Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 06, June-2023

New Technology Crimes – Reinforcing the Forensic Laboratory to Manoeuvre Ultra-Electronic Delinquencies

P N Ramakrishnan[1] & P R Harshith[2]
1 - Assistant Director & Scientist-C (Physics)
Physics & Digital Forensic Division
Central Forensic Science Laboratory,
Ministry Of Home Affairs,
Directorate Of Forensic Science Services
Ramanthapur, Amberpet Po, Hyderabad, Telangana, India

2 – Internship(Digital Forensic) Student B.Tech(It) 4th Year
Vardhaman College Of Engineering
Autonomous College Under Jntuh
Shamshabad Hyderabad

ABSTRACT

The rapid transformation of the crime landscape in recent years, particularly in the post-COVID era, has been marked by the widespread adoption of Information Technology (IT) across the world. Even underdeveloped countries have embraced the use of advanced digital technologies, electronic devices, and innovative IT applications in their day-to-day activities. However, these advancements have also given rise to new forms of organized and unorganized electronic crimes, including the misuse of contemporary digital currency, online transactions, hybrid models of education and employment, online trades, drone technology, Internet of Things (IoT), 3-D printing, digital certifications, nano-technology, and security-related documentation. Moreover, the proliferation of the Dark Web, proxy servers, and Artificial Intelligence (AI) has provided savvy criminals with unparalleled flexibility and anonymity in committing electronic delinquencies. In response, forensic science laboratories must strengthen their capabilities, resources, and expertise to effectively combat these emerging challenges within the boundaries of the law. This paper presents proposals for enhancing forensic laboratories to address the evolving nature of electronic crimes.

Key Words: Forensic Science laboratory, Electronic Crimes, new technology

1. INTRODUCTION

The threat to any country through the new advanced technology crimes have become serious and at times threat to the nation. The revenue generated by such high tech-savvy criminals are crossing millions and trillions in each currency value. This has more impact on the economy of the nations and which indirectly effects the society in general. While these technology advances like the Internet of Things (IoT) along with ease of availability of the Information Technology and electronic devices have been a boon to the nation and public. While with the same technology, the society is being abused and exploited with hidden intention. The remoteness of the tech-savvy criminals and adaptability to the changes in the area of IT field and utility of the technology, the speed and spread all across is very fast and identification of the *modus operandi*such delinquencies are highly challenging and its effect is more extensive. The minimize the redundancy period by the forensic scientists and technology in

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 06, June-2023

tackling such high technology crime scenarios in the wake of technological advancements and need for robust forensic capabilities to counter and help theland of law, is need of the hour.

2. OVERVIEW OF HIGH TECHNOLOGICAL DELINQUENCIES

The advancement of the emerging technology and influence of the internet has high impact in augmentation new form of high technological delinquencies. These delves deeper into the various forms of new technology electronic crimes that have gained prominence. The phenomenon has become global and borderless. The reconnaissance of such crimes has links to easy access to the detailed mapping technology and its data, satellite and street views andvast theft of the vital bank related information including the biometric digitalized data. This has vast linkage with most of the services and the electronic devices connected mostly through the internet and information technology including the Apps in form in the smart telecommunication devices like mobile technology and mobile phones. The world is still facing the threat aspects of cybercrimes involving ransomwares, malwares, online cash payments, online trades etc. It also entering the digital economies like cryptocurrency and data breaches or intellectual property and illicit contraband goods etc. in recent years.

The Intellectual Property Rights (IPR) is facing the infringement, this includes the high-quality counterfeit currency cross border transit. These high technology crimes are found being carried out through the Darknet and proxy servers. The Compromised Data is also found to have commonly traded through online and furtherance the boosting the financial fraud such as like the compromised payment card data or bank login account details etc.

In the field of the communication technology and cyber terrorism use of Voice-over-internet protocols (VOIP), Live Streaming etc. have rampantly used. Use of secure ‘Apps’ and the devices they operate upon also have become pertinent in increasing of secure with most advanced end-to-end encryption for such communications. This have become the forensic laboratories using the traditional examination techniques rendering to fail to meet the requirement to LEAs.

The advent of 3-D printing technology also had given room for the unauthorized making of hand guns, ATM Skimmers etc. for illicit purposes. The Drone technology and had been used by terrorist, transportation and delivery of drugs and other contrabands for distribution or trafficking may be a few obvious samples seen in new era of crimes. The Internet of Things (IoT) crimes exploits the vulnerabilities in any IoT systems and can execute malicious instructions that could endanger human lives such as pace makers, medical infusion pumps and smart cars etc. Also, at certain instances or environments IoT can be used as an eye witness as it can record the exact time of an intrusion and indicate the intruders route by the help of logs, like device hijacking, botnets and DDOS attacks.

Social Engineering frauds, political manipulation, undermining trust and authenticity of videos and images including the audio, impersonation and identity thefts using the Deep Fakes using the Artificial Intelligence (AI) technology where by giving a large enabling of the high-tech savvy criminals to commit the crimes related to both of social engineering and financial frauds.

In Nano-Scale espionage, these the high savvy criminals could exploit the nanotechnology to create advance surveillance devices that are nearly undetectable. Which can lead to the cases of unauthorized spying or gathering of the vital installations and sensitive areas like defence, air force and other maritime details.

With the introduction of Crypto Currency like Bitcoin, Ethereum, Solana, Monero etc. and its wide spectrum of handling by the society, it was found that new era of Fraudulent Initial Coin Offering (ICO), Ponzi schemes, Ransomware attacks,

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 06, June-2023

Money laundering, Darknet (like Silk road) market places, tax evasion etc. have become a hard nut to crack for the investigators as well as forensic scientists.

3. CHALLENGES AND STRENGTHENING FORENSIC LABORATORY CAPABILITIES.

Forensic science laboratories play a critical role in combating electronic crimes, but they face significant challenges in effectively addressing these complex offenses. The existing constraints faced by forensic laboratories which highlights the importance of technological advancements, increased capacity, and a skilled workforce to overcome these obstacles.

The paper emphasizes the need for specific measures to strengthen forensic laboratory capabilities. It proposes adopting state-of-the-art technologies and upgrading equipment to keep pace with evolving electronic crimes. Additionally, enhancing the skills of forensic experts through comprehensive training programs and fostering collaborations with academia and industry are vital steps towards improving laboratory capabilities.

Furthermore, the utilization of advanced technologies, including artificial intelligence (AI) and machine learning, is crucial in tackling electronic crimes. This section delves into the potential of AI in evidence analysis, data mining, and pattern recognition, offering insights into how forensic laboratories can leverage these technologies to streamline investigations and enhance efficiency.

Collaboration and information sharing are essential components of a comprehensive approach to combating electronic crimes. The paper also emphasizes the significance of establishing platforms for information exchange, fostering international cooperation, and promoting interdisciplinary partnerships among forensic laboratories, law enforcement agencies, and other relevant stakeholders.

While combating electronic crimes, it is essential to navigate legal and ethical boundaries. This section underscores the importance of adhering to legal frameworks, privacy regulations, and ethical guidelines to maintain the integrity of forensic evidence and ensure its admissibility in court.

4. CONCLUSION

In conclusion, this paper highlights the significance of strengthening forensic science laboratories to effectively tackle electronic crimes in the new era. By implementing the proposals outlined herein, forensic laboratories can significantly enhance their capacity to combat emerging criminal activities in the digital realm. Continuous adaptation, investment in technology, and collaborative efforts are essential to create a more secure and just society.

5. ACKNOWLEDGMENT

The author likes to express sincere gratitude to Mr. Sujay Saha, Director, CFSL, Hyderabad, for his support of this article. The author also acknowledges Dr. S K Jain, Director-cum-Chief Forensic Scientist, DFSS, MHA, New Delhi, for kind enough to nominate and timely guidance in completing this article within a short period. Lastly, the author extends thanks to all the Senior Scientists of the CFSL, Hyderabad, for their support and literary contributions.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 06, June-2023

6. REFERENCES

[1] Hargreaves, K. (2018). Strengthening the Forensic Science System: Ensuring Quality, Validity, Reliability, and Integrity. The National Academies Press.
[2] Casey, E., & Dietrich, D. (Eds.). (2017). Digital Forensics and Incident Response: Practices and Standards. Syngress.
[3] Gubbi, J., Buyya, R., Marusic, S., &Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.
[4] Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.
[5] Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering privacy by design. Computers, Privacy & Data Protection, 2011.
[6] Gercke, M., &Kryszczuk, V. (2013). Cybercrime and cloud forensics: Applications and research directions. In Proceedings of the 10th International Conference on Information Systems Security (ICISS), 1-16.
[7] Singh, L., & Chauhan, A. (2019). Leveraging AI for forensic analysis of digital evidence. In 2019 International Conference on Intelligent Sustainable Systems (ICISS), 7-11.
[8] Bouchard, M. (2020). Countering Darknet Marketplaces: An Exploratory Study on Legal Approaches and Challenges. In 2020 International Conference on Information Management and Technology (ICIMTech), 225-230.
[9] Interpol. (2018). Digital Forensics and Electronic Evidence: An Overview of Challenges and Tools. Retrieved from https://www.interpol.int/News-and-Events/News/2018/Digital-forensics-and-electronic-evidence

(This work is licensed under a Creative Commons Attribution 4.0 International License.)