International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 4, Issue 7, pp 9-13, July-2020

https://doi.org/10.47001/IRJIET/2020.407002

Exploring a Social Learning Perspective on Computer Forensics Barriers and Factors Affecting Cybercrime Investigation in Kenya

[1]Josephine Akinyi Odoyo, [2]Silvance Abeka, [3]Samuel Liyala

[1,2,3]Department of Information Systems, Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya

***Abstract* - As Kenya matures into an information society, she is exposed to various cyber threats and challenges resulting from the ubiquity of the internet and advancement of technology. Social engineering tricks have been applied to exploit vulnerabilities in people, processes and technologies used in varied environments. On the other hand, computer forensics development plays catch up with the rising challenges within the field especially on the levels of expertise. Social learning brings the element of gaining cultural knowledge, skills, attitudes, strategies, rules and beliefs through observing others. To determine the need for a proactive means of overcoming the ever challenging cybercrime, a Social Learning perspective into the development of standardized procedures in legislation, investigation processes, certification and training of cybercrime investigators is explored, so computer forensics can become a more effective and mature field in curbing cybercrime investigation barriers, especially in predicting and understanding of cybercriminals' behavior.**

Keywords: Social Learning Theory, Information Society, Computer Forensics, Cybercrime Investigation, Cybercriminal Behaviour.

I. INTRODUCTION

Often times, the Internet is regarded to have a great impact on cybercrime given the opportunities it presents. However, clarity on the issue at hand despite the various factors leading to the increase in cybercrime has been lacking. This is in assessing the exact thing about cyber that is new, given that what are termed as "traditional crimes" are more or less the same crimes committed online, only through a different platform. It is more confusing when it comes to the gap that is between estimated hundreds of thousands of incidents and the relatively small number of successfully known prosecutions [1]. The confusion caused by Cybercrime has in fact led some authors to question whether it can be best understood through existing theories or if it is a crime category in need of a new theory [1]. Jaishankar [2] even developed the Space Transition Theory that explains the causation of cyberspace crimes as an effort to further the cyber criminology discipline. This is because he felt the need for separate cybercrime theories as explanations in the general theories was found to be inadequate. Notably, theoretical perspectives need to be built in an attempt to determine deviant behavior and attitudes of investigators towards controlling cybercrime. Though theoretical theories within computer forensics are being worked on by researchers, cybercrime practitioners deal with entirely new sets of challenges [3].

II. COMPUTER FORENSICS AND CYBERCRIME EVOLUTION

In the mid-1940s, computers were introduced. Rapid development of computers was soon followed by a series of various computer offences. Even though numerous offenses happened, many went unreported, or prosecuted, or even unknown to the large public [4]. The 1970s and 1980s saw the rise of personal computers. This became common as individuals and businesses took on using computers on a regular basis. This led to awareness of Cybercrime by law enforcement agencies in technologically advanced countries by the 1990s. Systems were put in place for investigation and prosecution activities, giving birth to Computer Forensics. From as early as 1984, FBI laboratory in the US and other law enforcement agencies developed programs to assist in the examination of computer Evidence. This majorly was to address demands of investigators and prosecutors that were growing. The goal being to address these demands in a programmatic and structured manner leading to the establishment of Computer Analysis Response Team, CART [5].

Looking through the past number of years Computer Forensics has grown, increasingly becoming a technique of identifying, solving, documenting and enabling the prosecution of computer or cybercrimes. From the 1960s to date, Computer Forensics has transitioned from a time when it lacked a proper structure, clear goals, adequate tools, processes and procedures, to a time where we have proper structures, accepted procedures, and special tools developed to

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 4, Issue 7, pp 9-13, July-2020

https://doi.org/10.47001/IRJIET/2020.407002

enable criminal legislation to widely use digital evidences [23]. Today, we have real time collection of digital evidence, developed field collection tools, and even forensics becoming a service in companies. Computer Forensics now spans within four communities; Legal, Military, Private sector and Academic sectors. Despite the growth in the field though, there are many reasons why an investigation may not lead to a successful prosecution. As observed by Eloff, Kohn, and Olivier [11], the predominant reason is lack of preparation. The organizations investigating suspicious behavior often lacks the tools and skills required to successfully gather evidence and, individuals attempting to investigate such suspicious activities may at times lack the resources or tools to conduct such an investigation adequately, to ensure that the evidence is indisputable in all circumstances [10]. Furthermore, there are instances when the tools, skills, and resources have been adequately put in place by an organization, but due to a lack of training and correct procedure, the evidence collected gets easily disputed [11]. Cybercrime is also evolving greatly in line with opportunities presented online that aid with it becoming widespread, not to mention its damaging effects. The evolution is accosted to criminal organizations increasingly turning to the internet in order to facilitate their activities and more importantly, maximize profits in the shortest time possible.

III. CYBERCRIME INVESTIGATION BARRIERS

The process of investigating cybercrimes involves evidence collection, data examination, its analysis and reporting when responding to incidents [3]. Kenya is making a transition in dealing with cybercrime. However, like in most countries, local police agencies have a cultural problem in the way they deal with cybercrime especially in shifting from traditional investigation methods towards handling cybercrime investigations. Embracing cybercrime investigation has been slow with a more preference given to handling the old fashioned crimes.

Unfortunately, cybercrime is becoming an issue that needs proper preparation of officers or investigators handling cybercrimes. To respond efficiently to cybercrimes, the investigators need to realize that today, almost every crime in our communities has an aspect of technology to it. It is thence important that police departments adapt to the changing times and prepare for cybercrime by understanding how cybercrimes are committed and what can be done in the event an incident occurs [9]. Notably, the changing cyber threat landscape impacts policing in three ways: Police crime workload, public service delivery and the ability to carry out the police administration [6].

IV. STANDARDIZED PROCEDURES AND METHODOLOGIES

For many years, digital forensics development has been centered on tools driven by commercial developers for computer investigation processes. Combination of this with absence of set standards to guide cybercrime investigation practitioners operating in this field has led to issues that regard to reliability, verifiability and the consistency of digital evidence when presented in courts [7]. Lack of standardized procedures is further felt where the anonymity factor in the internet creates more barriers for cybercrime investigators in identifying the authorship of cyber incidents given that there are no standardized procedures to follow. Though a number of forensic modes are present today, they have only added complexity to the field as the present few procedures from different authors holds a number of discrepancies that hinder the investigation process [8]. It is still due to the lack of standardized procedures of handling investigation processes that you often find low level offenders operating unchallenged. This is because much focus by the agencies tends to focus their limited resources on large cases leading to the enforcing agents being challenged in their roles with cybercrime investigation [9].

Therefore, Kenya needs to have laws that provide a framework of standards, quality principles and approaches for detection, preservation, recovery, examination and use of digital evidence for forensic purposes. Also required are laws that regulate training and certification, to encourage more consistent investigative methodologies to produce more comparable results, to make computer forensics an integral part of the Kenyan law of evidence. The police and other law enforcement agents will also need these techniques and procedures to conduct investigations, analyze information and create computer systems capable of determining when, how, and who committed the computer crimes [10].

V. SOCIAL LEARNING THEORY

Focusing on theories that influence deviant behavior, four social learning theorists are considered, namely: Albert Bandura, Burrhus Fredrick Skinner, Edward Sutherland, and Ronald Akers.

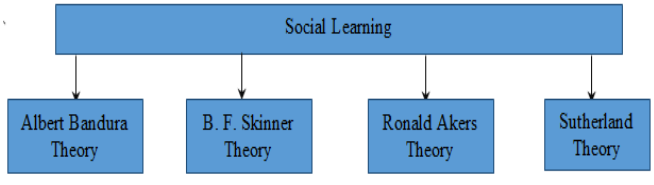

Figure 1: Social Learning Theoretical Framework

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 4, Issue 7, pp 9-13, July-2020

https://doi.org/10.47001/IRJIET/2020.407002

a) Albert Bandura's Social Cognitive Learning Theory

Social cognitive learning theory formulated by Albert Bandura takes a theoretical perspective where people can learn by observing others within contexts of social interactions, media influences, or experiences. The theory was founded on the model of causation where different human capabilities were analyzed. In modes of unidirectional causation, human behavior was portrayed as being shaped and controlled either by environmental influences or by internal dispositions. Social cognitive theory favors the causation model of causation where behavior, personal factors, cognition, and environment influences, all operate as interacting determinants that affect each other bi-directionally [12]. Social cognitive learning theory's highlight is in the idea that much of what humans learn occur in a social environment. That is, through observing others, people get to acquire knowledge of cultures, rules, strategies, skills, beliefs, and attitudes. People can acquire new behaviors and knowledge by observing models, consequences of modeled behaviors and in return people act in accordance with their beliefs concerning the expected outcomes of actions [13]. The cognitive theory assumes that people actively process information and that learning takes place through the efforts of people setting goals for themselves, organize, store and find relationships between information, and so link new knowledge to old knowledge, schema and scripts. This applies to the research as information technologies have to be learned for them to be used effectively. Learning of these technologies will always require that goals are set, organized and stored for reference. Looking at the trends in cybercrime investigation and cyber security, though globally we see an increase in tech savvy cybercriminals, the masses have not given much time to themselves to learn the present new technologies. Truly, convergence is the erosion of boundaries between previously separate services, networks, and business practices in the ICT sector [14].

b) Ronald Akers' Social Learning Theory

Ronald Akers Social Structure and Social Learning Model proposed that social structural factors have an indirect effect on an individual's actions through the social learning process [15]. Akers' four main concepts of social learning (Introduction, Evaluation, Application, and Differential Association) retain the process of differential association, referring to potential punishments and rewards for committing or not committing a crime or deviant act. In this process, rewards and punishments received in the past, present and those of the future are considered. Akers sites that when an individual decides to join a group that spends time committing illegal activities, the individual begins to learn the techniques of committing a crime, and after committing several crimes, the individual starts to think it is part of a normal behavior [15]. According to Akers [15], "A person becomes a delinquent because of an excess of definition favorable to violation of laws". Akers says that a person develops deviant behavior out of the reinforcement of using deviant behavior more that they use law abiding behavior. Rewards and modeling therefore tend to influence more people every day, including those in the criminal world. Akers Social Learning Theory hence suggests that the effects of principal behavior come from interactions in or under the influence of people or groups, that control an individual's major source of reinforcement and punishment, thus expose them to behavioral models and normative definitions [16].

c) B.F. Skinner's Operant Conditioning

Burrhus Frederic Skinner's Operant Conditioning believes that actions and decisions made by a person voluntarily are influenced and shaped by optimal patterns of stimulus and response to punishments and rewards found in the external world. Skinner observed that an important process in human learning is attributed to these factors. He believed that to understand behavior, it would be best to look at the causes of an action and its consequences. Skinner called this approach operant conditioning. Skinner's Operant Conditioning theory deals with operants - intentional actions that have an effect on the surrounding environment. Skinner set out to identify the processes which made certain operant behaviors are more or less likely to occur [17]. B. F. Skinner [19] devised the term operant conditioning to mean; changing of behavior by using reinforcement after a desired response.

According to Skinner, a behavior tends to be repeated when it is reinforced and die out or be extinguished when not reinforced. He identified three responses or operants that follow behavior; one being the neutral operants from the environment which neither decrease nor increase the probability of repeating a behavior. Two is the reinforcers. These are responses from the environment that increase the likelihood of a behavior being repeated. Reinforcers in this case can either be positive or negative. Three is the punishers, responses that decrease the probability of a behavior repeating as punishment weakens behavior. Skinner [20]; [21] suggests that people use reinforcers to control the society, picking the right enforcers that makes them feel free by doing what they feel they want. It is stated that the good do good and the bad do bad because they are awarded. Skinner further suggests that the society can take control by designing a culture where the good gets rewarded and the bad gets extinguished. He says, "With the right behavioral technology, we can design culture". Skinner encouraged concentration on observables referring to the environment and people's behavior in it.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 4, Issue 7, pp 9-13, July-2020

https://doi.org/10.47001/IRJIET/2020.407002

d) Edwin Sutherland's Differential Association Theory

Edwin Sutherland's unlike the previous theorists does not believe in human learning being a result of imitation alone. According to Sutherland [21], criminal behavior results from learning an excess of definitions that is favorable to crime. He proposes that individuals through interaction with others can learn the values, techniques, attitudes, and motives for criminal behavior. His conclusion is that scientific criminology should be able to go beyond listings of correlates of crime, and therefore seek a collective explanation of criminal behavior. Presented in nine steps, Sutherland's differential association introduces normative conflict, differential association, and differential group organization concepts. These explain crime at the levels of groups, individuals and society. Social learning theory shows that criminality is basically a result of engaging in inappropriate behaviors exhibited by people we interact with. Sutherland's thought is that people do not break laws because they saw someone else, especially one they are unfamiliar with do it. Sutherland's theory just like Akers Social Learning Theory believes that deviant behavior is learned through modeling or imitation, and reinforcement learned from intimate groups such as friends and family [16]; [22]

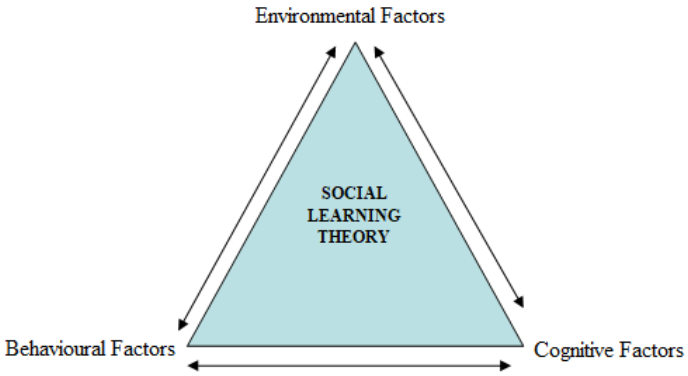

Figure 2: Social Learning Behaviour Determinants

Therefore, Social Learning theory proposes that both criminal and conforming behaviors are acquired, changed, or maintained by the same process of interaction with others. It implies that the social element can influence the development of new learning amongst individuals. The difference lies in the deviant direction or in conforming or the balance of the social influences such as reinforcement, values and attitudes, and limitation.

In this paper, the theoretical framework helps to build the behavioral determinants around environmental, behavioral, and cognitive factors.

IV. CONCLUSION

A proactive approach into Computer Forensics is drawn from the Social Learning Theory as a positivism theory of crime causes and incorporates facilitation of crime, including preventive and protective factors. Therefore, a Social Learning Perspective to computer forensics cannot only help in establishing the relationship between the barriers and factors influencing cybercrime investigations but also incorporate the preventive and protective factors in the investigation process so as to determine the behavior of cybercrime investigators towards cybercrime encompassing environmental, behavioral, and cognitive factors that work towards reinforcing, rewarding, or punishing criminal or deviant behavior among cybercrime investigators.

REFERENCES

[1] Wall, D.S. (2005/15).*The Internet as a Conduit for Criminals' pp. 77-98 in Pattavina, A.* (ed) Information Technology and the Criminal Justice System, Thousand Oaks, CA: Sage.

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

[3] Sremack, J. C. (2007). The Gap between Theory and Practice in Digital Forensics. LECG Washington

[4] Huebner, E., Bem, D., &Bem, O. (2007). Computer Forensics – Past, Present and Future.

[5] Whitcomb, C. M. (2002). An Historical Perspective of Digital Evidence: A Forensic Scientist's View. International Journal of Digital Evidence, Volume 1, Issue 1.

[6] Juan, C. Rivera-Vazquez, Lilian, V., Ortiz-Fournier Feliz Rogelio Flores, (2009), Overcoming cultural barriers for innovation and knowledge sharing", Journal of Knowledge Management, Vol. 13 Iss 5 pp. 257-270.

[7] Hewling, M.O. (2013), 'Digital forensics: an integrated approach for the investigation of cyber/computer related crimes'. PhD thesis. University of Bedfordshire.

[8] Lalla, Himal & Flowerday, Stephen. (2010). 'Towards a Standardized Digital Forensic Process: E-mail Forensics'.

[9] Police Executive Research Forum. (2014). 'The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime'. Washington, D.C. 20036.

[10] Wanderi, C. (2007). Computer forensics-Kenya needs a law to protect businesses against cyber/computer crime. Retrieved on 17th May 2015:

ISSN (online): 2581-3048
Volume 4, Issue 7, pp 9-13, July-2020
https://doi.org/10.47001/IRJIET/2020.407002

http://thekenyancolumn.blogspot.com/2007/09/computer-forensic-kenya-needs-law-to.html.

[11] Kohn, M., Eloff J., and Olivier M. (2006). "Framework for a Digital Forensic Investigation." http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/101_Paper.pdf

[12] Bandura, A. (1989). Social Cognitive Theory. http://www.uky.edu/~eushe2/Bandura/Bandura1989ACD.pdf

[13] Humes, G. (2001). Social Cognitive Theory of Learning. http://info.psu.edu.sa/psu/maths/007%20Social%20Cog%20Theory%2001.pdf

[14] Singh, R. and Raja, S. (2010). Convergence in information and communication technology: Strategic and regulatory considerations, The International Bank for Reconstruction and Development / The World Bank; Washington.

[15] Akers, Ronald L. 2000. *Criminological Theories: Introduction, Evaluation and Application*. Los Angeles: Roxbury.

[16] Collins, S. E., & Carey K. B., The theory of planned behavior as a model of heavy episodic drinking among college students. *Psychology of addictive behaviours : journal of the Society of Psychologists in Addictive Behaviors,* 21(4): 498-5-7. https://doi.org/10.1037/0893-164X.21.4.498

[17] McLeod, S. A. (2015). Skinner - Operant Conditioning. www.simplypsychology.org/operant-conditioning.html

[18] Skinner, B. F. (2014). Science and Human Behavior. The B. F. Skinner Foundation.

[19] Boeree, C.G. (2006). 'Personality Theories'. http://www.ship.edu/%7Ecgboeree/perscontents.html

[20] Deborah E Altus, Edward K Morris. 'B.F.Skinner's Utopian Vision: Behind and Beyond Walden Two'. Behav Anal. 2009 Fall; 32(2): 319-335.doi: 10.1007/BF03392195.

[21] Matsueda, R. L. (2006). Differential Social Organization, Collective Action, and Crime. (Springer Science and Business Media). University of Washington, Seattle, WA.

[22] Matsueda, R. L. (2000). Differential Association Theory. University of Washington, Seattle, WA

[23] Huebner, E., Bem, D., &Bem, O. (2007). '*Computer Forensics – Past, Present and Future'*. Journal of Information Science and Technology.

AUTHOR'S BIOGRAPHIES

J. Akinyi Odoyo: Pursued a Master's degree at Jaramogi Oginga Odinga University of Science and Technology, Department Information Systems.

Silvance Abeka: Senior Lecturer and Dean, School of Informatics and Innovative Systems of Jaramogi Oginga Odinga University of Science and Technology.

Samuel Liyala: Researcher, Lecturer and Head of Department, Information Systems and Technology at Jaramogi Oginga Odinga University of Science and Technology.

Citation of this Article:

Josephine Akinyi Odoyo, Silvance Abeka, Samuel Liyala, "Exploring a Social Learning Perspective on Computer Forensics Barriers and Factors Affecting Cybercrime Investigation in Kenya" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 4, Issue 7, pp 9-13, July 2020. https://doi.org/10.47001/IRJIET/2020.407002

****

