Towards the use of New Forensic Approach as a Panacea in Investigation of Cybercrime

DANLAMI GABI[1], NASIRU MUHAMMAD DANKOLO[2], DALHATU MUHAMMED[3]

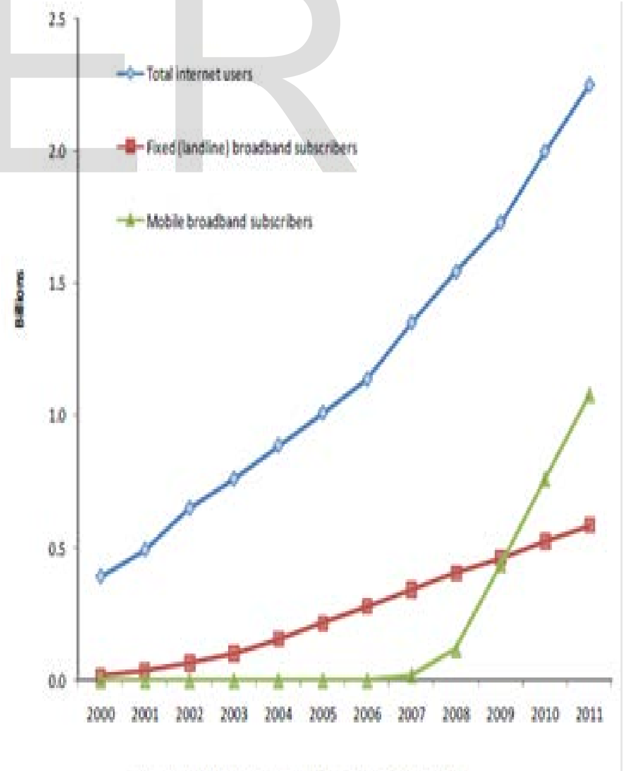
Abstract— Todays' cybercrime has spark doubt on whether data across network infrastructure are secure. Crime such as denial of service, spoofing, ID theft, DDOS, Sniffing, hacking, are used to compromise critical network infrastructure. These growing menaces have posed lots of damages to cyberspace thereby causing valuable data and financial losses to both users and companies. The emerging perpetrations of these crimes have no doubt unveiled the security implementation on network infrastructure as mere illusion. Today, end users can no longer ascertain that cybercrime can be eradicated, viewing at the kind of damages it causes in our time. Inevitably, we need to understand how these crimes are being facilitated to ensure proper design of counter mechanisms that will help in the apprehension of perpetrator(s). Tracing perpetrator(s) becomes an ever growing challenges' for cyber investigators, as perpetrator(s) can immediately cover their track when they facilitate an illicit act. A miscreant can take just 30 minutes to facilitate a crime online that can cause forensic investigator(s) 34 hours to discover traces and retrieve evidence that the perpetrated act has occurred. This show how lacking forensic investigators are in terms of response and proper forensic approach towards investigation. On the basis of this research, we explore the limelight of cyber forensic as an emerging field in unveiling cybercrime activities. We further proposed a new forensic approach that will serve as a panacea towards investigation of cybercrime. The model unveils how perpetrator(s) in the cause of their illicit act can be apprehended by team of cyber investigators.

Index Terms— Cybercrime; Cyber security; Cyber forensic; Existing model; New forensic model

1 Introduction

THE giant strive of internet as a means of communication and information dissemination facility is a welcome development to any developing country and the world at large. According to [4], "internet has become a widely medium for companies, schools, and governments to share data." Advent of this giant achievement has no doubt made communication more robust thereby improving the state of human existence. Internet offers limitless opportunities in recording and proving access to information what are at times personal and form part of our unique identity [14]. Internet has pioneered business to soar and at today, life can be meaningless without the existence to this great treasure.

Corporations today can easily establish their own cyberspace, maintained it and coordinate businesses around the globe. The ever unlimited achievement of this giant strive has so far made internet connectivity to soar. In fact, research shows that, by 2020 there will be one trillion computers that will be connected to internet. Fig.1 is global internet connectivity trend from 2002-20011 by ITU world telecommunication ICT indicators. These shows how rapidly internet is becoming.



Source: ITU World Telecommunication ICT Indicators 2012

Fig.1. Global internet connectivity 2000-2011 [12]

In spite all this benefits, there exists a global thread (cybercrime) that exposes this treasure into becoming an illusion. Internet has now become a domain where lots of crimes are facilitated. These crimes have causes setback to most especial ly, the financial institutes (Banks) causing loss of billions if not trillions yearly as a result of unauthorized invasion of customers account by miscreants. Crimes such as denial of service, spoofing, ID theft, DDOS, Sniffing, password attacks, hacking, have become a thread to global infrastructure.

Perpetrators of cybercrime now have the propensity to hide under cyber space and commit or facilitate illegal act without immediate response from law enforcement agency. These growing threads have no doubt become illicit and serious countermeasures are needed to fight these menace. However, in our research, we tend to use the preceding theory on the overview of cybercrime as highlighted in section 2, to develop a new forensic approach that will serve as a panacea towards investigation of cybercrime.

2 OVERVIEW OF CYBERCRIME

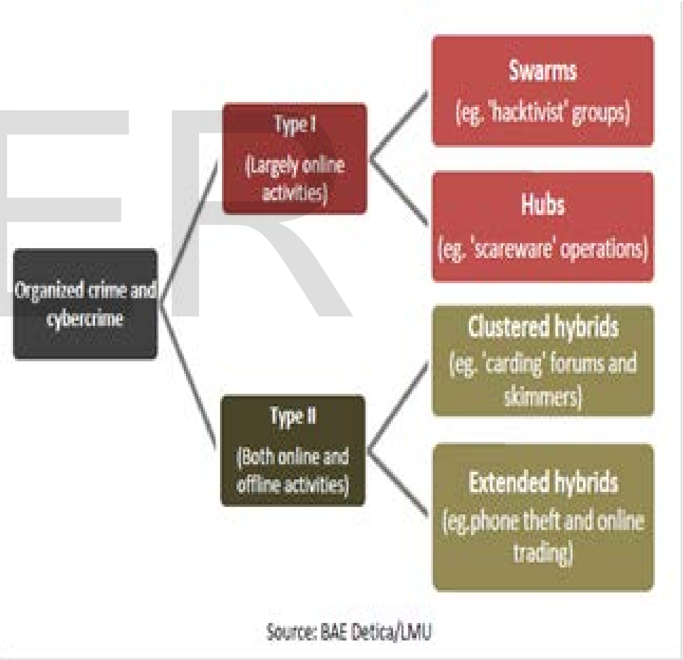
In view of the ever growing achievement of cyberspace (Internet) and also a disadvantage of being a vehicle for malicious attacks as highlighted in section 1, it is very important to have a clear understanding of cybercrime as viewed by several authors and used the preceding theory to develop a new forensic method that will help in apprehending perpetrator(s) of cybercrime. Per [6] defined cybercrime as: "…. a subset of crime that is committed by use of computer technology, either alone or in conjunction with real-world act and actors." Internet has no doubt become a vehicle for committing cybercrime activities with computer as a driving tool that facilitates the perpetrated act. [11] in their book on "mastering network forensic and investigation" highlighted the steps taken by attackers in committing cybercrime where they state: "……attackers generally perform a recon of their intended target to determine the structure of the network, locate potential vulnerabilities, and develop idea on which machine are most vulnerable to the attack… they will then exploits a vulnerable system and gain a foothold within the network from which they can perform further recon, lunch further attacks, set up rogue sniffers, and perform other steps to increase their influence within the network." Attackers are said to cover their track when they propagated such illicit act. [14], elaborated on the definition of cybercrime as'

> "……..*offences that are committed against individuals or groups of individuals with criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as internet (chat rooms, social networking sites, e-mail, notice boards and groups) and mobile smart phones internet applications."* (p.186)

However, a computer system with network connections is a clear domain in propagating cybercrime. We cite researcher [5], citing [6], in which he state:

> "……..*it accurately assesses that "persons…have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space," as well as the fact that, "identity flexibility, dissociative anonymity, and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime." (p.741)*

Using the preceding theory, it shows that, cybercrimes are easily committed on cyberspace than committing such act in physical space. Looking at the emerging threads of these crimes, a hacker can invade a system and violate the security policy of the system without anyone knowing when and where such invasion takes place. Fig.2 below shows the structure of organized criminal groups that are engaged in cybercrime.


Organized crime and cybercrime
Type I
(Largely online activities)
Type II
(Both online and offline activities)
Swarms
(eg. 'hacktivist' groups)
Hubs
(eg. 'scareware' operations)
Clustered hybrids
(eg. 'carding' forums and skimmers)
Extended hybrids
(eg.phone theft and online trading)

Source: BAE Detica/LMU

Fig.2. Structures of organized criminal groups engaged in cybercrime [12].

Looking at how cyber criminals are structured based on their mode of operations; it draws our attention to say that, we need to understand how cybercrime does occur so as to mitigate reoccurrence. Knowing how it occurs can also provide a step wise approach towards further investigation. In other to understand the basic approach towards investigating cybercrime, according to [15], "…..we need to understand the techniques and behaviors of these crimes so that we can build a defence mechanism that will counter their operations." [4], in their paper on 'Hacking: An analysis of current methodology' stated that:

> "……….*it is important to understand how hackers attack a system so that they can be stopped. In doing that, the methods used by hackers must be well understood." (p.1)*

These show that, for security experts to design a system that will counter cybercrime, they need to understand the crime itself and the way it do occur. These will lead to design of more robust counter mechanism that will elicit such occurrences in later time. To have knowledge about this infiltrated act of cybercrime, on the basis of this research, in section 4, we explore the limelight of cyber forensic as an emerging field of research to unveil cyber-crime activities.

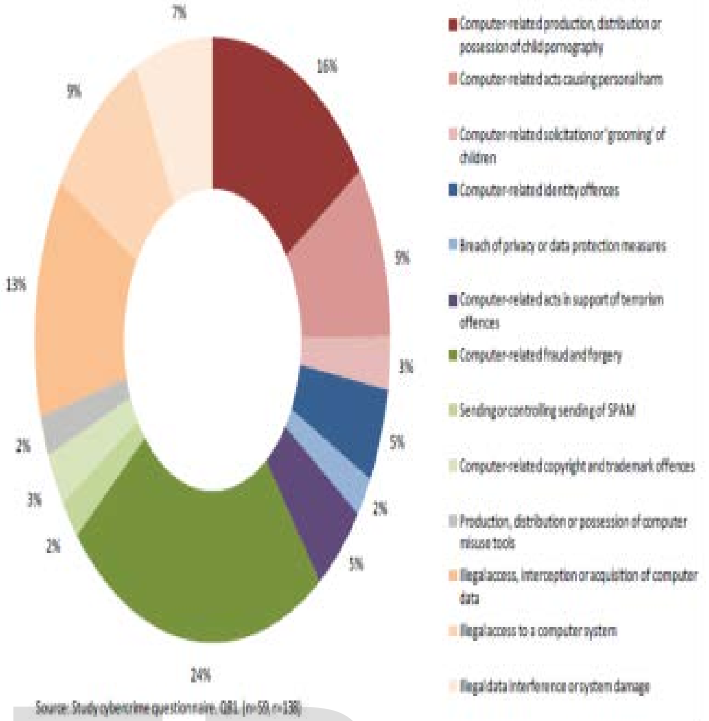
3 CYBER SECURITY

To further unveil the current approach needed in the investigation of cybercrime, it is very important to elaborate on the importance of cyber security and the need to explore in such field, so as to avert the escalation of compromising critical infrastructure by group of perpetrators. We cite [8] in their book titled 'Under cyber attack' saying:

> "*............for as much progress as organizations have made, many organizations still have a long way to go. As the rate and complexity of cyber attacks continue to increase, organizations need to act quickly to avoid leaving themselves exposed to a costly and brand-damaging security incident that shakes the confidence of consumers and shareholders." (p.8)*

This shows how significant cyber security is in ensuring that our records are kept secured. Cyber security is a phenomenon that plays an important role in the ongoing development of information technology, as well as internet services through enhancing security and protecting critical information that are essential to each nation's security and economic well-being [13].

The escalating violation of cyberspace has no doubt boost the existence of Information security experts in thinking beyond the box, henceforth, strategizing counter mechanism to resist any form of threads that may be detrimental to the security implementation on network Infrastructure. Even though, there is no universal solution to prevent being infiltrated, implementing security on cyber is a crucial need in fighting perpetration from perpetrators. Fig.3 is a pie chart illustrating the most significant cybercrime threats derived from cyber security questionnaire from law enforcement agency in the United States. Each percentage is map out based on the view of the most significant threats to less significant in occurrence.



Source: Study cybercrime questionnaire. Q81. (n=59, r=138)

Fig.3 Most significant cybercrime threats [12].

A network that did not undergo a routing test to ascertain it fitness in terms of security, may likely fall victim of hacking or invasion by unauthorized user(s). Per [9], highlighted the importance of security routing check where he pointed out that,

> "*……..threat landscape has progressed from unsophisticated "script kiddies" to hackers to insiders to today's state sponsored attacks, where enterprises are attacked because of who they are, what they do and the value of their intellectual property (IP)." (p.1)*

Firewall, antivirus, intrusion detection and intrusion prevention system (IDS &IPS) being among the security gadget in combating the menace of cybercrime has its own limitation, as information security expert have to create awareness about security breach and increases security in terms of the data stored on server. But there still remain an unresolved question; why security is being breached? We try finding some of these reasons as highlighted by [8] where they attributed some of the challenges to:

3.1 Lack of commitment from the Board

Most organizations that controls cyberspace lack executive support to establish a clear charter for the information security function and a long-term strategy for its growth. This has immensely affected the cyberspace to suffer infiltration of cybercrime, putting the organizations' data at broad risk (p.10).

3.2 Lack of Investment on cybersecurity

Looking at the cost effectiveness of implementing cyber security, most cyberspace owner needs to be willing to invest in cybersecurity. This is because; implementing security is a money consuming factor that needs better coordination so as to ensure business continuity (p.10).

3.3 Lack of continuous improvement

Organizations must establish a framework for continuously monitoring performance and improving their information security programs in the areas of people, process and technology (p.10).

3.4 Lack of proper physical security.

Organizations should ensure that all their information security technology is physically secure, especially with consideration for access to Wi-Fi. A security operation Centre (SOC) can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively. (p.10)

When security is being breached, information security experts in their part, only have understanding that certain crime has occurred but have little or no knowledge on how to trace evidence. Understanding types of crime and the way it occurs will help in mounting security tools to help fight crime. The concept of cyber forensic must be over emphasized to enable information security expert have a clear understanding on the kind of gadget they needed to develop that will meet the present challenges of security breach. Section 4, provides a clear knowledge about cyber forensic and the need to explore, so as to use the knowledge gain to create a counter mechanism that will fight cybercrime.

4 CYBER FORENSIC

This section describes the importance of cyber forensic and sets out the relevance of the design of our new forensic model that will serve as a panacea towards investigation of cybercrime. Cyber forensic is an area of scientific research that deals with investigation of criminal activities caused by criminal element that are at all cost, wanted to see the advent of internet becoming an illusion [1]. To embrace the existence of cyber forensic as an emerging field, first, we must admit that, there exists cybercrimes. We must also admit that, security expert alone cannot be entrusted in strategizing ways to eradicate cybercrime without cyber forensic experts. This is because; knowing types of cybercrimes (by security experts) and it effect on network infrastructure cannot provide remedy to the emerging challenges. Rather, understanding how it occurs (by cyber forensic) and the trace of evidence will help in strategizing the kind of countermeasures to put in place to prevent future reoccurrence. Perfectly erasing all traces is of course not always easy no matter how sophisticated an attacker is [10]. Therefore, since cyber forensic is an emerging field of research, it can be entrusted in curtailing the existence of cybercrimes. Cyber forensic will help to curtail the menace of criminal activities cause by criminal elements that intend to see cyberspace as an illusion. Cyber forensic investigations are often done as a post-event response to a serious information security or criminal incident. The examination is conducted in a systematic, formalized and legal manner to ensure the admissibility of the evidence and subject to considerable scrutiny of both the integrity of the evidence and that of the investigation process [3]. We cite researchers [1], citing Sin (2008), in which they state:

> *"Sin (2008) highlighted in his proceedings on new digital forensic investigation model that, 'Cyber forensic is the use of scientifically derived and proven methods towards the Preservation, Collection, Validation, Identification, Analysis, Interpretation and presentation of digital Evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations." (p. 53).*

However, most organizations foremost objective is not to secure evidence. But most often to find the offender, locate the intruder, and more importantly secure the infrastructure by minimizing, or if possible, get rid of vulnerabilities. In ensuring that, we need to explore through forensic readiness. Per [4] state that,

> *"Cyber forensic readiness is the organizations' potential to maximize the use of digital evidence to aid in an investigation, with the intent of: Reducing the time taken to respond to an incident, Maximizing the ability to collect credible and meaningful evidence, Minimizing the length/cost of a cyber-incident investigation, Reducing the incident recovery time, Preventing further losses."(p.7)*

Cyber forensic readiness claims that the time and cost required for an incident response during a digital forensic investigation should decrease while at the same time maintaining the level of credibility of the digital evidence being collected [4]. Therefore, in section 5, we proposed a new forensic model as a new approach toward the investigation of cybercrime.

5 NEW PROPOSED MODEL FOR CYBER FORENSIC

This sections lead to our design of new forensic model by evaluating already existed model adapted in the investigation of cybercrime and improving on it limitations towards ensuring quick response to incidence and trace of the perpetrators.

5.1 EXISTING MODEL

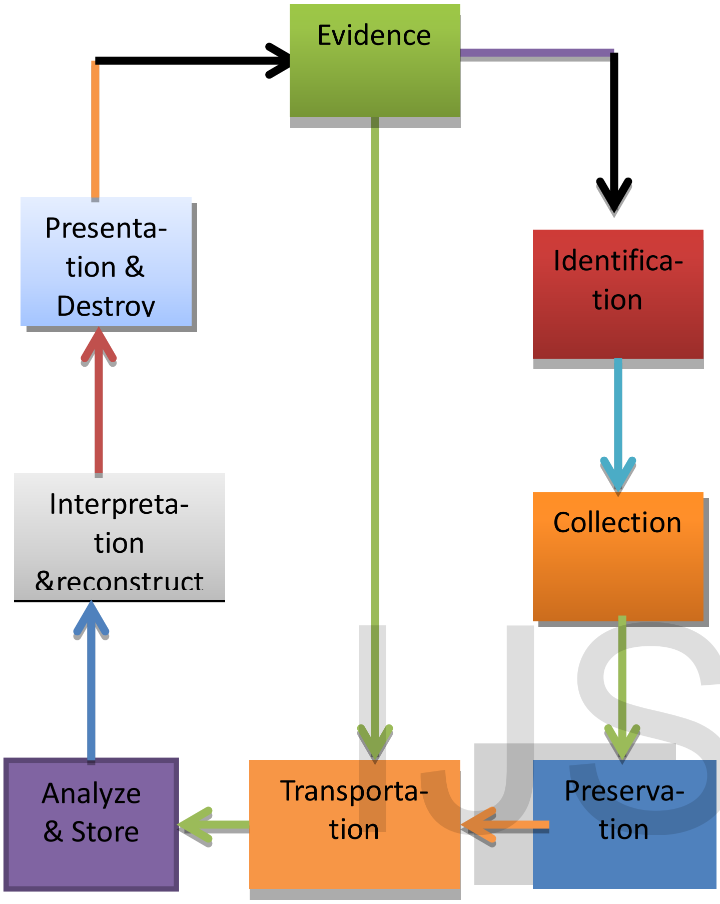


Fig.4. Existing model for cyber forensic investigation [7].

Fig.4 shows the sequence of the previous existing model of cyber forensic investigation as most often adapted by US federal bureau of investigation and association of chief police officer (ACPO). Some of the limitations of this model are that, investigations are carried out when a crime is reported to have occurred to law enforcement agency, this lack prompt response to incidence and also, time consuming to be able to link evidence to the perpetrator(s).

5.2 PROPOSED MODEL

The propose model is based on prompt response to cyber incidences. It will help find offender(s), locate the intruder(s), and most importantly secure the infrastructure through quick response. To then link the apprehended offender(s) with the committed act, the existing model in section 5.1, is then adapted for further search. Most importantly, the new model is derived from already existing model in section 5.1 by improving on its drawback. Below is the structure of the new forensic model for cybercrime investigation.

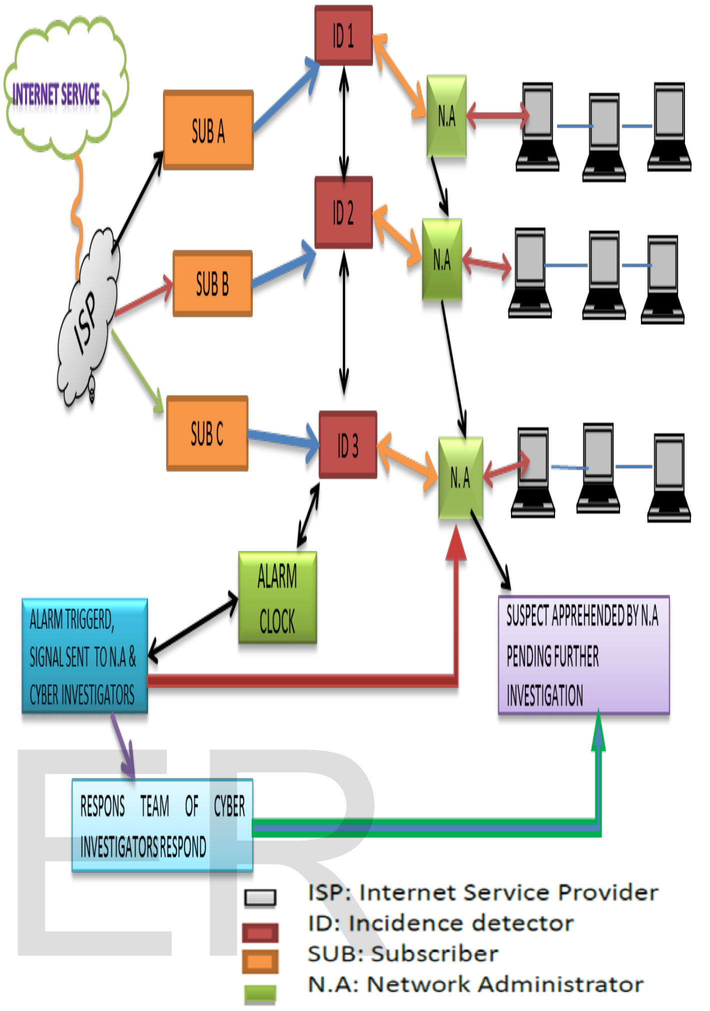

INTERNET SERVICE
ISP
SUB A
SUB B
SUB C
ID 1
ID 2
ID 3
N.A
N.A
N.A
ALARM CLOCK
ALARM TRIGGERD, SIGNAL SENT TO N.A & CYBER INVESTIGATORS
SUSPECT APPREHENDED BY N.A PENDING FURTHER INVESTIGATION
RESPONS TEAM OF CYBER INVESTIGATORS RESPOND
ISP: Internet Service Provider
ID: Incidence detector
SUB: Subscriber
N.A: Network Administrator

Fig.5. Newly proposed model for cyber forensic investigation in-apprehending perpetrator(s).

6 DISCUSSION

The design model in fig.5, is our new forensic model that will help in apprehending perpetrator(s) when they are facilitating critical cybercrime (DDOS, hacking, ID theft, password sniffing, online fraud, session high jacking) that affect network infrastructure. The proposed model is interpreted on cyber space located at the same geographical location. Further research will look at how we can replicate its concept on cyberspace operating in different geographical locations. In Section 5, figure 5, we experimented how three subscribers originated from an internet service provider (ISP).

Each subscriber extends his access to different network domain with a network administrator (NA) that monitors the activities of his network. Each network administrator has a separate communication link that extends communications to other administrator later terminated at the alarm clock through the incident detector (ID). The incident detector (ID) is monitored under the supervision of a forensic investigator(s). There is a smooth communication between the forensic investigators and the network administrator over any established network access. We also note the use of wireless networks by these subscribers. Administrator must ensure security to only allowed authorized users to connect to her network. If an intruder bypasses the security implementation of a network to guarantee access to his or her computer system, each network access by any computer system, from either subscriber(s), is generated by a secret code through the incident detector (ID) that will serve as a tag in monitoring the system performance. Every cyber activities from the three subscribers are being monitored by the incident detector (ID).

When a user is performing a suspicious act on the network, the incident detector (ID) will detect the subscriber's network tracing the computer system performing such act and alert the alarm clock, which triggered and sent information about the location of the incident; the type of computer; information about the system; and the operating system in used through a separate communication link to the network administrator and at the same time, alert the cyber investigators. The network administrator(s) then responds to the alarm that triggered on his system for prompt response to apprehend the perpetrator(s). A message via a secured link is sent to the cyber investigator(s) by the network administrator about the apprehension of the perpetrators and requires their quick response to begin carrying out the steps highlighted on the existing model in fig. 4, subsection 5.1. The greatest challenge that may arise from this type of model to work in apprehending perpetrators is the consistencies of network administrator(s) in monitoring their system at all times. This is the only hurdle that can posed thread to this model.

In ensuring that this model becomes achievable, jurisdiction must also play a vital role to ensure legal search warrant (license) is issue to forensic investigators to search and apprehend offenders at all times. The reason is that, depending on a countries jurisdiction, if an offender is being apprehended and further search for evidence is carried out by forensic investigators, without being granted license by the court to do that, on taking the perpetrator(s) to court, the jury may turn down the evidence by not being admissible. This is because, the court expect that, a case of intrusion must first be reported and later issue a search warrant that may guarantee further search for evidence. Not following the proper procedure may turn down evidence in court not to be admissible. This is another drawback to cyber investigations. To make this model works successfully, every country must give a full search warrant to forensic investigators to facilitate search for evidence at all times, not necessary a case of intrusion have to be reported to court and wait for search warrant, before embarking on investigations. These processes causes delay and leads to perpetrator(s) escape even when evidence is being traced. We note that, our new model is meant to apprehend offenders that are committing illicit act online.

Conclusively, the model ensures that, the cyber investigators have full access to all subscribers network by mounting up their forensic gadget at strategic position so as to monitor the countries cyberspace. It is expected that for such method to succeed, a country must agree to enact the use of cyber forensic, by investing so much on forensic equipment to ensure control traffic movement so as to detect any suspicious act.

7 CONCLUSION

Since cyberspace has become an ever demanding treasure of our time, there remain many security issues to confront ensuring that it can be secure. Crimes such as denial of service, spoofing, ID theft, DDOS, Sniffing, hacking, have geared towards compromising critical network infrastructure. The growing menace has posed lots of damages to cyberspace thereby causing valuable data and financial losses to both users and companies. This research elaborated the concept of cybercrime and relates the need on cyber forensic as an emerging field for investigation.

The research was able to highlight the importance of new forensic model to serve as a panacea towards the investigation of cybercrime. In the new model, we demonstrated the need of forensic investigators in apprehending perpetrator(s) on a network domain through deployment of incident detectors, alarm clock to a subscriber network to monitor and alert any suspicious activities. In our analysis, we further elaborated the needs to adapt on the existing model for further forensic search after apprehension of the perpetrator(s).

Our research later elaborated on the needs for jurisdiction to cooperate with forensic investigators in issuing a search warrant that may enable flexibility in their search for evidence. We later highlighted the need to replicate this new model across different geographical location to be in used by forensic investigators.

REFERENCES

[1] D. Gabi and A. Al-Nemrat, "Password Guessing Attacks: Analysis and Discovery of Evidence in Computer Forensic Investigation," In: S.R.G.Weir and A.Al-Nemrat (eds), *Proceedings of 2012 2nd International Conference on Cybercrime, Security and Digital Forensic (Cyfo – 12).* University of Strathclyde, pp. 53 – 72. 14-15 May, 2012.

[2] I. Gul and M. Hussain, "Distributed Cloud Intrusion Detection Model," Vol. 34, pp.71-82, 2011, [Online]. Available at: http://www.sersc.org/journals/IJAST/vol34/8.pdf (Accessed: 22 October, 2013).

[3] J.A. Fick, "Cyber Forensic Readiness: *An Integrated Approach,*" In proceedings on cyberCon Africa 2012,Enperor's Palace, Johannesburg, south Africa, 24-25 October,2012,pp.1-21.

[4] J. Tobler and K. O'Cannor, "Hacking: An Analysis of Current Methodology," In School of Computing, Information Technology and Engineering. Module Handbook, SDM025, University of East London, UK, pp. 1-33, 2011.

[5] J. Warner, "Understanding Cybercrime: A View from Below," *International Journal of Cyber Criminology*, 5(1), pp. 736-749, 2011.

[6] P. Danquah, O.D. Ogunsanwo and O.B. Longe, "Beyond E-Mail Headers: An Ethnography Based Model for Counteracting Socially

Engineered Cyber Deception," *In African Journal of Computing & ICT,* Vol.6 (5), pp.9-26, 2013. [Online] at: http://www .ajocict.net/ uploads/V6N5P2-2013 AJOCICT - Paper 2.pdf, (Accessed: 6th June, 2014).

[7] P. Sommer, "Directors' and corporate Advisors' Guide to Digital Investigations and Evidence," Second Edition, Version 2.1, Swidon, UK: IAAC, pp. 1-100, 2009.

[8] P. van Kessel and K. Allan, "Under Cyber Attack: *EY's Global Security Survey 2013*," UK: EYGM limited, pp. 1-24, [Online]. Available at:http://www.ey.com/Publication/vwLUAssets/EY2013GlobalInformation_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf, (Accessed: 9 June, 2013).

[9] R. Meadows, "'Five Things Every Organization Should Know about Detecting and Responding to Targeted Cyberattacks," press release, 2013. [Online]. Availableat :http://www.ey.com/US/en /New sroom/News-releases/News Five-Things-Every-Organi zation-Should-Know-about-Detecting-and-Responding-to-Targeted-Cyberattacks, (Accessed: 9 June, 2013).

[10] R. Bohme, C.F. Freiling, T. Gloe and M. Kirchner, "Computational Forensics," In: H.M.J.Z.Geradts, Y.K.Franke and J.C.Veenman (eds) *Proceeding of the Third International Workshop (IWCF 2009).* Hague, Netherland, pp. 1-180. 13-14 August, 2009.

[11] S. Anson and S. Bunting, "Mastering Windows Network Forensics and Investigation," Canada: Wiley Publishing, Inc, 2007.

[12] S. Malby, R. Mace, A. Holterhof, C. Brown, S. Kascherus and E. Ignatuschtschenko, "Comprehensive Study on Cybercrime," Vienna, Australia: UNODC, pp.1-300, 2013.

[13] S. Yadav, T. shree and Y. Arora, "Cybercrime and Security," *International Journal of Scientific and Engineering Research,* vol.4, Issue 8, pp. 855-861, 2013.

[14] W. Kapuku-Bwabwa, H.A. Tawail, H. Jahankhani and H. Jahankhani, "Using Semantic Web Techniques to Build an Intelligent Cybercrime Reporting System for The UK," In: S.R.G.Weir and A.Al-Nemrat (eds), *Proceedings of 2nd International Conference on Cybercrime, Security and Digital Forensic (Cyfo – 12).* University of East London, UK, pp.185 – 196, 14 – 15 May, 2012.

[15] Z. Goetz, V. Berk, G. Jiang and D. Burroughs, "Cyber Attack Techniques and Defense Mechanisms," *Investigative Research For Infrastructure Assurance Group*, Institute for Security Technology Studies, Dartmouth College, pp.1-49, 2002.