International Journal of Social Science and Economic Research

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

THE EFFECT OF MORAL DISENGAGEMENT ON INTERNET HACKING AMONG CYBERCRIME PRISONERS FROM SELECTED PRISONS IN LAGOS AND EDO STATES, NIGERIA

[1]Francis Ehiamhen Obaweiki, [2]Dr. Margaret Njoroge (Ass Prof), [3]Dr. Anne Kanga

[1]Department of Psychology, Faculty of Arts and Social Science,
The Catholic University of Eastern Africa, P. O. Box 62157 Nairobi, 00200, Kenya

[2]Department of Psychology, Faculty of Arts and Social Science,
United States International University Africa, P.O. Box 14634 Nairobi, 00800 Kenya

[3]Department of Education and Curriculum Development, Faculty of Arts and Social Science,
The Catholic University of Eastern Africa, P. O. Box 62157 Nairobi, 00200, Kenya

DOI: 10.46609/IJSSER.2020.v05i07.003 URL: https://doi.org/10.46609/IJSSER.2020.v05i07.003

ABSTRACT

Internet hacking among youth has been identified as a global and progressive crime which poses threat to individuals, corporate organizations, and government institutions. The nature of cybercrime activities are indicants to Bandura's moral disengagement which helps individuals to behave in harmful ways while retaining a self-view as virtuous. The purpose of this study was to examine the effects of moral disengagement on internet hacking among cybercrime prisoners. The study was anchored on Bandura's social cognitive theory. It adopted mixed methods paradigm, specifically, the triangulation convergent design. The target population was 250 cybercrime prisoners, between the ages of 21 and 35 years old. The sample size was 214 inmates. The researcher used simple random and purposive sampling techniques to get them. Quantitative data were collected using Moral Disengagement Scale with reliability coefficient of 0.962, and Cybercrime Questionnaire with reliability coefficient of 0.956. Qualitative data were collected using interview and focus group discussion guide. Data analyses were carried out using correlation analyses, multiple regression analyses, and thematic analyses supported by narratives. Findings showed that moral disengagement has a strong positive statistically significant correlation with internet hacking ($p<0.01$, $r = .718$). Moral disengagement also had a good predictive value for internet hacking ($\beta = 0.377$, $p=.000< .001$).Qualitative results also indicated that moral justification, euphemistic labeling, advantageous comparison, displacement of responsibility, and dehumanization were strong predictors of internet hacking. The study

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

established the need for a holistic approach to address the individual, societal and behavioural challenges promoting moral disengagement and internet hacking among the youth.

Keywords: Moral Disengagement, Internet Hacking, Cybercrime, Prisoners, Cyber space

INTRODUCTION AND BACKGROUND

A global concern today is the issue of cybercrime among youth which constitutes a huge security, economic, and mental health threat to individuals, corporate and government organizations in different countries. For example, a global economic crime survey by Armin, Thompson, Ariu, Giacinto, Roli, and Kijewski (2015) puts the annual cost of cybercrime to the global economy at more than € 300 billion Euros, while the cost of cybercrime for the European Union (EU) was estimated to be 0.4% of its GDP amounting to € 13 Billion per annum. This report claimed that Poland, Germany, and United Kingdom, lost € 377 million, € 2.6 billion, and € 2 billion per annum respectively (Armin et al., 2015). These figures among others, showed that cybercrime globally constitutes a serious financial threat to the economy, and the wellbeing of their innocent victims. It also follows logically that, a crime of this magnitude are possible when individuals removed self-censure and self-sanctions from their behaviour.

A recent study by Internet Organized Crime Threat Assessment (hereafter IOCTA) (Wainwright,2017) indicated that North America alone has 88% internet penetration and 86% internet users is a core target for financially motivated cybercrime. This part of the globe is host to 37% business email frauds, 49% of global data breaches, top target for ransomware with 34% of all ransomware detection, top target for banking malware, host to 50% of world phishing sites, 39% of global botnet control serves, and primary origin of child abuse imagery (Wainwright, 2017). This shows that cybercrime comes in different forms and targets anyone, hence the need to examine this social reality.

The progressive nature of cybercrime activities are indicants to Bandura's moral disengagement which helps individuals to behave in harmful ways while retaining a self-view as virtuous (2016). The eight mechanisms of moral disengagement as postulated by Bandura have been grouped into four broad categories: 1) behavioural reconstrual, 2) agentic role of action, 3) the effects of action, and 4) victim aspect of moral disengagement. The first set of moral disengagement consists of three psychosocial mechanisms namely, moral justification, euphemistic labelling, and advantageous comparison. These mechanisms are used by the individual to reconstrue or turn harmful behaviour into good behaviour (2016). In social and moral justification, people adduce different reason through rationalization as justifications for their behaviour. Also, people use euphemistic labels to detach and depersonalize doers from harmful activities (Lutz, 1987). Lastly, exploiting the contrast principle can make even highly detrimental activities appear righteous.

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

The second set of disengagement practices (displacement and diffusion of responsibility) operates by obscuring or minimizing one's agentic role in causing harm. For example, studies have shown that people will behave in ways they would normally repudiate if a legitimate authority accepts responsibility for the effects of their conduct (Milgram, 1974). Thus, the exercise of moral control is weakened when personal agency is obscured by displacing or diffusing responsibility for detrimental behavior. The third set of moral disengagement (distortion of consequences) focused on the effect of action. This principle operates by minimizing, disregarding, ignoring, misconstruing, or even disputing the harmful effects of one's actions. This mechanism is used to avoid facing the harm they cause or to minimize it when people pursue activities that harm others (Bandura, 2016).

The fourth set of disengagement (dehumanization and blame) operates on the victims of detrimental practices using dehumanization and attributing blame. Dehumanization involves stripping people of their humanity which makes it easier to treat them cruelly as subhuman objects. This principle is based on the view that, the strength of moral self-censure for harmful practices depends on how the perpetrators regard the people they mistreat. This mechanism has been used in most inhumane forms of crimes like the Nazi's persecution of the Jews and the Rwandan genocide of 1994, where the Tutsis were called "cockroaches" and "snakes" that are not human (Haslan & Lughman, 2012). Lastly, external attribution of blame turns the perpetrator into a victim, perceived as faultless and driven to injurious actions by forcible provocation. This exonerates the perpetrator who claims that the victim or some outside force provoked his/her actions. Recipients are seen as deserving their punishment. Similarly, ascribed culpability on the victims serves as further moral justification for more cruel behaviour on the part of the individual (Bandura, 2016). Thus, the researcher asks if the issue of internet hacking among youth in Nigeria is not associated with a growing trend of moral disengagement in the individuals.

Cybercrime is a generic term used to describe two distinct, but closely related criminal activities: cyber-dependent and cyber-enabled crimes (McGuire & Dowling, 2013). Cyber-dependent crimes are offences that can only be committed by using a computer, computer networks, or other form of information and communication technologies (ICTs) (Ajayi, 2016). These acts include the spread of viruses and other malicious software, and distributed denial of service (DDoS) attacks. Cyber-enabled crimes comprises those traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICTs (Ajayi, 2016). Cyber-enabled crimes consists of fraud such as mass-marketing frauds, phishing e-mails and other scams; online banking and e-commerce frauds; theft of personal information and identification-related data; and sexual offences against children (Ajayi, 2016). But unlike cyber-dependent, cyber-enabled crimes existed before the advent of cyber network systems, but ICTs

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

have only come to expand its reach and targets for these individuals. Ironically, the use of ICTs renders the victim anonymous, making it easier for cybercriminals to 'dehumanize' their victims, and this again constitutes one of the mechanisms of moral disengagement.

Africa as a continent is not exempted from internet hacking for the obvious reasons of the growing number of individuals and corporate internet users. Also, the lack of adequate cybersecurity framework and public awareness to protect individuals, and corporate organizations from the menace of cybercriminals is another enabling factor. For example, reports from Wainwright (2017) has it that, one third of African countries has less than 10% internet penetration, and Africa is home to almost 10% of the world's internet users. In this report, most EU Member States highlighted Africa as the source of specific cyber threats such as cyber-facilitated frauds, romance scams, phishing, attacks on critical infrastructure, and card-not-present (CNP) fraud using compromised EU cards (Wainwright,2017). Thus, Africa is mentioned as exporting cybercrime to most EU countries. Suffice to note that, findings like this, does not include individuals and some organizations who may not disclose their loss for some reasons like shame of been labeled gullible or loss of customers' confidence in their products or services. Thus, the impact of cybercrime globally may be much more than what is reported by the media.

Another study on social organization of cybercrime among university undergraduates in Nigeria, revealed among others, that with an alarming unemployment rate in the country, cybercrime becomes a means of survival and sign of creativity for the youth (Tade & Aliyu, 2011). Thus, with such social-economic justifications offered by cybercriminals for their actions, a key element of moral disengagement plays out. Justification of cybercrime as being creative and proactive enough to prevent future unemployment and poverty caused by the Nigerian government will serve to encourage more of such acts.

To further compound this issue, different countries in Africa, use different euphemistic labels to describe cybercrime and cybercrime offenders. In Ghana, it is called 'Sakawa' or 'Yahoo yahoo' (Coonsom, 2009), 'Faymania' in Cameroon (Oumarou, 2007), and yahoo yahoo in Nigeria, while the perpetrators are called yahoo boys (Adebusuyi, 2008; Tade & Aliyu, 2011). These social labels came from the ways the cybercriminals defraud their unsuspecting victims, which involves sending sinister and deceptive e-mails using 'Yahoo mail'. Ironically, euphemistic labeling constitutes one of the mechanisms of moral disengagement which serves as moral deodorant to diffuse the censure which the society should attached to such despicable conducts.

Some studies on the composition of the main actors of cybercrime in Nigeria, revealed that the majority of cybercriminals are youth mainly in the universities (Adeniran, 2008; Tade & Aliyu, 2011). But, this group from the researcher's point of view, also have within its ranks both the

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

employed, unemployed university graduates, and university dropouts. This no doubt portend a serious crises for the future of the country and our continent if we still hold to the saying that 'the youth are the future leaders of tomorrow'. Thus, the researcher argues that internet hacking is the symptom of a disease: A growing trend of moral disengagement (influenced by situational inducement) among the youth which needs urgent attention from the society.

Interestingly, studies on the factors influencing cybercrime among youth in the country, showed that unemployment, corruption in the politics, economy, education, and social institutions (Tade & Aliyu, 2011), peer influence, materialistic value, age and gender (Eigbadon & Adejuwon, 2015) are leading causes. These studies as it were, failed to consider the individual personal variables in cybercrime of which moral disengagement is central. Otherwise, how do we explain that in spite of these and other environmental factors, there are many youth who are not involved in cybercrime in the country?

Effort to curb cybercrime related offenses in Nigeria is currently spearheaded by the Economic and Financial Crime Commission (EFCC) guided by the Cybercrime Act 2015. This drive according to the former chairman of EFCC Ibrahim Lamorde, led to the conviction of 288 persons over various internet crimes in 2012, while 234 were still being prosecuted in courts across the country (EFCC, 2012). Yet, the rate of scammers is on the daily increase as indicated by the arrest of 80 Nigerians in the US by FBI over charges of internet hacking, phishing e-mails and other scams; online banking and e-commerce frauds; theft of personal information and identification-related data, and business e-mail compromised in August 2019. This means we may have been searching for the right answer in the wrong places. That is, to understand the issue of internet hacking among youth, the individual and environmental variables promoting this behaviour needs to be considered together holistically. The observed effect of moral disengagement on behaviour may equally be true for cybercrime because, cyber space provides anonymity and pseudonymity which may further exacerbate moral disengagement since the victims are not seen by the perpetrators. Thus, according to Social cognitive theory (Bandura, 1986), the cyber space could actually be influencing the cybercrime and the individual's disposition towards internet hacking. Internet hacking among Nigerian youth constitute sources of serious mental health challenges to their victims but studies are scanty on psychological (moral disengagement) explanation of internet hacking in Nigeria hence the need for this study.

Research Question: What is the effect of moral disengagement on internet hacking among cybercrime prisoners in Lagos and Edo States, Nigeria?

METHODS

This study was conducted in Lagos and Edo States in Nigeria. Two prisons each from Lagos and Edo States were selected because of the presence of cybercrime prisoners there. This study

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

adopted the mixed methods paradigm, specifically the triangulation convergent design. It combined correlational and phenomenological research designs in a one-phase approach (Creswell &Plano-Clark, 2007). Using this model, quantitative and qualitative data were collected and analysed separately and the results mixed during the interpretation.

The target population of this study was estimated to be 250 cybercrime prisoners in four selected prisons in Lagos State, and Edo State (Prisons Authority, 2019). A sample size of 250 respondents were selected using census sampling technique. Simple random and purposive sampling techniques were used to select 231 participants for the quantitative strand and the 19 participants for the qualitative strand respectively.

This study used a 32-item Moral Disengagement Scale (Bandura, 1996), with a Cronbach's alpha coefficient of 0.962 which indicated a very good reliability. Also a 6-item internet hacking Questionnaire developed by the researcher to measure participants' rate of involvement in internet hacking, with a Cronbach's alpha coefficient of 0.956. Lastly, Interview guide was used in this study to collect qualitative data on moral disengagement and internet hacking.

Data Collection Procedures: The researcher obtained permission from the Controller of prisons in the Lagos State and Edo State Commands in Nigeria where the data collection was done. Next, the researcher employed the services of a male and female research assistants in the process of data collection. Their work during the study was to help the researcher take comprehensive field notes during the interview since the prison laws prohibit audio or visual recording of prisoners by any person.In both states, the researcher went to the Deputy Controllers of Prisons (DCP) of the selected prisons, with the research permit from the Controller of Prisons in each State Command. After a briefing on the purpose of the study by the researcher, the DCPs in turn directed the Welfare Officers to assist the researcher and his team in conducting the study in compliance with the laws of Nigerian prisons.

Data Analysis and Presentation: Quantitative data from 195 participants were analysed using the Statistical Package for Social Sciences (SPSS) version 22. The qualitative data from 19 participants were analysed thematically for emerging themes. Quantitative data were analysed using multiple regression analysis to establish the effect of moral disengagement on internet hackingamong the sample. Next qualitative data were analysed through content analysis to validate and establish the effect of moral disengagement on internet hacking.

RESULTS

Demographic Information

The demographic information of the participants were examined to help define the sample demographic characteristics and to give a better understanding of the population in the current

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

study. It was also to provide a basis for comparative analysis by future researchers. Demographic details of the participantsof the quantitative strand are summarize and presented in table 1.

Table 1

Demographic Characteristics of the Participants n = 195

Categories		**Frequency**	**Percent**
Age of Participants	21-25	30	15.38
	26-30	47	24.10
	31-35	118	60.51
Gender	Male	186	95.4
	Female	9	4.6
Educational Attainment	Secondary School	56	28.7
	Undergraduates	40	20.5
	Bachelor Degree	65	33.3
	Master Degree		7.69
	Others		9.74
Employment Status	Unemployed	125	64.1
	Employed	39	20
	Others	31	15.9
Number of Times imprisoned	First time in prison	124	63.6
	In prison before	71	36.4

The result from table 1 indicated that majority of the participants (60.5%) were between the ages of 31 and 35 years. An overwhelming majority were male (95.4%), and 41% of the participants had at least completed their first degree. Again majority of the participants (64.1%) were unemployed, which means that unemployment is a major factor in moral disengagement and internet hacking. Lastly, 63.6% were first timers in the prison which indicated that recidivism has effect on moral disengagement and internet hacking.

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

For the qualitative strand, 7 participants were between the ages of 31 - 35 years, 5 were within the age range of 26-30 years and 6 participants were between 20-25 years. On the educational attainment, 6 participants had completed their first degree; with 2 had completed master degree, 6 undergraduate, while only 5 had completed secondary school. On the employment status, 14 participants were unemployed, 4 were employed before their arrest, while one was in the category of others. Lastly, 13of the participants were in prison for the first time and6 had been imprisoned before.

The objective of the study was to explore the influence of moral disengagement on yahoo plus among cybercrime prisoners in Lagos and Edo States, Nigeria. Consequently, the research explored the objective and subjective experience of moral disengagement of the participants in relation to internet hacking. The results from the quantitative and the qualitative strands are presented concurrently following the triangulation convergence model.

Testing of Hypothesis

The study hypothesized that, there was no statistically significant relationship between components of moral disengagement and internet hacking. The relationship between moral disengagement and internet hacking among the cybercrime prisoners was examined using Pearson's correlation analysis. Results of Pearson correlation analysis is presented in Table 2.

Table 2

Correlation between Moral Disengagement and Internet Hacking (n = 195)

		Internet Hacking
Moral Disengagement	R	.718**
	Sig.	**.000**
	N	195
Moral Justification	R	.733**
	Sig.	**.000**
Euphemistic Labeling	R	.628**
	Sig.	**.000**
Advantageous Comparison	R	.614**
	Sig.	**.000**
Displacement of Responsibility	R	.542**
	Sig.	**.000**
Diffusion of Responsibility	R	.596**
	Sig.	**.000**
Distortion of Consequence	R	.353**

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

	Sig.	**.000**	
Dehumanization	R		.615**
	Sig.	**.000**	
Attribution of Blame	R		.652**
	Sig.	**.000**	
	N		**195**

The study found a strong positive and statistically significant relationship between moral disengagement and internet hacking ($p < 0.01$, $r = .718$). This means that an increase in moral disengagement, results in proportionate increase in internet hacking. A breakdown of the correlation between the eight components of moral disengagement and internet hacking also indicated that seven components had a strong positive and statistically significant relationship with the highest been moral justification ($p < 0.01$, $r = .733$), and distortion of consequences had a weak positive correlation ($p < 0.01$, $r = .353$). To further substantiate this finding, a regression analysis was carried out and the results presented in Tables 3, 4, and 5

Table 3

Regression Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.718[a]	.516	.513	.48538

a. *Predictors: (Constant), Moral Disengagement*

b. *Dependent Variable: Internet Hacking*

The statistics from the regression model summary output on Table 3 showed the *R* value is .718, and the *R* Square value is .516. The *R* value indicates that, there is a significant variance shared by the independent variable and the dependent variable. Also, the R Square value indicates that 51% of the variance in the dependent variable (internet hacking) is explained by the independent variable (moral disengagement) in this study. This means that 49% of the variation in internet hacking is accounted for by extraneous variables. Hence, there must be other variables which have an influence on the internet hacking among the respondents which require in-depth exploration.

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

Table 4

Regression ANOVA[a] Output

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	48.423	1	48.423	205.539	.000[b]
	Residual	45.469	193	.236		
	Total	93.893	194			

a. Dependent Variable: Internet Hacking

b. Predictors: (Constant), Moral Disengagement

The analysis of variance (ANOVA) in Table 4 shows that the *F*-ratio is 205.539, which is significant at $p = .000$, <.001. This output indicates that, there is less than a 0.1% chance that an *F*-ratio this large would happen if the null hypothesis was true. Hence, we can conclude that our regression model results in significantly good prediction of internet hacking if we use the mean value of scores in internet hacking. Thus, moral disengagement is a good predictor of internet hacking among the respondents.

Table 5

Regression Coefficients[a] Output

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	.377	.097		3.885	.000
	Moral Disengagement	.337	.023	.718	14.337	.000

a. Dependent Variable: Internet Hacking

Table 5 regression output gives us the coefficients which explains the individual contributions of variables in the model. This output showed that the Y intercept value (*B*) is .377. This can be interpreted to mean that, when moral disengagement score X is 0, the model predicts that internet hacking score will be .377. Also, the b_1 value from this output is .337 which means if moral disengagement (our predictor variable) is increased by one, our model predicts that internet hacking will increase by .337. This indicates that moral disengagement makes a significant contribution (p=.000< .001) to predicting internet hacking among the respondents. Therefore, the fourth null hypothesis was rejected and the alternative hypothesis which says that, moral disengagement has effect on the internet hacking among cybercrime prisoners was accepted.

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

The result from the interviews were generally consistent with findings from the questionnaire, but provided more clarifications and in-depth information on the influence of moral disengagement on internet hacking among the participants. In the interviews, the participants showed they understand internet hacking as an aspect of cybercrime but not everyone can practice this form of cybercrime because it required some level of IT competence. A factor which could account for the other extraneous variables indicated in the regression analysis. The responses were analysed and categorised into groups according to the eight mechanisms of moral disengagement. Thus, social and moral justification, euphemistic labeling, advantageous comparison, displacement of responsibility and dehumanisation mechanisms emerged from the analysis.

Social and Moral Justification

From the responses of the participants, the use of social, economic and moral justification in internet hacking stood out. These were evident in the responses of the cybercrime prisoners as they all made reference to the prevailing socio-economic, political and religious situation in the country which could be contributing to youth involvement in internet hacking. To begin with, a participant took a swipe at the government for lack of efficient biometric on her citizenry saying:

> In Nigeria it is difficult to track people because we have data issues then it gives way to easy crime. Unlike Europe where I did my Masters, you have your data such that what you do on the internet can easily be tracked. In Nigeria they cannot assess the data. In Nigeria, you can change location and that is the end. (P3, Focus Group Discussion 2, June 19, 2019)

This means that lack of comprehensive biometric data on citizenry and non-citizenry in the country could be a contributing factor in internet hacking in the country which the youth are exploiting. This participant expounding the justification for internet hacking with reference to systemic failure in the society said:

> In terms of priority, the society as a whole celebrate ill-gotten wealth. Nigerians don't investigate where or how people make their wealth. Unlike some other societies where there are agencies that investigate ill-gotten wealth. Those people throw about such money anyhow. When the youth see that regardless of how you make your money you are celebrated, we also go into internet hacking. No reward for hardworking… no welfare for unemployed people that are within certain range of age. (P3, Focus Group Discussion 2, June 19, 2019)

Yet another participant justified internet hacking from the standpoint of individual personal factors and societal influence. This was aptly expressed saying:

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

> Internet hacking is related to lack of contentment among youth. The youth want to make it by all means, live a luxurious life at a tender age. Environmental influence that is, the world celebrating those who have made it by yahoo more than those that have made it by diligently working to the top." (P3, Focus Group Discussion 1, June 7, 2019)

This view was corroborated by another participant who said: "*For me, internet hacking is related to prosperity gospel and lack of fear of God, economic influence, poor education, and single parenting. The father is not there to take care of the children*." (P1, Focus Group Discussion 1, June 7, 2019)

Still participants justified internet hacking among youth with reference to the prevailing high unemployment level in the society. In his words:

> For me, I will say unemployment of the youth also contribute to internet hacking. Let me ask you this question, as you do this research, after graduating, you have no job awaiting you with your intelligence what will you do? It makes the youth to start to think otherwise and enter into internet hacking or any other yahoo stuff.(P3. Individual Interview, July 10, 2019)

Lastly, another participant added peer influence to economic factor saying:

> Internet hacking is because of the economy of the country, and peer groups because of need to do what your friends are doing. You know sometimes when you see your friends driving big cars and you are still on the road you will want to be like them too." (P7, Individual Interview, July 11, 2019)

The findings from this current study showed the place of social and moral justification in internet hacking among cybercrime prisoners in Nigeria. With such justifications from social, economic, and moral perspectives, it stands to reason that more youth would join this criminal act if nothing serious is done by the government and the society to correct this trend among youth.

Euphemistic Labeling

This mechanism uses sanitizing language to make harmful activities respectable thereby assuming a different appearance. The participants were unanimous in their admission that the use of varied sanitizing words to describe internet hacking had a great influence on the practice of hacking among youth today. Such euphemistic language include IT work, and brain work.

Using this principle, a participant describing himself as IT worker said: "*If you ask me what is my job before I was arrested I will tell you I am IT expert. I help to secure IT systems, or I do IT work on people's systems*." (P1, Focus Group Discussion 1, June 7, 2019). This view was supported by another participant who said:

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

> I did my master program in Programming in abroad. I came back to Nigeria seven years ago and I have no job. So I employed my knowledge of IT to do IT work in this city and it has been very good. When people ask me about my job I usually tell them I am an IT consultant. (P3, Focus Group Discussion 2, June 19, 2019)

Another sanitizing language used to describe internet hacking by the participants was brain work. This view was expressed by another participant who said:

> For me en, I will not lie to you. Internet hacking na 'is' brain work. Why I say so is because you need to be intelligent and smart to be able to break into a secured IT system and operate without been found out. So I see myself as someone who is using his brain to create what I need to help myself and my family. (P2, Individual Interview, July 10, 2019)

Another participant described internet hacking as a sign of being creative like God the creator. According to him: "*In Genesis we are told when God needed things, he created many things. We the youth need things and we are using our brain to create things too. That is how I see it simple*." (P4, Individual Interview, July 10, 2019)

The responses from the participants agreed that euphemistic labels used to describe internet hacking by the hackers themselves and the society makes hacking appears as a respectable business and more appealing to youth.

Advantageous Comparison

The participants made reference to advantageous comparison in their responses to explain internet hacking. Their responses showed that hacking enjoys a tacit approval by the large society when compared to other crimes in the society. Using the contrast principle, the participants in their responses compared internet hacking against armed robbery, corruption, and kidnapping in the society to give internet hacking a general approval as a better option and a benevolent alternative. Like in other variant of cybercrime in the current study, comparison was made with reference to legal standpoint on hacking, and the punishment due to internet hacking in Nigeria.

A participant made reference to legal stipulation on the maximum terms due to internet hacking compared to other crimes like armed robbery, and kidnapping for ransom in Nigeria. According to him:

> Internet hacking is preferable because the consequences of offence in Nigeria is low is not as high as outside the country. Someone can hack a company account and steal millions of dollars and they sentence them to 7 years imprisonment and outside the

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

> country they can give them life imprisonment. Youth now see it is preferable here. (P5, Focus Group Discussion 2, June 19, 2019)

Another participant corroborated this view saying:

> Internet hacking is much better. When you come to the constitution, where you check internet hacking, kidnapping, and armed robbery, for example, it I hack someone's account and steal his money, the highest is 7 years imprisonment, and if you are not sentenced yet you can be granted bail. But when it comes to armed robbery, kidnapping, this country is more against them than internet hacking. (P4, Individual Interview, July 10, 2019)

Still on why internet hacking is better than other crime for making quick money in the society, a participant said: "*If you want to know which is better, you look at the advantages and disadvantages, you look at the consequences. Like that of cybercrime is lesser than armed robbery and kidnapping even though they are all crime*." (P7, Individual Interview, July 11, 2019)

These findings indicated the place of advantageous comparison in the perpetuation of internet hacking by cybercriminals in Nigeria. With such comparisons, from both legal and economic standpoints, it follows that if nothing is done to arrest this trend, more youth will take to this behaviour of hacking people's account for money thereby inflicting more mental health challenges on their victims.

Displacement of Responsibility

The participants showed the use of displacement of responsibility in internet hacking practices. Most of the responses to the interview questions laid responsibility for internet hacking mainly on the government for youth unemployment and the attendant poverty in the country. The participants were unanimous in this regard as they argued that internet hacking required a good knowledge of IT and most of the hackers are unemployed IT experts and IT undergraduates.

A participant who made reference to the youth unemployment in the country said: "*In expansion to what my brother said is unemployment and also poverty. Like someone who study accounting and after graduation you look for work and no work, and you have knowledge to defraud someone's account, you will defraud*." (P5, Focus Group Discussion 2, June 19, 2019)In the same vein, another participant displaced the responsibility to government, parents and the hackers saying: "*The government should be blamed primarily for internet hacking. Secondarily, parents and those who are engaged in internet hacking.*" (P2, Focus Group Discussion 2, June 19, 2019)

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

Another participant in the group blaming the government for internet hacking made reference to his friend saying:

> The government should be blamed and partially the yahoo guys should be blamed. I know of a graduate that didn't get a job, started thinking of such bad things. Since he did not want to do armed robbery, he simply used his IT knowledge to make money without trouble from police. (P4, Focus Group Discussion 2, June 19, 2019)

A participant explained it from the frustration among youth caused by the prevailing youth unemployment saying:

> I will still put the blame on the government because as a father, you spent a lot of money on your child from nursery school to higher institution. Still yet, your son has graduated there is no job. This can lead to frustration and desperation to do something which can bring money like internet hacking. So I will still blame the government for no job. (P3, Individual Interview, July 10, 2019).

Emphasizing this point further another participant said:

> For me ooh, the government should be blamed to a very great extent because before many of these boys that are involved in internet hacking are graduates. After staying long in our labour market, no jobs, they will go into internet hacking as plan B which is still a better alternative of making money than robbery or kidnapping. (P6, Individual Interview, July 11, 2019)

These explanations offered by the participants tend to portray the internet hackers as victims of circumstances beyond their control which is youth unemployment and poverty in the country. Thus with responsibility for the ills of internet hacking comfortably laid on everyone except the hacktivists themselves, they will most probably continue in their act until they are made to take responsibility for their action regardless of the compelling situations.

Dehumanisation

The participants showed their use of dehumanisation mechanism in their responses to the interview questions. Findings showed that participants used this principle in their dealings with the victims of internet hacking since in most case they don't need to have prior personal contact with their victims. This act was made possible with the anonymity of the cyber space and the desire for quick money by the participants, and revenge for perceived past wrongs. Explaining the influence of the anonymity of the cyber space in dehumanisation of the victim, a participant said:

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

> In IT, there is what we call Cesspit Obscurity. What I mean is you don't have a feeling or emotions because you don't see the countenance of the person. So victims go to the extent of emptying their accounts or commit suicide. So the person committing the crime does not know what the person have in his account or how they feel hence the criminal is meant not to feel compassionate about it. (P3, Focus Group Discussion 2, June 19, 2019).

Still on the anonymity create by the cyber space and its influence on dehumanisation of victims of internet hacking, another participant said: "*Cyber space is a small village. It provides an avenue to defraud someone you never know. It allows deceits and we don't feel the pain because you don't see this person*." (P3, Focus Group Discussion 1, June 7, 2019)

On internet hacking as a business, a participant said:

> I feel that we don't feel remorseful because it is our business. Everybody is serious with his own office or business where you get money because it is pure business. Person should not feel remorseful for succeeding in business. Look, I hope you are not trying to stop peoples' business?" (P5, Focus Group Discussion 2, June 19, 2019)

Another dimension of internet hacking as revenge for past and present wrongs committed against Africans by the Whites was reported by one of the participants who said:

> Why I can fraud outsiders than Nigerians is because of what happened in the past, like slave trade and colonialism. Even up till now, US, China and Europe, they don't like Blacks they see us like monkeys. I prefer to dupe them to show them that Africans have brains, we are humans we are not animals and monkeys cannot dupe humans (P4, Individual Interview, July 10, 2019)

Lastly, a participant made reference to the influence of too much suffering on one's ability to show empathy to others saying: "*Yahoo boys don't feel compassionate because someone that has suffered too much is ready to do anything for the money even if the owner of the money commit suicide it does not concern them*" (P2, Individual Interview, July 10, 2019).

DISCUSSION

This study found a strong positive and statistically significant relationship between moral disengagement and internet hacking ($p < 0.01$, $r = .718$). This means that as moral disengagement increases, internet hacking among youth also increases. In-depth explorations from the qualitative strand revealed a strong relationship between moral disengagement and internet hacking with moral justification, euphemistic labeling, advantageous comparison, displacement of responsibility and dehumanisation as the most used moral disengagement mechanisms. Thus, this study found congruence between the quantitative and the qualitative strands of this study on

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

the relationship between moral disengagement and internet hacking. Moreover, the narratives from the interviews revealed that internet hacking is mainly practiced by people who possess some level of training in IT and computer programming. This means that internet hack is much complex than the other forms of cybercrime hence not every cybercriminal could practice it. This study found that the lucrative nature of internet hacking together with corruption, unemployment, peer influence, prosperity gospel in the churches, get-rich-quick syndrome and poor family and societal values all contribute to the prevailing moral disengagement which in turn influences internet hacking among the participants.

The findings are consistent with Hsu and Pan (2018) which showed that advantageous comparison and non-responsibility were the significant predictors of students' misbehaviours in physical education among Taiwan student. In the same vein, findings from this study are consistent with Young and Zhang (2014) which indicated a strong negative correlation between individual's commitment to conventional activities, belief in following the norms of the society, and the likelihood to engage in illegal hacking behaviour. This showed the influence of moral disengagement not only in internet hacking but in other types of crime in different society. Also the findings resonate with Madarie (2017) which indicated that, there is strong positive relationship between aversion of conservation values and the motivations to hack. The findings re-echoed the results of Oluwasoye and Thorne (2015) that, cognitive reconstrual of acts (justification, euphemistic labeling, and advantageous comparison) were the most commonly employed morality among Niger-Delta oil militants in Nigeria. This means that, efforts to promote moral engagement and prevent internet hacking among youth will need to take into consideration the individual's cognitive factors. Moreover, the findings are consistent with the theoretical framework of the present study which holds that, a combination of individual personal factors, environmental, and behavioural factors influence despicable behaviour (Bandura, 2016). Furthermore, findings supported the tenets of Space Transition Theory that people behave differently when they move from the physical space to cyberspace aided by the anonymity offered by cyber space (Jaishankar, 2007). This attest to the cross cultural nature of the influence of moral disengagement in internet hacking and other crime in the society.Suffice to reiterate here that scanty literature on the influence of moral disengagement oncybercrime in general and internet hacking in particular both within Nigerian and African context meant not much literature was available for the review of the findings. It follows therefore that findings from the current study serves dual purposes. First, the current findings represent seminal work on moral disengagement and internet hacking in Nigeria and African context. Second, it contribute immensely to the growing literature on the influence of moral disengagement on despicable behaviour in Nigeria and the global context among youth.

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

CONCLUSION AND RECOMMENDATIONS

From the results, this study concludes that moral disengagement has a strong influence on internet hacking among the sample. This implies that, the individual's moral disengagement, the lucrative and highly rewarding yahoo plus with non-commensurate legal deterrents and the enabling environmental factors like anonymity of the cyber space, corruption, unemployment, peer influence, get-rich-quick culture, low parental and societal values all interface to influence one another. The study also concludes that social cognitive theory, offered a good theoretical framework for understanding, explaining and intervening internet hacking. Lastly, the study found congruence between the qualitative and the quantitative strands in this study. The qualitative data corroborated findings in the quantitative strand indicating the use of different mechanisms of moral disengagement in perpetuating the different variants of cybercrime.

The study made recommendations in three broad areas of theory, practice, and policy formulations. On the aspect of theory, findings from this study on the influence of moral disengagement on internet hacking indicate there is the need to review the present curriculum to promote moral engagement among pupils and students at various levels of education in the country. The government could use the findings of this study to initiate youth-oriented policies in the form of social welfare scheme for different categories of unemployed youth. This will help cushion the effect of the present mass unemployment, and current economic hardship which the study found to influence cybercrime practices among youth. This could also include the creation of employment opportunities to the teaming unemployed graduates in the country as majority of the participants were unemployed but educated youth.

Psychologists especially those working with correctional facilities could use the findings to come up with treatment plan to address the influence of moral disengagement on the individual's disposition toward internet hacking and other crimes in the society. This will both promote and enhance capacity for moral engagement of the prisoners when faced with situational factors which can encourage moral disengagement and cybercrime. This will go a long way to prevent the effect of recidivism on crime among youth.

The government should strengthen its anti-corruption agents in the fight against corruption. The government must therefore be seen not only to be fighting corruption but above all, it must eschew corruption from its rank and files. This implies that the fight against corruption must necessarily begin from the government itself. This will again promote moral engagement and prevent or reduce internet hacking among youth. Moreover, government could come up with a national orientation programme to help redirect the value system from pro-moral disengagement orientation (corruption across the social strata, wealth without work, and culture of short horizons) to pro moral engagement orientation in the country. Lastly, to address internet hacking

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

(the behavioural dimension), government should strengthen their cyber security network, and through legislation impose stiffer penalties in the law for corrupt practices and cybercrime related offenses in the country. This would make the punishment strong enough to serve as deterrent to the behaviour thereby ensuring extinction or at least the reduction of internet hacking among the youth in the country.

REFERENCES

Adeniran, A. (2008). The internet and emergence of yahoo boys sub-culture in Nigeria. *International Journal of Cyber Criminology*, *2*(2), 363-381.

Ajaegbu, O. (2012). Rising youth unemployment and violent crime in Nigeria. *American Journal of Social Issues and Humanities*, *2*(5), 315-321. doi: 10.1.1.684.5857.

Ajayi, E. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, 6(1), 1-12, doi: 10.5897/JIIS2015.0089.

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Piotr Kijewski, P. (2015). 2020 Cybercrime Economic Costs: No measure No solution, 10th International Conference on Availability, Reliability and Security. *CYBERROAD PROJECT* (pp. 701-710). London: Conference Publishing Services.

Bandura, A. (2016). *Moral disengagement: How people do harm and live with themselves.* New York: Worth Publishers.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs, NJ: Prentice-Hall.

Bandura, A., Barbaranelli, C., Caprara, G.V., & Pastorelli, C. (1996). Mechanisms of moral disengagement in the exercise of moral agency. *Journal of Personality and Social Psychology*, *71*(2), 364-374.

Creswell, J. (2007). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research (4th ed.).* Boston: Pearson.

Economic and Financial Crimes Commission. (2012). *Economic and Financial Crimes Commission Quarterly Reports.* Abuja: EFCC.

Eigbadon, E., & Adejuwon, A.G. (2015). Psychodemographic factors predicting internet fraud tendency among youth in Southwestern Nigeria. *Journal of Educational and Social Research*, *5*(2),159-164. doi:10.5901/jesr.2015.v5n2p159 .

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

Haslam, N., & Loughnan, S. (2012). Prejudice and dehumanization. In J. Dixon & M. Levine (Eds.), *Beyond prejudice: Extending the social psychology of conflict, inequality and social change* (pp. 89-104). Cambridge: Cambridge University Press.

Hsu, W.T., & Pan, Y.H. (2018). Moral disengagement and student misbehaviour in physical education. *Journal of Sports Science and Medicine,17*, 437-444.

Jaishankar, K. (2007). Establishing a theory of cyber crimes. *International Journal of Cyber Criminology*, *1*(2) 7-9.

Lutz, W. (1987). Language, appearance, and reality: Doublespeak in 1984. In D. Boardman (Ed.), *The legacy of Charlton Laird* (pp. 103-119). Reno: University of Nevada Press.

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017). Flipping 419 cybercrime scams: Targeting the weak and the vulnerable. *International World Wide Web Conference Committee*, doi.org/10.1145/3041021.3053892.

Madarie, R. (2017). Hacker's motivations: Testing Schwartz's theory of motivational types of values in a sample of hackers. *International Journal of Cyber Criminology*, *11*(1), 78–97. https://doi.org/10.5281/zenodo.495773

McGuire, M., & Dowling, S. (2013). *Cyber-crime: A review of the evidence, summary of key findings and implications (Home Office Research Report 75).* London: Home Office

Milgram, S. (1974). *Obedience to authority: An experiemntal view.* New York: Harper and Row.

Oluwasoye, P.M., & Thorne, S. (2015). Oil terrorism-militancy link: Mediating role of moral disengagement in emergency and crisis management. *Journal of Emergency Management*, *13*(5), 447-458. doi:10.5055/jem.2015.0254.

Oumarou, M. (2007). Brainstorming advanced fee fraud: 'Faymania'—the Camerounian experience. In I. N. Ribadu, I. Lamorde (Eds.). *Current Trends in Advance Fee Fraud in West Africa,* (pp. 33-34). Abuja: EFCC.

Suleman, L. I. (2018). Birds of a feather flock together: The Nigerian cyber fraudsters (yahoo boys) and hip hop artists. *Weatern Criminology Review, 19*(2), 63-80.

Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, *5*(2), 860-875.

Wang, X., Lei, L., Yang, J., Gao, L., & Zhao, F. (2017). Moral disengagement as mediator and moderator of relation between empathy and aggression among Chinese male juvenile delinquents. *Child Psychiatry and Human Development*, *48*(2), 316-326.

ISSN: 2455-8834

Volume: 05, Issue: 07 "July 2020"

Wainwright, R. (Executive Director of Europol). (2017). *Internet organized crime threat assessment (IOCTA).* Hague: Europol, European Cybercrime Center doi 10.2813/55735.

Young, R., & Zhang, L. (2014). Illegal computer hacking: An assessment of factors that encourage and deter the behaviour. *Journal of Information Privacy and Security*, *3*(4), 33-52. https://doi.org/10.1080.15536548.2007.10855827

