Algerian Journal of Management Sciences (AJMS) Vol. 03, N°01 (2024), pp1- 17
ISSN : **2830-8115**

SOCIAL LEARNING AND CYBERCRIME IN NIGERIA: A SOFT SYSTEMS METHODOLOGY APPROACH

Francis E. ANDEM[1]
Bus. Mgt Dept, University of Uyo, Nigeria.
Francisandem.pgs.phd@uniuyo.edu.ng
0000-0001-7713-3571
Prof. Isaac A. AYANDELE[2]
Bus. Mgt Dept, University of Uyo, Nigeria.
yinksure@yahoo.com
0009-0004-3486-3151
Francis I. OGOSI[3]
Mgt Science Dept. Western Delta University, Delta State, Nigeria.
Francis.ogosi@wdu.edu.ng
0000-0002-3892-4175
Rupert A. INWANG[4]
Marketing Dept, University of Uyo, Nigeria.
Aniekanrupert@mail.com
0009-0004-5320-6093

Date de Réception : 03/04/2024	*Date d'acceptation :27/05/ 2024*	*Date de Publication :25/O9/2024*

Abstract: Social learning is still useful in explaining criminal behaviour. Cybercrime is on the increase in Nigeria, with a 537 per cent growth in attacks on commercial banks alone in 2017. Cybercrime in Nigeria is heterogeneous; therefore, cybercrime studies interest policymakers, businesses, and researchers. This study used the Soft Systems Methodology (SSM) to assess cybercrime in Nigeria within the framework of social learning. SSM revealed incentives for cybercrime and actions needed for cybercrime deterrence. Some incentives revealed in the study include poor family religious attitude, unemployment, poor law enforcement capabilities, poor legal framework, and victims' vulnerabilities. Incentives create a favourable environment for cybercrime growth. We found that improved government actions in legislation, law enforcement, and socio-economic conditions will lead to cybercrime deterrence. Further findings revealed that an improvement in awareness, knowledge, and information on cybercrime will reduce victims' vulnerability to cybercriminal attacks. We conclude that SSM can provide a holistic method for solving the cybercrime problem in Nigeria. It brings out definitive actions to be taken by actors toward cybercrime deterrence in Nigeria. We recommend the use of SSM in solving unstructured cybercrime problems in Nigeria.

Keywords: Learning, Cybercrime, Systems Thinking, Action, Deterrence
JEL Classification Codes: I18; I31; H28; M38; M14; Z18

[1] Corresponding author: E-mail: Francisandem.pgs.phd@uniuyo.edu.ng

1.0 Introduction

1.1 Background to the Study

The Social Learning notion evaluates the learning process in individuals, groups, and society. It assesses how we acquire social behaviour through observation and imitation of others. Social learning thrives in favourable environments with high ability and propensity to observe, model, and imitate others. This learning process influences our behaviours, attitudes, and emotional counteraction. It creates an understanding of the interaction between the learning environment and cognitive factors, which is geared towards influencing human learning and behaviour. As a result, it creates a system of thinking that human behaviour is because of imitating and modelling (Resnick, 2012). It can also lead to learning the consequences of an action (Hunter-Reel, 2013). Accordingly, individuals' capabilities to act and defend actions are also parameters for adjusting behaviour. In doing so, they seek self-efficacy to control their capabilities and gain confidence for action. Social learning explains this process by highlighting capabilities through encoding, organizing, and retrieving information in cognitive processes (Hunter-Reel, 2013). The cognitive process is the easiest way to influence behaviour and create an understanding of environmental events. It is determined by how individuals interpret information from their environment (Li and Tan, 2020; Gong et al, 2014). In this process, an individual can self-regulate by developing the ability to identify and arrange environmental incentives. They weigh these incentives against the perceived application of consequences through the justice system, law enforcement, and threats to social (family) life. In reality, self-regulation is not restricted to one's ability to select how to react in specific situations; it also applies to decision-making capabilities in response to the impact of exposure to specific stimuli. The crux is that social learning explains an individual's criminal behaviour and offers explanations for cybercriminal behaviour in Nigeria.

Cybercrime is a learned behaviour. It requires sophisticated and extensive learning. The criminals do this learning through observation, imitation, and adaptation. Any cybercrime requires the use of a computer (or similar devices) as a weapon or a victim. Therefore, cybercrime is any crime committed on the internet using the computer and internet as a tool or as a targeted victim (Bello, 2017; Omodunbi et al., 2016). Frequently committed cybercrime in Nigeria are fraudulent electronic mail, unsolicited pornography, identity theft, hacking, cyber harassment, spamming, spoofing Automated Teller Machines, piracy, and phishing (Omodunbi et al., 2016). There is an increase in cybercrime globally and in Nigeria. In Nigeria, commercial banks lost a cumulative of fifteen billion naira in 2018 which was far over the 2.37 billion naira loss recorded in 2017. This shows a 537 per cent increase in cybercrime against commercial banks alone. Also, over 17 600 bank depositors and customers lost N1.9 billion due to cyber theft, showing a 55% rise from the previous year (Ogbonnaya, 2020). This situation will not change as long as there is an increase in internet usage, Information Communication Technology (ICT) knowledge, and extravagant human need. It is predicted that by 2030, Nigeria's cybercrime loss will rise to US$6 trillion through phishing and identity theft. This will continue as our social interactions, which influence our moral definitions and desires, move mostly online (Dearden and Parti 2020). Nigerian youth are mostly the ones involved in cybercrime (Ibrahim et al. 2020). This is so because most young people have gained sophisticated information and communication technology skills without being able to do a job to utilise such skills. This provides incentives in the Nigerian socio-economic environment and "*reasonable*" justification to engage in cybercrime. Omeire and Omeire (2017) suggested that the socio-cultural pressure on youths to succeed financially resulted in the establishment of cybercrime as a subculture in Nigeria. Therefore, the improvement in the sub-culture has led to growth in sophistication. It has made it difficult to enforce laws and policies that will lead to its reduction. Thus, awareness of their strength, tactics, and intentions for victims, law enforcement, family, and government can create a learning system that systematically heals itself

and reduce cybercrime in Nigeria. The Soft Systems Method (SSM), as developed by Peter Checkland, can offer an opportunity to model and consistently improve such a learning system. It has proven its effectiveness in offering an organised method of defining and taking action to improve unstructured problem situations (Ebrabimi, 2020).

Problems posed by cybercrime in Nigeria are messy, unstructured and unconventional. Soft Systems Methodology suits restrictive learning and improves traditional change management of social systems (Asadi, 2020). It tackles complex, messy, and unstructured problems (Hindle, 2011). SSM offers a holistic analysis that will lead to the identification of active stakeholders; showing their interactions; and relationships. Furthermore, the SSM structure stirs discussion between stakeholders (Hindle, 2011). Therefore, these capabilities of SSM will create a structured social learning system among stakeholders of cybercrime in Nigeria. It is action research that will stir discussions on cybercrime posture and corrective actions needed (Checkland, 2000). The goal is to discover methods for comprehending and overcoming the complex challenges of acting as people, organizations, entities, and society to ameliorate the messy condition brought on by our everyday lives and ongoing changes (Asadi, 2020; Checkland, 1996; 2000). Cybercrime in Nigeria is on the geometrical increase and social learning only offers useful explanations for cognitive, behavioural, and environmental factors influencing cybercriminal behaviours without direction. Therefore, this paper intends to apply soft systems thinking in evaluating cybercrime in Nigeria to give direction towards the reduction of cybercrime in Nigeria.

1.2 Objective of the study

This study's major objective was to investigate social learning and cybercrime in Nigeria using the Soft Systems Methodology. In particular, the project aims to:

i. Model a Soft Social Learning System that can enrich cybercrime deterrence in Nigeria.

1.3 Research Questions

i. The major research question was:

ii. (i) Can Soft Systems Methodology model a Soft Social Learning System to enrich cybercrime deterrence in Nigeria?

2.0 Literature Review

2.1 Conceptual Framework

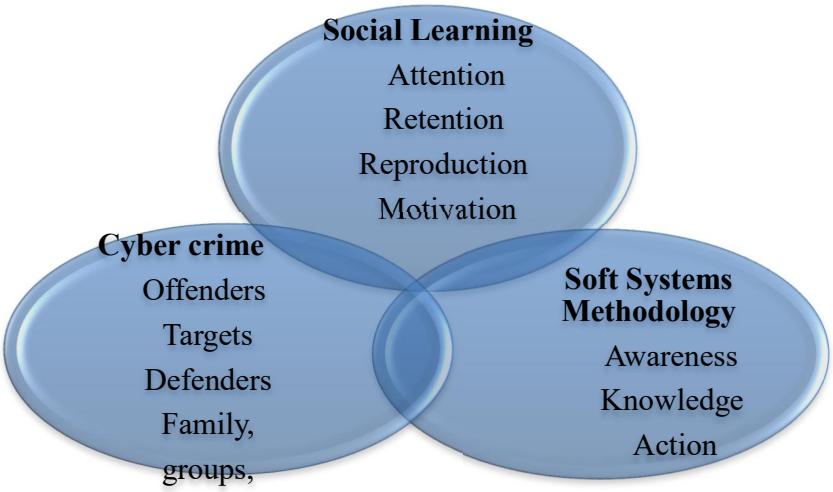
The general idea of Social Learning is that individuals learn to behave in a certain pattern when they observe others and imitate their behaviour. In doing this, the individual observes action and the consequences of actions taken by others (Berge, 2012). The observer views the consequences through environmental factors such as norms, moral justification, parents' religious attitudes, and so on. Social Learning explains these using four components namely: attention, retention, reproduction, and motivation (Figure 2.1). In Attention, the individual's interest focuses on an event to initiate learning. Second, Retention specifies that an individual must store learning from observed behaviour to remember and model such behaviour. He enhances this through imagery and mental models. Soft systems thinking offers capabilities for intervening and regulating mental models positively. Third, Reproduction involves the translation of learned social behaviour into action. Last, Motivation occurs if something, circumstances, and scenario associated with the individual provide incentives for action. SSM analysis offers an enriched picture that defines scenarios that will trigger involvement in cybercrime and conceptualise actions to mitigate them.

Cybercrime is a learned behaviour acquired through social learning. In essence, there is an interrelationship between social learning and cybercrime although social learning does

not show direction for action. Any crime or aberrant behaviour committed using a computer or information system as a tool or as a target is referred to as cybercrime. Computer and information systems are frequently used in a wide variety of criminal acts, either as a major tool or as a primary target (Bendiek et al, 2017). According to the definition, cybercrime includes traditional offences like fraud, forgery, and identity theft as well as offences involving content, like the online distribution of child pornography or the incitement of racial hatred, as well as offences specific to computers and information systems (such as attacks against information systems, denial of service and malware). It also includes cyber-dependent and cyber-enabled crimes including bullying, stalking, and sexual grooming (Hull et al, 2018). These crimes form a complex whole of actors – a system. The cybercrime system consists of the offender (criminals); victims (humans, businesses, and computers); defenders (cyber security experts, law enforcement, and government), and family (of offenders and victims). The interactions of these components are unstructured and cannot be defined by a simple structured framework. It is even more difficult to define and predict dynamic changes in sophistication.

Soft Systems Methodology (SSM) was developed by researchers at Lancaster University credited to Peter Checkland (Checkland, 2000). SSM has proven to be effective in offering an organised method of defining and taking action to improve a messy problem situation offered by cybercrime in Nigeria (Ebrahimi, 2020). It is an "action research" which creates a practical and pragmatic approach to identifying and solving "soft" "messy" and ill-structured society's problems (Burge, 2015). In recent times SSM is used as a learning and meaning development tool (Williams, 2005; Burge, 2015; Ebrahimi, 2020; Salavati et al, 2021). It was created as a set of tools for detecting and improving situations with ill-defined causes (Tsuro and Hardman, 2020). Thus, Soft Systems Methodology detecting and improving capabilities can regulate social learning by detecting causes of cybercriminal behaviour and providing insight towards improving cognitive learning and defining actions to be taken by stakeholders for a holistic improvement of the systems. Consequently, SSM can reduce cyber victims' vulnerabilities through improve knowledge, awareness, and action (Ho and Luong 2022; Abdullah and Jahan, 2020). This will increase their resistance to Cyber-attacks. Also, the sociocultural outlook toward cybercrime in Nigeria will be enhanced through improved systems and models (Li et al, 2022).

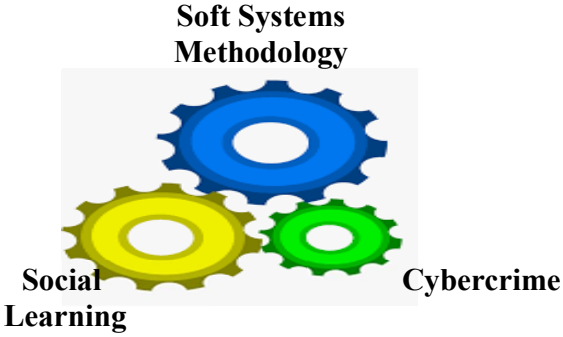
Figure 2.1: Conceptual Frame work adapted from Caulkins (2017)



Source: Authors' Construct (2024)

Caulkins (2017) argued that a Venn diagram is a useful tool for representing the discussed interrelationships. Therefore, Figure 2.1 defines the interrelationships that exist between social learning, cybercrime, and Soft Systems Methodology. The intersection of the Venn diagram shows that there are actions, activities, or components in the variables that overlap each other. However, a more practical look is viewing the elements as mechanical gears (see Figure 2.2)

Figure 2.2: Proposed Modification



Source: Authors' Construct (2024).

Figure 2.2 is the proposed modification of the social system. Learning cybercrime behaviour through social learning created a system that is not regulated and controlled. A third gear, soft systems methodology is introduced to improve the system and regulate the actions of the stakeholders.

2.2 Theoretical Framework

Two theories give impetus to this study: Social Learning Theory and Systems Theory.

2.2.1 Social Learning Theory (SLT)

A useful theoretical foundation for the study of criminal behaviour has been provided by the Social Learning Theory (SLT), a cognitive and behavioural approach (Black and Mendenhall, 1990; Morris and Robie, 2001). SLT was first proposed by Bandura (1977), who identified four essential elements: rewards, retention, reproduction, and attention. The setting gives cybercriminals incentives to carry out assaults with a sense of positive reward. According to the social learning theory (SLT), people who associate differently with criminals; are exposed to more delinquent models; expect or receive more rewards and fewer punishments for cybercrime, and have a greater number of definitions favourable to cybercrime are likely to engage in it. The social structure-social learning paradigm, which was recently formed by combining SLT with social structural ideas, is the foundation of many delinquency preventions and offender treatment programs (Ward and Brown, 2015).

The concepts of behaviourist operant learning were combined with other psychological theories that emphasized imitation and vicarious learning as a theory of criminality to create social learning theory. Differential association theory was reconstructed by Ronald Akers and colleagues as an operant learning theory in 1966, and Akers and associates later created a more comprehensive social learning theory. The social learning hypothesis has undergone more empirical research than any other delinquent theory (Jesen, 2015). Social learning theories stress other actors a lot (Spivak and Howes, 2011). But research keeps demonstrating that parents and family can have an impact

on pro-social behaviour (Grusec, 2020). The Social Learning Theory investigates how social cues affect cognition and behaviour. An observer will copy a person's actions if they receive praise for them or avoid behaviour if there are negative outcomes. SLT shows that socialization, culture, and the media all have a role in the formation of behavioural expectancies.

The social learning theory is mostly criticized for assuming passivity in the form of the observer who receives rewards or penalties. It also fails to explain why certain people would not adhere to social standards or why particular behaviours are rewarded or punished (Jensen, 201). Soft systems thinking (SST) is a different way of thinking that addresses some of these challenges by emphasizing individual behaviour rather than the collective behaviour of the connected pieces.

2.2.2 Systems Theory

Due to its failure to provide a larger study of the "generic System," the General Systems Theory (GST) has failed in its application of a holistic approach to the idea (Checkland, 2000). This failure does not in any way suggest that systems thinking have failed; rather other components of systems thinking have flourished beyond anticipation since 1954. Maturana and Varela (1980) created one of these improved systems thinking components, which offer a way to articulate the core of an autonomous living system without relying on an observer's conceptions of "purpose," "goal," "information processing," or "function." It departs from Miller's Living Systems (1978), which offers a general representation of a living creature presented in the observer-centric language without emphasizing what gives the entity autonomy. A good illustration of how systems concepts can be expanded upon and the subject of systems theory concerning this work is Maturana and Varela (1980). The ability of the autonomous system to self-regulate and repair malfunctioning system components is stressed. One example of how systems thinking can be applied to illuminate a particular subject area is Chorley and Kennedy's (1971) reinvention of physical geography as the study of the dynamics of four different types of systems. This study is an example of the third form of development, which Peter Checkland (2000) described as a combination of the first two types. The goal was to see if soft systems thinking, which is a broad definition of systems thinking, could help in resolving the complex problems of change management

2.3 Empirical Review of Related Literature

A summary of cybercrime and cyber-security was attempted by Ibekunle and Odunayo (2013). They displayed those participating and their motivations, revealing that socioeconomic factors were the main driver of involvement in cybercrime which led to exponential rise of cybercrime in Nigeria (Omodunbi *et al*, 2016). Odoyo, *et al* (2020) held the opinion that security needed to be improved to keep up with the escalating problems caused by cybercrime. They discovered that social learning includes elements of acquiring cultural information, skills, attitudes, tactics, rules, and beliefs; and the need for a proactive framework for combating cybercrime. This can be accomplished by adopting a social learning perspective using standardized practices in law-making, investigative techniques, certification, and cybercrime investigator training. They drew attention to how various parts are interconnected, how they have an impact on the individual parts, and how a comprehensive framework is necessary.

Igba *et al*. (2018) contend that financial stress is a contributing factor in youths' participation in cybercrime. Using 207 students from their institution, their findings showed that students view cybercrime as a tool for professional growth. Igba *et al* (2018) showed that learning is required to model behaviour, while Cundril, *et al* (2012) observed that social learning theory and soft systems thinking reveal flaws in the underlying assumptions that complex systems can be managed by observers' objectives. Instead, their concepts demonstrate that social process and engineering are better managed through adaptive management - a learning system that is allowed to set its objectives and tentative ideas become a source of enriched ideas and actions. They held that complex social interactions are defined by activities taken toward a common objective, which

will eventually result in the introduction of new information, alternative values, and novel worldviews. Cybercrime is a rapidly expanding area of crime. People, the government, and society had all suffered significant harm from cybercrime and unless immediate action is taken to eliminate it, cybercrime will destroy nations. Adopting a comprehensive strategy to safeguard countries like Nigeria from the devastation caused by cybercrime is of need (Bello, 2017). Nigerian cybercrime has many different forms. Ibrahim, *et al* (2020) looked at these forms and prevention strategies. They suggested that the government improve the socioeconomic status of youths because they are the most prevalent. Olayemi (2014) aimed to investigate the societal and technological elements affecting it. Using interviews with law enforcement and governmental organizations that deal with cyber security to better understand the motives, objectives, and techniques of Nigerian cybercriminals, he claimed that Nigerian legislation does not currently contain any laws that specifically address cybercrime.

Despite this gap, Okeshola and Adeta (2013) suggested that agents should adopt a culture of lifelong learning to keep up with the dynamic state of cyberspace. By doing this, they reasoned, users will be well-informed about current trends in cybercrime, various sorts of crime, and the methods used by cybercriminals to commit their horrific acts. As a result, they can lower the likelihood that thieves will succeed. Also, Eke and Ofoeze (2020) saw that information and communication technology has made it possible for people to constantly learn to keep up with the demands of an evolving social and economic system. They claimed that Nigeria is losing the ability to combat cybercrime because of inadequate funding for the investigation of cybercrime. According to Lahcan*, et al* (2020), cyber law enforcement must be improved as a result of the increasingly skilled hackers. They concur that focusing on social and behavioural issues will yield better outcomes in our efforts to make the current situation better. They contend that people work best in a learning environment offered by the Soft Systems Methodology.

Dearden and Parti (2020) believed that social learning theories would explain how the moral definitions and motivation for crime are influenced by the people we associate with. Using a countrywide online sample of 1,109 participants, they observed that social learning has a significant impact on cyber-offending. They concluded that social learning can predict the reduction in cyber offences. Ibrahim (2016) sought to identify the unique characteristics of cybercrime in Nigeria and determine whether these indicate issues with the current taxonomies of cybercrime. He contends that geopolitical, sociological, and socioeconomic concerns can all be used as justifications for cybercrimes and that a better understanding of cybercrime is required in Nigeria. To create more understating, Ezekiel, *et al* (2021) focused on the historical assessment of cybercrime in Nigeria. Their findings showed that cybercrime is linked to a desire for wealth, a lack of enforcement of cybercrime laws, and corruption. They showed that Nigeria's growth is affected by cybercrime. Eya and Odo (2019) discovered in their study that 44.3%, 14.3%, and 14.3% of respondents concur that youth involvement in cybercrime is determined by unemployment, poverty, and a lack of internet security respectively. They proposed that through learning about the risks, repercussions, and hazards associated with cybercrime, deterrence can be archived. Omeire and Omeire (2017) observed the formation of a cybercrime subculture in Nigeria is a result of sociocultural pressure on youths seeking financial success. They posit that unemployment and structural inequalities in the country are the main causes of cybercrime and suggested that value re-orientation, the enactment of suitable legislation, and job development will deter cybercrime involvement. Ogunjobi (2020) added that youth involvement in cybercrime is primarily caused by unemployment, poor governance, and poverty. Hamisu *et al* (2021) revealed that despite government efforts, the threat of cybercrime in Nigeria is still high, as criminals continue to take advantage of flaws in socio-technical systems. Sule et al. (2021) observed that

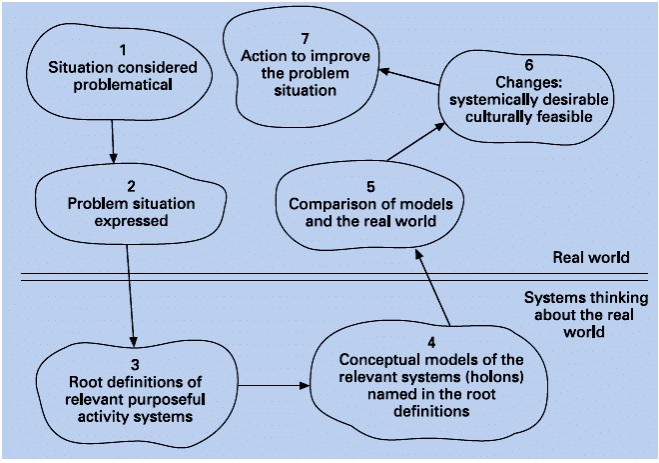
cybercrime is unchecked and thriving in Nigeria. They believed a learning system in an online environment will deter cybercrime. The question is, can SSM improve help?

Sharma, *et al* (2019) argued that the SSM technique being questioned for its lack of "rigour" and "replicability is its strength and usefulness. They asserted that quantitative modelling is unlikely to produce a greater understanding of intricate socio-technical systems. Mendeley (2015) observed that SSM is a systemic tool for locating and analysing stakeholders at numerous levels of a socio-technical system. The Soft Systems Methodology (SSM) will fit the required solution since it moves between the world of systems and the observed reality (Torres, 2018). SSM defines a set of activities for people to engage in with the environment to identify the factors with which it interacts (Torres, 2018). Dynamic internet environments create new opportunities for criminal behaviour (Marttila *et al*., 2021). Victims' vulnerabilities also induce cybercrime victimisation (Ho and Luong, 2022). Helping victims learn resistance will deter cybercrime.

A key element in cyber deterrence is law enforcement, Abdullah and Jahan (2020) explored the difficulties in cyber policing and discovered that standard crime recording is ineffective in detecting gang culture, commercial victimisation, and digital fraud. In addition, they cited equipment and gadget shortages, command responsibility, disciplinary impediments, and electronic evidence as major obstacles in crime policing. They suggested a proactive strategy to help reduce cybercrime. Ebrahimi (2020) sought to create understanding on the use of SSM as an intervention measure in optimising change by highlighting the big picture and the effects of actions in a larger environment and offering practical, long-term, and sustainable solutions. Additionally, Asadi (2020) demonstrated how SSM was applied to limit and enhance conventional change management. He saw that SSM's strength lies in its participatory nature, which is fostered by active engagement from all parties concerned. It heavily relies on the knowledge of the actors. Irawan and Samsunyadi (2019) established that the aim is to increase, process, and use the current to provide value to the entity to achieve its objectives. In all these, Soft System Methodology can enhance understanding of social learning systems that will lead to cybercrime deterrence in Nigeria.

3.0 Soft Systems Methodology

Figure 3.1: The Seven Steps of Soft Systems Methodology



Source: Google.com (2024)

The Soft Systems Methodology (SSM) was developed as a result of research done at Lancaster University on applying systems engineering techniques to address

"management/business difficulties" where mathematical (Hard) systems had failed. The key contributors to the development of the SSM are Peter Checkland (1999) and Brian Wilson (2001); who put together a practical and pragmatic approach to solving ill-defined problems. Checkland and Wilson devised a collection of tools that makes this strategy more than just a method. Figure 3.1 depicts the seven steps in the SSM strategy. It displays seven different system thinking methodologies. Guiding decision-making on how to respond to the unstructured problem, SSM converts chaotic real-world disagreements into defendable and logical models that can be compared to the real world. They are pictures of needed improvement; unfortunately, the SSM language is not widely spoken.

From Figure 3.1, the bottom half of the image represents abstract systems thinking, whereas steps 3 and 4 involve constructing conceptual models for the necessary actions. Figure 3.1's upper portion deals with the real world, starts on the left with an analysis of what one should consider. The right-hand side is focused on what may be done constructively using the knowledge discovered by contrasting logical Conceptual Models with the actuality experienced.

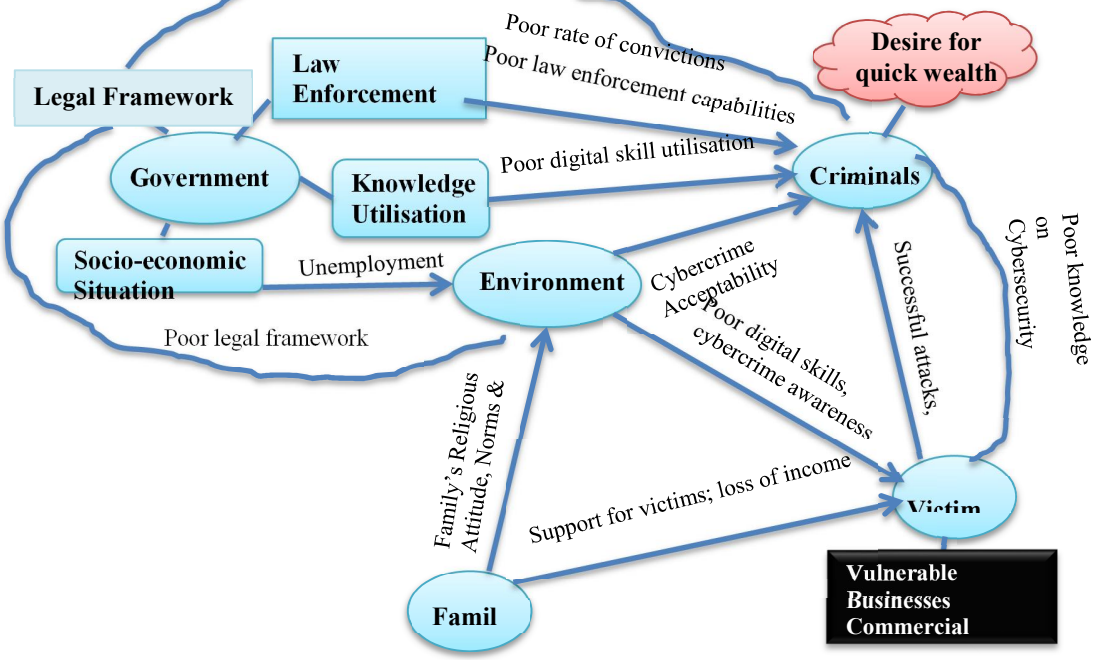
4.0 The Analysis of Social Learning and Cybercrime using SSM Stages

Stage 1: Unstructured Cybercrime Situation in Nigeria

Cybercrime is growing geometrically in Nigeria both in dimension and the number of successful attempts by cybercriminals. The spiritual and cultural support of cybercrime in Nigeria makes the situation messy and unstructured such that conventional and mathematical (hard) systems are failing in creating understanding and bringing the needed solution. The sophistication and dynamic development of these criminal agents outshines law enforcement capabilities and even increase the vulnerabilities of victims because of low digital knowledge. The poor legal and regulatory frameworks worsen the cybercrime situation in Nigeria. In reality, poor socio-economic conditions have made cybercrime a subculture

Stage 2: Problem Situation Analysis (Rich Picture)

Figure 3.2: Rich Picture of Cybercrime in Nigeria



Source: Authors' Construct (2024)

Figure 3.2 shows a rich picture of the cybercrime problem situation in Nigeria. It is a diagrammatic way of exploring, acknowledging, and defining the messy problem situation. Cybercrime is flourishing in Nigeria undetected (Sule *et al*, 2021; Bello, 2017; Omodunbi *et al*, 2016). There is poor equipment for the detection and prevention of cybercrime in Nigeria (Omodunbi *et al*, 2016). This creates vulnerabilities for businesses, commercial banks, and individuals in Nigerian Cyberspace. These victims of cybercrime are losing a huge amount of money which creates incentives for criminals who want to get rich quickly through cybercrime. Most cybercriminals are youths between the ages of 18 – 45years within productive age (Ibrahim *et al*, 2020; Ogunjobi, 2020). Socio-economic conditions such as unemployment, poor legal framework, poor law enforcement tools and family values fuel the incentive in the environment for cybercrime involvement (Ogunjobi, 2020; Olayemi, 2014). Unemployment is the main cause of cybercrime followed by poor governance and poor utilisation of digital skills acquired by the youths. The poor governance has affected the equipment provided for law enforcement to fight cybercrime. Traditional recording of crime has failed to identify digital fraud and law enforcement lacks the required equipment to fight cybercrime (Abdullah and Jahan, 2020). More disturbing is the acceptance of cybercrime as a norm among the socioeconomic and psychosocial classes in various geopolitical regions (Ibrahim, 2016). Social Learning Theory suggests that adverse consequences trigger cybercrime avoidance but in the Nigerian situation there is poor electronic evidence which leads to a poor conviction rate. This situation leaves nothing that deters youths from cyber-crime involvement.

The victims of cybercrime are vulnerable because they lack digital skills that will enhance their capabilities to identify an attack on time. Most individuals are not aware of what constitutes cybercrime, how cybercriminals operate, and what they should do to guide their digital information. This increases the level of their vulnerability (Ho and Luong, 2022). Also, a low knowledge base resulting from low research into cybercrime and increasing dependence on online activities creates new possibilities and vulnerabilities for criminal behaviour to thrive (Marttila et al, 2021). The increase in successful cybercrime in commercial banks alone up to 537 per cent is an incentive for cybercrime increase (Sule et al, 2021; Ogunjobi, 2020; Eya and Odo, 2019). The motivation to indulge in cybercrime is the desire the acquire wealth as quickly as possible (Ho and Luong, 2022; Sule et al, 2021; Ogunjobi, 2020). This desire fuels the learning and sophistication of cybercrime that makes law enforcement difficult.

Stage 3: Root Definition

SSM provides methods for explaining multiple points of view, underlying assumptions and logical consequences. One of the tactics for this is CATWOE (Checkland and Scholes, 1999); an abstract evaluation view that captures the essence of the relevant system. Each root concept, according to Checkland, indicates a different method of conceiving the problem circumstance.

C – (Clients/Customers) the clients and customers in this evaluation are the victims of cybercrime in Nigeria such as businesses, commercial banks, and individuals that are vulnerable to cybercriminals. These entities are the ones affected by the growth of cybercrime in Nigeria and will benefit if there is any reduction in cybercrime in Nigeria. They desire to explore the cyber space without any loss.

A – (Actors) The actors perform one or more activities that influence cybercrime in Nigeria. They create problems in the system or help in providing a solution to the problems created by other actors in the cybercrime system. They include youths who engage in cybercrime in Nigeria, law enforcement organizations who act to stop cybercrime, information security managers of organisations including commercial banks, government regulatory agencies including those in

investigation and the Justice System. The families of individuals who either engage in cybercrime or are victims of cybercrime in Nigeria are also actors.

T – (Transformation). This stage is the transformation of inputs from the messy cybercrime situation in Nigeria to a favourable outcome. It emphasises the transformation of negative social learning inputs (incentives) in the environment to alter the behaviour of the actors and clients in the social system. In this case, our transformation is, understanding the behaviour of the clients (cyber criminals) and the incentives in the environment through social learning. This insight will lead to the creation of a learning system to enhance the information and knowledge of policymakers, government, organisations security managers, law enforcement, and individuals that will alter their behaviours which increases the incentives in the environment for cybercrime. The growth in knowledge will reduce vulnerabilities and increase consequences that will deter would-be cybercriminals not to act on their social learning but working back away from learned behaviours that would have caused involvement in cybercrime. The government will invest heavily to improve law enforcement capabilities and infrastructure for the detection and prevention of cybercrime. The government will also learn to improve the socioeconomic situation which will improve employment and digital skills utilisation.

W – (Weltanschauung or Worldview) presents a worldview of the situation as an analysis without the naïve and reductionist presuppositions (Vidal, 2008). It both justifies the system's existence and gives the change process significance. Technological growth and internet usage in every aspect of humans have increased the number of users or actors in cyberspace. Internet use is a fact of contemporary societies such as Nigeria. Youths' increased use of the internet will diversify the Nigerian economy. Fairly safe cyberspace will lead to an increase in transactions over the internet and will also lead to cultural integration, social education, and rapid economic development in Nigeria. It will integrate Nigeria into the global village.

O – (Owners) the government of Nigeria is the owner of the system. It also includes business organisations such as banks, which have invested in the use of Information and Communication Technology. Even individuals who are interested in the protection of their resources exposed to cyber threats are also owners of the system. Through learning these owners naturally take action to improve the system.

E – (Environment) the environment exists outside the system but offer incentives to youths who are involved in cybercrime such incentive include unemployment, poor legal framework, poor law enforcement infrastructures, and capabilities, and poor cyber security capabilities by business organisations and society's new norm of accepting cybercrime. Even the media popularisation of successful cybercriminals without exposing their nefarious acts provides an incentive to cybercriminals. The underutilisation of digital skills to create meaningful employment also contributes to a favourable environment for cybercrime to thrive.

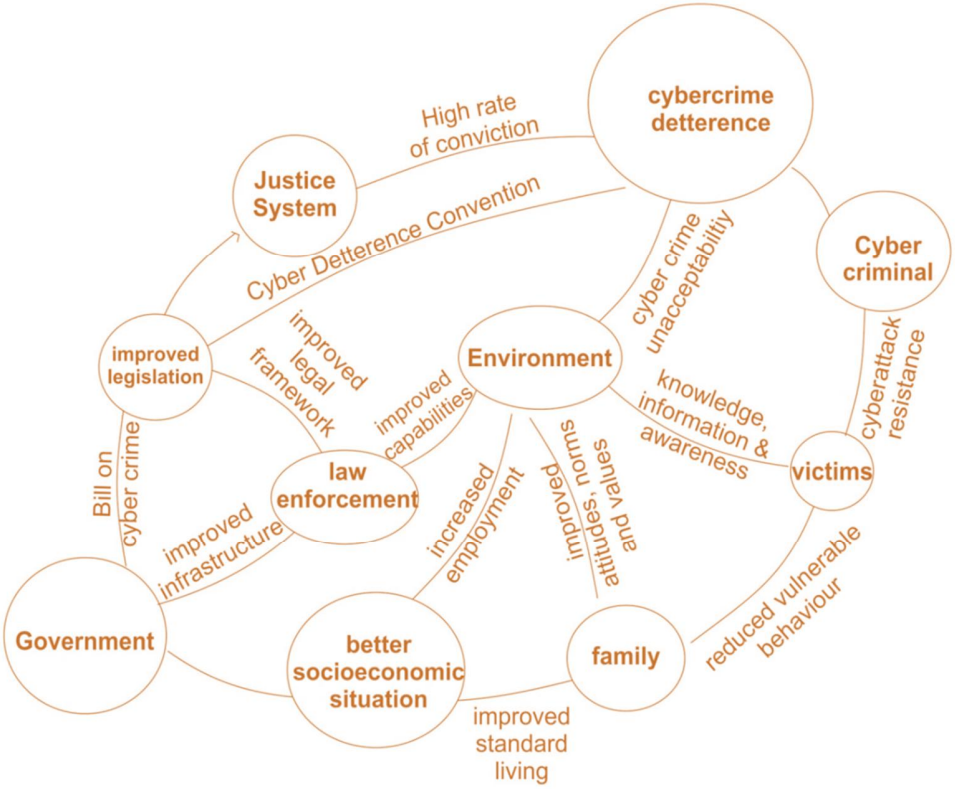
Stage 4: Conceptual Model

At this point, the human activities required to institute the system are logically represented to achieve the purposes of the system as discussed in the root definition (stage 3).

The human activities in a soft system conceptual model to support decisions that will lead to Cybercrime Deterrence include: Improving the justice system to achieve a high rate of conviction of those who have committed cybercrime in the country; adherence to the convention proposed for cybercrime deterrence; creating awareness to make cybercrime unacceptable; removing vulnerable factors and making victims have cyber-attack resistance; creating employment in the economy; improving law enforcement capabilities to detect and prosecute crimes; and improving families living standard alongside religious attitudes, values, and norms

that will alter the behaviour of cybercriminals. The changes in criminal behaviour will lead to a reduction in cybercrime.

Figure 4: Bubble Diagram



Source: Authors' Construct (2024)

Stage 5: Conceptual Model versus Problem Situation Analysis

The need to compare the conceptual model with the problem situation evaluated in stage 2 is necessary here to establish why the conceptual model can help solve the messy problem situation presented by cybercrime in Nigeria. The ultimate desire by cybercriminals to make quick wealth created a problem situation. This can be reduced if the family's well-being and living standards are increased through the creation of employment. Family norms, values, and attitudes will be changed in favour of good behaviour which will influence the youths to stay away from cybercrime. Unemployment is seen as the key factor in the socio-economic environment that encourages involvement in cybercrime; thus system thinking approach by the government to increase employment can lead to cybercrime deterrence. The greatest problem faced by law enforcement in Nigeria in their fight against cybercriminals is poor infrastructure, therefore, improving infrastructure and law enforcement capabilities will increase their capabilities to fight crime. No criminal wants to be caught in the act; therefore, the youths will be deterred from involvement in cybercrime in Nigeria if they perceive that there is a higher chance of failure than success.

Furthermore, cybercrime strives with vulnerable victims as shown in the problem situation, a learning approach that will increase the knowledge and information available to the victims will

increase their strength to resist cybercrime either as individuals or businesses. The essence of cybercrime is income; increased resistance will result in a reduction of the income available to the cybercriminal since few attacks will be possible, this will lead to a change in criminal behaviour and cybercrime deterrence. No law or legislation in Nigeria is specifically for cybercrime; thus any improvement in the legal framework will lead to improvement in the justice system for enhanced conviction and reduction of cybercrime.

Stage 6: Desirable and Feasible Changes

The victims of cybercrime were identified and the actors in the cybercrime system and government as the owner. These two elements in the system will have to work together to determine the desired and feasible changes that are needed to deter youths from getting involved in cybercrime. Some of those changes will be discussed in the subsequent paragraphs.

The government through arms and components institutions should work towards improving the fight against cybercrime by providing legislation that will be in line with the global convention on cybercrime deterrence as this will enhance the legal framework for cybercrime deterrence. Law enforcement is incapable to police the ever-changing dynamics of cybercrime, therefore it is desirable and feasible for the government to improve the law enforcement infrastructure to enhance the capabilities of law enforcement agencies to fight cybercrime. Cybercrime has a socio-economic dimension which is typically occasioned by unemployment. It is feasible and the key function of government to create employment in the economy, thus government should increase the creation of jobs both by evolving the use of youths' digital skills and capabilities to enhance the functioning of government and by creating employment in every other industry.

The government through social engineering should strengthen the families' socio-economic status and close social disparity gaps to improve family behaviour which will lead to improvement in norms, attitudes and values. This will lead to a reduction in the acceptance of cybercrime as a way of life. The victims are successfully attacked by identifying their vulnerabilities and weakness; growth in knowledge and information will reduce vulnerability and increase resistance to cybercrime. The government can create awareness of the methods, styles, and dangers of cybercrime among the victims. The victims can seek knowledge, information, and capabilities to enable them to repel cyber-attack. Fear and a higher propensity to be caught in criminal behaviour lead to deterrence; the government through the justice system can increase the rate of cybercrime conviction and punishment that will remove the incentives to engage in cybercrime.

Stage 7: Action for Improvement

After you've determined the adjustments that can be made, allocate responsibilities as outlined in step 6 above. The Ministry of Finance and the Central Bank of Nigeria should be given the responsibility to provide funds for improving infrastructure for law enforcement. The legislative arm of government should sponsor technically sophisticated bills for cybercrime. The country's general economic status should be improved. Government agencies should promote cybercrime education and awareness. It is up to the appropriate parties to put the recommendations into action. A structure for feedback, monitoring, and evaluation should be implemented into the system for system self-healing and sustainability. The response of the system's input and output to desired modifications is constantly assessed. We will suggest a multidisciplinary institution for studies into cybercrime that will stir relative action.

5.0 Conclusion and Recommendation

Social Learning Theory offered a useful foundation for explaining individual deviant behaviour. This theory gave insight into the process of human behaviour towards cybercrime but without guidance towards guided behaviour and a holistic view involving other stakeholders. It offered a pointer to a system of thinking of behaviour imitating and modelling deviant behaviour (Resnick, 2012). Social Learning showed that learning the consequences of an action can adjust human behaviour either to do wrong or right (Hunter-Reel, 2013). While Soft Systems Methodology (SSM), anchored on the systems theory, offered a useful tool to holistically evaluate the process of social learning and cybercrime behaviour. SSM highlighted the interrelationship between the agents, actors, and stakeholders in the Nigerian cybercrime system. Using Soft Systems Methodology, this study provided a restrictive and improved method of managing change in a social and information system (Asadi, 2020). Thus, using Social Learning and Soft System Methodology to analyse and model Nigeria's cybercrime posture offers a fast and reliable tool for the actualisation of the cybercrime deterrence needed to stir socio-economic growth in Nigeria.

Knowledge, information, and awareness are major methods of reducing the vulnerability of victims which will increase their resistance to cybercrime. Most individuals and groups are not aware of what constitutes cybercrime in Nigeria (Ho and Luong, 2022). Thus, awareness, knowledge acquired and action taken within a learning framework as provided by SSM on cybercrime in Nigeria will be a useful tool in reducing victims' vulnerability (Ho and Luong, 2022; Abdallah and Jahan, 2020). Knowledge and information outlook will also shape family norms, attitudes and culture towards cybercrime deterrence in Nigeria (Li *et al*, 2020). Resistance to cybercrime will reduce available income to cyber criminals and incentive to manifest criminal behaviour. The essence of involvement in cybercrime is the desire to acquire quick wealth; a reduction in income and an increase in law enforcement capabilities will deter a lot of youths from getting involved in cybercrime. SSM is a learning system that employs and uses feedback for an iterative process of consistent increase in awareness, knowledge, and information on cybercrime posture in Nigeria. This will offer useful adjustment and continuous improvement in the cybercrime system.

References:

Abdullahi, A. and Jahan, I. (2020). Challenges of Cyber policing in response to cybercrime to reduce victimization *International Journal of Research and Innovation in Social Science.* 4(5):219-226.

Asadi, Samira (2020). Soft systems Methodology: Approach to IS change management, *International Journal of Industrial Engineering and Management Sciences* 7(1):84-92

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. Psychological review, 84(2), 191.

Bello, T (2017) Anatomy of cybercrime in Nigeria: *The Legal Chronicle alkilabe* at SSRN: https:/SSm.com /abstract or doi.org /10.2139/ssm.3055743

Bendiek, A.; Bossong, R. and Schulze, M. (2017). The EU's Revised Cyber Security Strategy, SWP Comments 47, available at https://www.swp-berlin.org/publications/products/comments/2017C47_bdk_etal.pdf retrieved 02/11/22.

Black, J. S., and Mendenhall, M. (1990). Cross-cultural training effectiveness: A review and a theoretical framework for future research. *The Academy of Management Review, 15*(1), 113–136.

Burge, S. (2015). System Thinking: Approaches and Methodologies. An Overview of the Soft Systems Methodology. Burge Hughes Walsh. Available at: https: //www.burgehugheswalsh.co.uk/Uploaded/1/Documents/Soft-SystemsMethodology.pdf

Caulkins, B. (2017). Lecture title Modeling and Simulation of Behavioral Cybersecurity. In: Lahcan, R., Caulkins, B., Mohapatra, R. and Kuman, M (2020) Review and insight on the behavioural aspects of cyber security, *Cybersecurity* 3(10): 1-8.

Checkland, P (2000). Soft Systems Methodology: a thirty-year retrospective, Systems Research and Behavioural Science, 17(S1), S11 – S58.

Checkland, P. (1996). Systems Thinking, Systems Practice. John Wiley and Sons.

Checkland, P. and Scholes, J. (1999). Soft Systems Methodology in Action. John Wiley & Sons.

Chorley, R. J and Kennedy, B. A. (1971). *Physical Geography: A systems approach*. Prentice-Hall International, London.

Dearden, T. and Parti, K (2020). Cybercrime, differential association and self-control, a revised manuscript available at https://vtechworks.lib.vt.edu/bitstream/handle/10919/106589/Dearden.Parti.AJCJ.PROOF.pdf retrieved on 02/11/22.

Ebrabrimi, M. (2020). The use of soft systems methodology for change management is available at https://www.researchgate.net/publications/343150808 retrieved on 28/02/2022.

Eke, O and Ofoeze 4. (2020). Tapeworm in the bloodstream: addressing the effect of cybercrime for human security and development in Nigeria *Journal of Humanities and Social Science* 25(6) 8-16.

Eya, O. and Odo, C (2019).Public perceptions on the determinants of Youths' involvement in cybercrime in Enugu Urban, Enugu State, a framework for social workers, *International Journal of Innovative Research in Social Sciences and Strategic Management Techniques* 6(1):34-48.

Ezekiel, M. Abdullahi, G. and Rukayyat, A. (2021). A Historical assessment of cybercrime in Nigeria: Implication for schools and National Development, *Quest Journals* 9(9):84-94.

Gong, Y; Zhang, J and Li, Y (2014) From the Social Learning Theory to Social Learning Algorithm for global optimisation, IEEE International Conference on Systems, Mana and Cybernetics, October 5 – 8, San Diego, CA, USA.

Grusec, JE (2020). Social Learning Theory, International Encyclopaedia of the Social & Behavioural Sciences 2nd eds., 221 – 228.

Hamisu M, Idris AM, Mansour A, Olalere M (2021) 'Analysis of cybercrime in Nigeria', 2020 IEEE 2nd International Conference on Cyberspace (CYBER NIGERIA) - Abuja, Institutes of Electrical and Electronics Engineers Inc.

Hindle, GA(2011). Case Article-Teaching Soft Systems Methodology and a blueprint for module, INFORMS Transaction on Education, 12(1), 31 – 40.

Ho, H and Luong, H (2022). Research trends in cybercrime victimization during 2010-2020: a bibliometric analysis, SN *Soc. Sci*. 2:4.

Hunter-Reel, D(2013). Interpersonal factors and addictive disorders, DOI:101/016/B978-0-12-398336-700030-9.

Ibikunle, F. and Enenyi, O. (2013). Approach to cyber security issues in Nigeria: Challenges and solution, *International Journal of Cognitive Research in Science, Engineering and Education* 1(1):1-12.

Ibrahim (2016). Social and Contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals, *International Journal of Law, Crime and Justice* 47:44-57.

Ibrahim, S. Nnamanic , D and Soyele (2020). An analysis of various types of cybercrime and ways to prevent them. *International Journal of Education and Social Science Research* 3(2). 1-7

Igba, I., Igba, E. and Nwanbam, A. (2018). Cybercrime among University Undergraduates: Implications on their academic achievement. *International Journal of Applied Engineering Research* 13 (2): 1144-1154.

Irawan and Samsunyadi (2019) Hybrid soft systems methodology (SSM) and Becerra approach for madding knowledge management system, *Journal of Physics* Doi:10:088/1742-6596/1/0/2055.

Jensen, GF (2015). Social Learning Theory, International Encyclopaedia of the Social & Behavioural Sciences 2nd eds.

Lahcan, R., Caulkins, B., Mohapatra, R. and Kuman, M (2020) Review and insight on the behavioural aspects of cyber security, *Cybersecurity* 3(10): 1-8.

Li, W and Tan, X (2020). Cognitively-constrained learning from Neighbors available at http://econ2017.sites.olt.ubc.ca/files/2020/04/pdf retrieved on 02/11/22.

Li, Y., Li, J., Fan, Q. and Wang Z (2022). Cybercrime's tendencies of the teenagers in the COVID-19 era: assessing the influence of mobile games, social networks and religious attitudes.

Lyons, S.D.and Berge, Z.L. (2012). Social Learning Theory. In: Seel, N.M. (eds) Encyclopedia of the Sciences of Learning. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-1428-6_1257.

Marltila, E., Koivulas, A. and Rasanen, P. (2021) Cybercrime Victimization and problematic social media use. Findings from a nationally representative panel study, *American Journal of Criminal Justice*. https://doi.org/10.1007/3/2/03-021-09665-2.

Maturana, H. R., and Varela, F. G. (1980). Autopoiesis and Cognition: The Realization of the Living. In: Mingers, J (1991), The cognitive theories of Maturana and Varela.

Miller, A. (1978). Conceptual systems theory: A critical review. *Genetic Psychology Monographs, 97*(1), 77–126

Morris, M. A., and Robie, C. (2001). A meta-analysis of the effects of cross-cultural training on expatriate performance and adjustment. *International Journal of Training and Development, 5*(2), 112–125

Novani, S. and Mayangsan, L. (2017). Soft systems agent-based methodology: Multi-methods Approach between soft systems methodology and agent-based modelling DOI: 10:1007/978-981-10-36662-0-13.

Odoyo J; Abeka S. and Liyala s. (2020) Exploring a social learning perspective on computer forensics barriers and factors affecting cybercrime investigation in Kenya, *International Research Journal of Innovations in Engineering and Technology* 4(7):9 – 13.

Ogunjobi, O. (2020). The impact of cybercrime on Nigerian Youths is available at hyyps://www.researchgate.net/publication/347436728.

Okeshola F. and Adeta, A (2013). The nature cause and consequences of cybercrime in tertiary institution in Zaria – Kaduna State, Nigeria, *American International Journal of Contemporary Research* 3(9): 1-17.

Olayemi O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria, *International Journal of Sociology and Anthropology* 6(3):116-125.

Omeire, E. and Omeire, C (2017). Social structure and the production of young cybercriminals in Nigeria. *International Journal of Social Sciences, Humanities and Education* 1 (2):1-8.

Omoduanbi, O. Odiase, O. Olaniyan, M and Esan, A. Cybercrimes in Nigeria: Analysis, Detection and Prevention, *FUOYE Journal of Engineering and Technology* 1 (1): 1-7.

Resnick, M. (2012). Reviving Papert's Dream, *Educational Technology*, 52 (4), 42-46.

Salavati, S; Mirijamdotter, A; Elm, P and Perez (2021). Coordinated SSM an adaptaion of the SSM learning cycle, Systems, 9, 49 – 58.

Sharma, R; Zhang, C; Wingreen, SC; Kshetri, N; and Zahid A (2019). Design of blockchain-based precision healthcare using Soft Systems Methodology. *Industrial Management Data Systems*.

Spivak, A.L. and Howes, C. (2011). Social and relational factors in early education and pro-social actions of children of diverse ethno-cultural communities. Merrill- Palmer Quarterly, 57(1): 1-24.

Sule, B., Yahaya, M. Sambo, U and Mat, B. (2021). Cyber security and cybercrime in Nigeria: The implications on National Security and Digital Economy, *Journal of Intelligence and Cybersecurity* 4(1):27-59.

Torres, (2018). Cyber security and cyber defence for Venezuela: an approach from the soft systems methodology, *Complex and Intelligence Systems* 4:213-226.

Tsuro, L and Hardman, S (2020). A Soft Systems Methodology approach to improving the supply chain of a construction project in Gauteng Province, South Africa, Journal of Construction Project Management and Innovation, 10(1), 86 – 96.

Ward, JT and Broan, CN (2015). Social Learning Theory and Crime, International Encyclopaedia of the Social & Behavioural Sciences 2nd eds., 409 – 414.

Williams, B. (2005). Soft Systems Methodology. The Kellogg Foundation. Available at: http: //users.actrix.co.nz/bobwill.