GRAND ACADEMIC PORTAL
RESEARCH JOURNALS

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

ROLE OF FORENSIC PSYCHOLOGY IN CYBER INVESTIGATION

Savithri. K.K, Dr. Priyanka Kacker

M.Phil. Forensic Psychology Student, School of Behavioural Sciences, National Forensic Sciences University, Gandhinagar, Gujarat

Senior Assistant professor
School of Behavioural Sciences, National Forensic Sciences University, Gandhinagar, Gujarat

Abstract

This paper focuses on the application of forensic psychology tools in cyber investigation and tries to light on cyber forensic equipment. The internet helped us greater in communiqué and all similar trends. Except for those features, the digital global has extended its hands to unlawful activities. We can't blame technology for crimes, it is all about who is using it. Cybercrimes is likewise about the maladaptive behaviour of human and Disrupted existence. In cybercrime investigations analysing human behaviour is inevitable. Cyber psychology is interdisciplinary vicinity wherein behavioural science and cyber technology merge. Exceptional forensic tools are used in the cyber investigation are autopsy, O.S. forensic toolkit, RAM forensics, TrueCrypt, DFF, and Wireshark, etc. Cyber-crook behaviour may be analysed via the utility of forensic psychology strategies. Forensic psychology investigation tools are applicable in cybercrimes as well. Cyber-criminal behaviour can be analysed through the application of forensic psychology techniques. It can be utilized for the identification, and authentication of the perpetrator who has executed cybercrime or to show his innocence. Deception detection techniques are very beneficial to screen those criminals who've been committed cybercrimes. Criminal profiling and Geographical profiling will plot the personality picture of the cyber offender.

Keywords: *Cybercrime, Geographic Profiling, Criminal Profiling, Forensic tools, Forensic Psychology*

INTRODUCTION

Human brains are just as computers or more complicated than computers. How much the brain mechanisms are complicated that much the human behaviour is also complicated. Society binds every individual with socialization. Socialization binds the human brain in a way the society needs a human. Through this training of society, individual behaviour attuned with the culture. The love and care which starts from the family itself shaping an individual to be a good citizen or law abided one. The ruptures in the pace of life make an individual's behaviour eviler, based on how the person perceives those ruptures. Broken childhood, broken mind break the mould of socialization and promotes irregularities in human behaviour. Facing abandonment, avoidance from caregivers and parents at the earlier ages of life contributes to disruption in mental development. Lack of moral development may the result of abnormalities in the brain areas, especially in the orbitofrontal cortex, amygdala [12]. Impairment in the executive functions of the prefrontal cortex also alters the expression of aggression and criminal behaviour [12]. Being more introverted, melancholic but hardly trying to get mingle with society. But the broken wing of them not allows being a part of society. Harassment, bullying that encountered in the path of life makes them more against society.

Broken-winged people may turn into anti-heroes of society. We can see some of them in prisons, correctional homes, etc. But some of them are in the dark. We cannot see their real face in the light. They will put a super colourful mask over their behaviour. In the sunlight, they all like socialized humans. But in the dark world, some of us experienced their nasty activities. A dark world doesn't mean a crowded, congested underground for goons. Moreover, the dark world stands for the virtual world, where we might feel we are safe; but we are not. One click in your sophisticated computer will show you the entire universe, from the neighbouring to White house of America. You are not that much a social being in real life but you are the angel of mercy in your social media accounts. As a social media person, you might protest there only and share your emotional swings there. It's enough for a black hat hacker to control you. They hide their maladaptive behaviour in public and they show the teeth in the Internet world. What they perceived from their life, could be a grudge, rage, violence, and pain, or anything else, they will inject that pain into their victims. We might think our phone is off but it talks to others, it shows our privacy to the world. Invisible criminals and invisible attacks are extremely demanding in this technoid period. Internet becomes the easiest way to get prey without a shield. It is the trouble-free road for cybercriminals to acquire their needs; it could be money or personal grudges such as defaming someone etc. What not possible in Virtual reality. The Internet helped us more in communication and all further developments.

Besides those qualities, the virtual world has extended its hands to unlawful activities. We cannot blame technology for crimes, it is all about who is using it. Their intention and thoughts put others in peril.

I. CYBERCRIMES AND INVESTIGATION

Cybercrimes, it's not all about computers and the internet. Cybercrimes is also about the maladaptive behaviour of human and Disrupted life development. In cybercrime investigations analysing human behaviour is inevitable. Cybercrimes it's about human behaviour. When we analyse human behaviour in cyberspace it is called cyber psychology. It is an interdisciplinary area where behavioural science and cyber technology merges. Cybercrime investigators are who know the internal process of computers and technology. An investigator must aware of cyber technology and the behaviour pattern of criminals. Cyber forensics is the discipline where the investigations of high-tech crimes were done. Cyber forensics is also called digital forensics. Cybercrimes are vigorously growing offenses all over the world. Computer-related crimes are two kinds' cyber-enabled crimes and cyber-dependent crimes. Cybercrime investigation enables probes in different ways using ICT (Information and Communication Technology).

Digital forensics deals with the collection, examination, and analysis of the evidence of cybercrime and the presentation of that evidence in the court of law. Cyber forensics aims to the vigilant collection, well chain documentation of the pieces of evidence. Digital forensic analysts follow a protocol to collect evidence. They physically seclude the affected device and make a digital copy of that device. After copying the device, the analyst will seal the entire device for further analysis. Using different Forensic tools analyst will check the device and recovered files. Damaged files, malware activity, other recovered files will be verified for resolving phishing, bank fraud crimes, money laundering, and child exploitation. The memory of the computer or any device will be examined by forensic analysts; this discipline is known as Memory forensics. Cybercrimes are ranging from online harassment to big bank financial frauds.

Cybercrimes are about the data derived from computer systems, networks, wireless transmissions, and other devices. In digital forensics, analysts authenticate the data and submitting it to the court of law. Computer and network forensics are used to track down the computers that were stolen. This area deals with the theft of trade secrets or other evidence of homicide, murder, etc. in the system. In a murder scene, forensic scientists will collect all biological evidence and physical evidence. Like that in high-tech crimes, investigators will collect all possible evidence from the software and hardware of the device. Different forensic tools that are used in the cyber investigation are autopsy, O.S. forensic toolkit, RAM forensics, TrueCrypt, DFF, and Wireshark, etc.

II. FORENSIC TOOLS USED IN CYBER INVESTIGATION

Autopsy: Generally, the term autopsy is the thorough examination of a corpse and its internal organs to find out what caused the death of a person. It is a Medical examination of dead bodies found in suspicious circumstances. When autopsy comes to the area of cyber forensics, it is the examination of hard disk drives and smartphones. An autopsy is a tool used in cyber forensics that allows the investigator to find out add-on programs or develop programs in Java, python. This tool automatically explores the disk contents. Autopsy enables the recovery of all data from the memory card. Autopsy provides two types of investigations. The first one is the Dead investigation means total analysis of a suspected system. The second analysis is a live investigation, where the suspected system is analysed in running mode. In this method, autopsy runs in an untrusted environment using a CD. In dead investigation mode, autopsy runs in a reliable environment.

Digital Forensics Framework, shortly known as DFF. It is open-source software used by experts and non-experts. DFF is used to collect, preserve, acknowledge the data from the device without making any difference in data, system, and network. Easy retrieval of original data without any correction is the main feature of DFF. DFF uses python interpreters and coded with C++, python languages. DFF works in both Windows and Linux.

SIFT is another forensic tool used to help the cybercrime response teams and researchers to assess the data on systems. SIFT allows an investigator to access any local or remote devices. It runs on Windows and Linux systems.

Oxygen Forensic detective, a multi-platform application used by professionals and non-professionals. OFD helps investigators to extract data from any device. It grabs passwords from encrypted devices. OFD is capable to extract flight information from drones. This tool can be run in Linux, Windows, and Mac OS.

Open Computer Forensics Architecture, is software developed by Dutch National Police Agency. Open Computer forensics Architecture is entwined with popular cybercrime investigation tools such as the sleuth kit, scalpel, photoRec, and others.

Bulk Extractor extracts critical data from digital evidence. URLs, email addresses credit card numbers, etc., can be extracted by this Bulk extractor.

WIRESHARK is a network analyser used by cyber investigators to determine the network activities, connection, protocol, and network traffic. It is a free open-source packet analyser, which analyses all packets of the network. A Packet can be defined as a small section of the large message transmitted through networks or a small division of the network. Wireshark inspects a high level of traffic in our network. Wireshark can be used in Mac, OS X, Windows, and UNIX - based systems.

True Crypt is a free open-source tool for encryption. True Crypt is a freeware that encrypts the hard disc facility of the system, which gives full encryption to data and information. True crypt encodes the information.

Operating System Forensics is also denoted as O.S. Forensics. It is a toolkit that directly explores the memory of the system. This tool provides the facts about the computer and its files loaded in memory. O.S. manages the task performance of the system and enables the details of kid's activity on the system. Operating system forensics tool directly installed in the memory. The aforementioned tool is capable to discover evidence faster than any other equipment; it identifies malicious file activity, using RAM forensics effectively. These are the forensic tools that are used in cyber forensics to investigate cybercrimes.

III. FORENSIC PSYCHOLOGY INVESTIGATION IN CYBER CRIMES

Crimes are all about maladaptive human behaviour. How the offenders possess their behaviour is a predestined fact, which roots from how their life situations play havoc with their perception. In cyberspace, people follow certain etiquette and rules. The one who breaks that etiquette in the cyber world is an offender. Cybercrimes are equally elucidating on criminal behaviour in the cyber world. Forensic psychology as a super disciplinary knowledge area deals with numerous aspects of criminal behaviour at the individual level. Forensic psychology investigation tools are applicable in cybercrimes as well. Cyber-criminal behaviour can be analysed through the application of forensic psychology techniques. It can be utilized for the identification, and authentication of the offender who has done cybercrime or to prove his innocence. Deception detection techniques are very useful to screen those criminals who have been committed cybercrimes. Criminal profiling and Geographical profiling will plot the personality picture of the cyber offender. Software called GeoCrime Geographic profiling using geographic profiling techniques to find serial cyber offenders [4]. The action of forensic psychology in the cyber field creates a multifaceted study area called forensic cyber psychology, where we use forensic psychology tools and theories to find out the offender and collect corroborative evidence to support the primary evidence of cybercrime.

IV. APPLICATION OF FORENSIC PSYCHOLOGICAL TOOLS IN CYBERCRIMES

Some theories of forensic psychology are very much applicable in cybercrimes. Routine activity theory, rational choice theory, and social learning theory are explained about the chance of being victimized in cybercrimes and it gives insight into internet crimes, victimization, and criminal behaviour in cyberspaces. Routine activity theory states three different aspects of cybercrimes. It stresses on the offender and the offender looks for a target without protection or looks for vulnerable targets. Those types of targets mostly available in cyberspaces, they are unprotected and very vulnerable to attacks.

Criminal profiling and geographical profiling can be utilized to find cyber offenders, especially serial hackers. Criminal profiling aiding cybercrime investigation with to intentions: identify and understand the offender [6]. Lie detection techniques are utilized as a screening for offenders and to detect whether they have done the crime or they haven't.

Criminal Profiling is the technique used by the investigative agency or crime investigators to identify and understand the offender. The investigation officer makes inferences about the characteristics and personality of the offender. Few terms are equivalent to criminal profiling. "Offender profiling", "criminal investigative analysis", "crime action profiling" is synonyms for criminal profiling. The criminal investigative analysis is the term that given by the federal bureau of investigation to criminal profiling. Chasing the criminal behaviour in a virtual crime scenario is difficult when comparing to the real crime scene. Therefore criminal profiling in cyberspaces is a challenging task for forensic psychologists; they need more experience with cyber activities. Offender profiling is a very robust technique in cyber-crime but some researchers look over it as an immature science [1].

The primary objective of criminal profiling is to recognize and pick out the cyber offender. It is not an easy task when there is a day-by-day advancement in technology. Deductive and inductive approaches are the two techniques used under criminal profiling to make offender profiles. Identifying connections is very important in offender profiling. The queries that about profiling are how accurately the behaviour of computer criminal can be assessed and can be profiling is successful [15]. Based on available studies and research, it is possible to analyse the behaviour accurately and almost all criminals are caught through criminal profiling. So the answer to both questions is "yes".

Geographic Profiling is another psychological profiling to locate the area of an offender. Geographic profiling is often used in the detection of serial killers. It is a criminal investigative analysis where different locations are connected with the series of crimes happening. In cybercrimes, the offender might alter their location by changing their IP address frequently. However, investigator will use advanced technologies to overcome the aforementioned issue. Geographical profiling has been used in Credit card skimming and phishing crimes. Researchers developed software called GeoCrime geographic profiling to assist in mapping, location, and statistical analysis in certain cybercrimes [4]. Cyber forensics always makes use of digital profiling. Digital profiling is much different from criminal profiling and geographic profiling. But it is using the basic approaches of criminal profiling [7].

Usage of Lie detection techniques in Cyber investigation: Polygraph is a forensic psychological tool that uses psychophysiological changes in the body to analyse the deception of the offender. Pneumograph, sphygmograph, skin conductance, plethysmograph, and movement monitoring system are the five parameters that we used in the polygraph. Polygraph is mostly used as a lie detection technique by investigation agencies and investigation officers. In India, the polygraph is considered corroborative evidence. In Cyber investigation polygraph is utilized as a preventive measure. Most of the researches used polygraphs after conviction. Post-conviction polygraphy can be employed as a solution for the prevention of victimization in child pornography [3]. Deception detection techniques can be used as screening of the cyber offenders to assure if they have done the crime or not; HSBC employee, Nadeem Kashmiri went through polygraph and Narcoanalysis for a cybercrime (BPO fraud case) [18]. Deception detection techniques are more advanced today; it is advancing day by day. In a developing era, Brain tells the truth. The brain is being monitored by the researchers to know the deception and truth. Indian Scientist, Prof. Dr. Mukundan developed a forensic psychological tool called BEOS – ***Brain Electrical Oscillation Signature Profiling***. It is used to detect the offender by detecting experiential knowledge about the crime. BEOS using probes to extract the electrical activities of the brain. Probes are the short semantic meaningful statements. These verbal statements will provoke the remembrance of a personal event associated with sensory, motor, and other components of the individual [9]. Cyber investigation can be done through BEOS profiling. Here investigator will be used two sets of probes. Using standard probes for cybercrimes, it is possible to detect the offenders from the suspects in BEOS [13]. There are another forensic psychology tools but have been not used or applied in cyber forensics. More researches should be done in this area that is a future goal. Multidisciplinary knowledge interaction makes more advancement in the realm of cybercrime investigation.

REFERENCES

[1] Bednarz, A. (2004, November 29). Profiling cybercriminals: A promising but immature science. Network World. Retrieved from https://www.networkworld.com/article/2327820/lanwan/profiling-cybercriminals--a-promising-but-immature-science.ht

[2] Bossler, Adam & Berenblum, Tamar. (2019). Introduction: new directions in cybercrime research. Journal of Crime and Justice. 42. 1-5. 10.1080/0735648X.2019.1692426.

[3] Buschman, J., Bogaerts, S., Foulger, S., Wilcox, D., Sosnowski, D., & Cushman, B. (2009). Sexual History Disclosure Polygraph Examinations with Cybercrime Offences. International Journal of Offender Therapy and Comparative Criminology, 54(3), 395–411. doi:10.1177/0306624x09334942

[4] Butkovic, Asmir & Mrdovic, Sasa & Uludag, Suleyman & Tanovic, Anel. (2018). Geographic Profiling for serial cybercrime investigation. Digital Investigation. 28. 10.1016/j.diin.2018.12.001.

[5] Ebisike, N. (2007). The use of offender profiling evidence in criminal cases. Theses and Dissertations, 23.

[6] Garcia, Natasha. (2018). The use of criminal profiling in cybercrime investigations.

[7] Kaur, Mandeep & Kaur, Navreet & Khurana, Suman. (2016). A Literature review on Cyber Forensic and its Analysis tools. IJARCCE. 5. 23-28. 10.17148/IJARCCE.2016.5106.

[8] Kipāne, Aldona. (2019). Meaning of profiling of cybercriminals in the security context. SHS Web of Conferences. 68. 01009. 10.1051/shsconf/20196801009.

[9] Mukundan CR. (2008). BEOS Profiling in Crime Investigation. Abstract, the Annual Conference of Division of Forensic Psychology. *British Psychological Society*, 24-26. 14.

[10] Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. Digital Investigation, 2(4), 261–267. doi:10.1016/j.diin.2005.11.004

[11] Nykodym, Nick & Taylor, Robert & Vilela, Julia. (2005). Criminal profiling and insider cyber crime. Computer Law & Security Review. 2. 408-414. 10.1016/j.clsr.2005.07.001.

[12] Reddy, Kalapalli & Rajan Menon, Karishma & Hunjan, Unnati. (2018). Neurobiological aspects of violent and criminal behaviour: Deficits in frontal lobe function and neurotransmitters. International Journal of Criminal Justice Sciences. 13. 44-54. 10.5281/zenodo.1403384.

[13] Roy, G.S., and Kacker, P. (2019). Cyber Crime Investigation through BEOS Profiling https://www.gapinterdisciplinarities.org/res/articles/67-72.pdf.

[14] Spicer,J.(2019). Cyber criminal profiling. Edpacs, 117. doi:10.1080/07366981.2019.1675965

[15] Tafoya, W. L. Criminal Investigation Analysis and Behavior: Characteristics of Computer Criminals (p. 55). CRC Press. In Johnson, T. A. (2006). Forensic computer crime investigation. Boca Raton : CRC, Taylor & Francis, 2006, pp. 55-90.

[16] Tompsett, Brian & Marshall, Angus & Semmens, N.C.. (2005). Cyberprofiling: offender profiling and geographic profiling of crime on the Internet. 2005. 21 - 24. 10.1109/SECCMW.2005.1588290.

[17] Veena, K., & Visu, P. (2016). Detection of cyber crime: An approach using the lie detection technique and methods to solve it. 2016 International Conference on Information Communication and Embedded Systems (ICICES). doi:10.1109/icices.2016.7518885

[18] https://www.outlookindia.com/newswire/story/nadeem-kashmiri-undergoes-polygraph-test/396417