conceptions and misconceptions and allowed to correct their misconceptions when learning crime prevention concepts in Civic Education and Social Studies Education. Government should empower teachers with participatory learning facilities in secondary schools and adopt bottom up approach in developing curricula in Civic Education and Social Studies. Government could also use the Action Cyber Crime Prevention Programme to train commercial cyber café operators on the risks of indulging secondary school students who use Internet to defraud foreign nationals.

The views represented in this paper, and any errors that accompany them, are, of course, ours.

# **References:**

Adesina, A.D.O. and Adeyemi, B.A. 2007. Teaching to Achieve Social Studies Values: A case of reeducation of Teachers. Retrieved Oct. 10, 2010 http://www.deta.up.ac.za/archive2007/presentations/word/Teaching%20to%20Achieve%20Social%2 Ostudies%20values%20ADEYEMI.pdf

Akers, R.L. & Sellers, C.S. 2004. Criminological theories: Introduction, evaluation and application (4<sup>th</sup> ed., p.33). Los Angeles, CA: Roxbury. and Technology. Publication of the National Association of Academies and the University of Texas. Winter, 2003.

Bossler, A.M & Holt, T.J. 2007, November 14. Examining the utility of routine activities theory for cyber crime. Paper presented at the annual meeting of the American Society of Criminology. Atlanta Marriot Marqius, Atlanta, GA.

CESAC. 1993. Nigerian Secondary Schools Social Studies Project. Book 1. Lagos: NERC.

Chiemeke, C. S, and Longe, O. B. 2007. Information and Communication Penetration in Nigeria: Prospects, Challenges and Metrics. Asian Journal of Information Technology, 6(3) 280-287.

Choo, K.K.R. 2008. Organised Crime Groups in Cyberspace: A Typology Springer Science + Business Media, LLC.

Cohen, L.E. & Felson, M. 1979. Social change and Crime rate trends: A routine activity approach. American Sociological Review. 44.

Dick, T and Herbert, L. 2003. Youth, Pornography and the Internet. Issues in Science

Felson, M. & Clarke, R.V. 1998. Opportunity makes the thief: Practical theory for crime prevention. Policing and Reducing Crime Unit: Research, Development and statistic Directorate. 98: 1-36.

Fulcher, J. and Scott, J. 2007. Sociology 3<sup>rd</sup> Edition. Oxford University Press. Retrieved June 28 from http://docs.google.com/viewer?a=v&q=cache:loyxiY3axbE

Gagnon, G.W. and Golly, M. 2006. Constructivist Learning Design. Retrieved Apr.25, 2010 from http://www.google.com

Holt freter, k., Reisig, M.D., & Pratt, T.C. 2008. Low Self-control, routine activities and fraud victimization. Criminology. 46: 189-220.

Holt, T.J. & Bossler, A.M. 2009. Examining the applicability of lifestyle- routine activities theory theory for cyber crime victimization. Deviant Behaviour. 30: 1-25.

Holtfreter, K., Beaver, K. M., Reisig, M. D., & Pratt, T. C. 2010. Low self-control and fraud offending. [DOI: 10.1108/13590791011056264]. *Journal of Financial Crime*, 17(3), 295-307.

Hutchings, A. & Hayes, H.2009 Routine Activity theory and phishing victimization: who got caught in the 'net'? Current issues in Criminal Justice.20: 432-451.

Independent. 1994. 'Genes linked to Violence and Crime Condemned'. February 15. Retrieved June 28, 2011 from http://www.independent.co.uk/news/genes-link-to-violence-and-crime-condemned-1573089.html

Independent. 1994. 'The Human Genome Project'. March 8. Retrieved June 28, 2011

From http://www.independent.co.uk/news/genes-link-to-violence-and-crime-condemned-1573089.html

Jaishankar, K. 2008. Space Transition Theory of Cyber Crimes. In Schnallagar, F. & Pittaro, M. (Eds.). Crimes of the Internet (Pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Kigerl, A. 2011. Routine Activity Theory and the Determinants of High Cybercrime Countries. Social Science Computer Review. 000(00).1-17.

Koshy E. Koshy V. Waterman H. 2010. *Action research for health care*. London: SAGE Nigeria: Prospects, Challenges and Metrics. Asian Journal of Information Technology, 6(3) 280-287.

Nigerian Educational Research and Development Council (NERDC). 2007. UBE Civic Education Curriculum. Abuja. Federal Government Press.

Obidoa, A. 1991. A Re-appraisal of Liberal Arts and Social Studies Education in Nigerian Schools in National Secondary School Curriculum Review Conference Proceedings, Ibadan: Macmillan Nigeria Publishers Limited.

Pease, K. 2001. Crime futures and foresight: Challenging criminal behaviour in the information age. In D. Wall (Ed.), Crime and the internet. London, England: Routledge

Roberts, M.R. 2005. Curriculum Development Process. Northern Arizona, CTE 592.

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

Shadish, W.R., Cook, T.D. & Campbell, D.T. 2002. Experimental and quasi-experimental designs for generalized causal inference. Boston: Houghton Mifflin Company.

The National White Collar Crime Center .2010. IC3 2009 Internet Crime Report (January 1, 2009 to December 31, 2009). Retrieved May 3, 2008 from http://www.IC3.state.gov. Pg. 1-29.

The National White Collar Crime Center .2011. IC3 2010. Internet Crime Report (January 1, 2010 to December 31, 2010). Retrieved May 3, 2008 from http://www.IC3.state.gov. Pg. 1-29.

The National White Collar Crime Center. 2002. IFCC 2001 Internet Fraud Report (January 1, 2001 to December 31, 2001). Pg. 1-27. Retrieved Apr. 27, 2007 from http://www.IC3.gov

The National White Collar Crime Center. 2003. IFCC 2002 Internet Fraud Report (January 1, 2002 to December 31, 2002). Pg. 1-27. Retrieved Apr. 27, 2007 from http://www.IC3.gov

The National White Collar Crime Center. 2004. IFCC 2003 Internet Fraud Report (January 1, 2003 to December 31, 2003). Pg. 1-28. Retrieved Apr. 27, 2007 from http://www.IC3.gov

The National White Collar Crime Center. 2005. Internet Fraud-Crime Report (January 1, 2004 to December 31, 2004). Pg. 1-29. Retrieved Apr. 27, 2007 from http://www.IC3.state.gov.

The National White Collar Crime Center. 2006. Internet Crime Report (January 1, 2005 to December 31, 2005). Pg. 1-27. Retrieved Apr. 27, 2007 from http://www.IC3.state.gov.

The National White Collar Crime Center. 2007. Internet Crime Report (January 1, 2006 to December 31, 2006). Pg. 1-27. Retrieved Apr. 27, 2007; from http://www.IC3.state.gov.

The National White Collar Crime Center. 2008. IC3 2007 Internet Crime Report (January 1, 2007 to December 31, 2007). Retrieved May 3, 2008 from http://www.IC3.state.gov. Pg. 1-29.

The National White Collar Crime Center. 2009. IC3 2008 Internet Crime Report (January 1, 2008 to December 31, 2008). Retrieved May 3, 2008 from http://www.IC3.state.gov. Pg. 1-29.

Thornhill, R. and Palmer, C.T. 2000. A Natural History of Rape: Biological Bases of Coercion. Cambridge: MA. MIT Press.

Yar, M. 2005. The Novelty of Cyber Crime: An assessment in Light of Routine Activity Theory. European Journal of Criminology. 2: 407-427.