# *"Cybercrime profiling: A Literature Review."*

## Abstract

*Humanity has always been fascinated by the crime profiling field's contribution and achievements, particularly in serial murderer instances that local communities have faced over the years. Tracing back the roots in the 19th century and the Jack the Ripper's case and coming forward to the modern era, criminal profiling has evolved significantly as an investigative aid for the conventional and digital crime. The prevalence of technology and the digitalisation of the contemporary world have transformed crime correspondingly, stressing the profiling domain to adapt accordingly.*

*This paper examines the literature to explore the cybercrime profiling field and its fundamental theories, techniques, tools, and developments that have formed this domain hitherto*, *intending to extract conclusions and identify gaps to aid the race against cyber criminality.*

## Introduction

The pervasiveness of cybercrime has become unequivocally one of our modern world's most intractable and persistent problems. Its exponential rise has an inconceivable impact on every facet of our lives across the globe. The term cybercrime from this point on will be interpreted as "criminal acts committed using electronic communications networks and information systems or against such networks and systems" (European Commission, 2007). This term implies that offenders can use electronic means for their purposes, or their target could be the means itself. Where the electronic means is just the crime tool, the digital profile retrieved from the device and the corresponding evidence may be instrumental in the actor's investigation (Rogers & Seigfried-Spellar, 2014).

According to Cybersecurity Ventures, the total cost from the cyber attacks is expected to reach 10 trillion US dollars by 2025, an estimation that constitutes the most significant economic wealth transfer in human history (Morgan, 2021). Aside from the irrefutable economic impact, technological and communication advancements have also provided new opportunities for conventional crime to cover obscure activities by upgrading their actions' efficiency and complexity. This fact urges now more than ever the need for multidisciplinary collaboration in the profiling process.

Criminal profiling principles and practices still apply despite the crime's digital transformation and the differentiation of the threat landscape. Human is still the prevalent factor behind every crime committed online or physically. The most significant contribution of the profile investigator is to provide insight into the offender's motives and way of thinking, narrowing the suspect list and optimising the process and the given resources (Steel, 2014).

## A. Fundamental Profiling Theories - Approaches

### *Inductive / Deductive approach*

Inductive criminal profiling is a method of argumentation that moves from the broad to the particular. In this respect, a comparison or statistical correlation is employed to ascertain an offender's psychological and behavioural characteristics. In contrast, the deductive follows the opposite way and relies on evidence or logical assumptions and hypotheses to conclude. It depends on the premise that the conclusion is correct if the previous arguments are correct. In their review, Bada and Nurse (2021), in their literature review, noticed that the deductive technique was the most frequently used method since it was deemed more applicable to case-based research in which the offender's specific features are the intended conclusion.

### *FBI framework*

The FBI model possesses a prominent position in the criminal profiling field, and it is mentioned in almost every paper that has been examined. This framework is based on specific attributes like social and sexual competence, birth order, access to a car, work and marital status and other relevant characteristics to conclude (Rogers, 2003). It is predicated on a dichotomy of organised and disorganised perpetrator types. It has been extensively criticised for being intuitive and generalised, with no scientific proof to back it up. Turvey (2012b) disagrees with the framework's absolute nature in his book. Among others, he points out that only forensic analysis can shed light on how and why a crime scene presents itself in a particular instance. Furthermore, due to its extensive reliance on demographic data, this strategy is considered inefficient when used in online criminal cases, omitting similar methodologies' social and psychological components. (Bada & Nurse, 2021).

### ***Investigative Psychology***

Canter and Youngs also criticise the FBI model in their work for its scientific inefficiency and lack of empirical data. They attribute the extent of its diffusion to the "Hollywood effect," which refers to the fictional manner criminals are depicted in movies or newspaper headlines (Canter & Youngs, 2005). As its name implies, Canter's model is founded on psychological principles and follows the inductive approach. He presented a wide variety of empirical research in known criminal cases to draw conclusions and establish connections with unknown perpetrators in order to answer questions like what criminal traits are essential? Which data is deemed critical? Where is the suspect located, and is he involved in other cases? (Canter & Youngs, 2005).
Like most inductive methods, it has also been criticised for its heavy reliance on data accuracy (Donato, 2021).

### ***Behavioural Evidence Analysis***

Behavioural Evidence Analysis (BEA), developed by Brent Turvey in 1997 and unlike the previous methods, is inherently deductive, not reliant on statistical data and utilises a mixture of forensic science, psychology, and psychiatry to reconstruct the crime and define the offender's profile. The method consists of four steps, starting from the Equivocal Forensic analysis, which aims to establish the most likely interpretation of a collection of documents related to a crime scene. Forensic Victimology involves the study of the victim's psychological characteristics. Crime scene analysis is the assessment of a crime scene to derive traits defining the offender's behaviour and, ultimately, to define the criminal's personality or components that may aid in identification (Turvey, 2012c).
Rogers (2003) criticised BEA for its application difficulties, citing that its field necessitates a broad spectrum of forensic scientific skills, including crime scene investigation, criminology, and psychology, while Nikodym (2005) characterises BEA's nature intuitive.

### ***LRAT (Lifestyle Routine Activity Theory)***

In contrast to the theories above, which focus on the offender's role, victimology seeks to understand why someone becomes a victim. As a significant victimology representative, Lifestyle Routine Activity Theory attempts to define criminal actions in terms of the common actions of offenders and victims by combining environmental crime theories and the Routine Activity Theory by Clarke and Felson (1979). Their theory suggested that a criminal event requires three variables to coincide. These variables were a motivated offender, a suitable target and an absence of guardians. LRAT's contribution to cybercrime is significant by pointing out that victim's lifestyle and online exposure are directly related to cybercrime risk. Additionally, guardianship's role underlines the importance of technical countermeasures and the legislation's foresightedness (Jahankhani & Al-Nemrat, 2011).

## B. Modus Operandi – Signature - Motivation

**Modus Operandi**, the method or the way that perpetrator uses for his/her purpose, is a vital aspect of the profiling sector both for digital and the physical world crimes; hence it possesses a prominent place in the examined literature. Rogers (2016) claims that MO is linked to the possibility of success and that it should not be viewed statically in many circumstances since the offender may gain expertise and, as a result, develop his approach over time. In the same fashion, Casey (2012) contends that sometimes when criminals use computer automation to commit a crime, it may be difficult to discern between automated processes and offender behaviour. Another critical element reinforcing the preceding MO constraint is that the offender may purposefully change his manner if he believes his acts have been discovered.

According to Turvey (2012a), the **Signature** is associated with activities made by an offender that are not necessary to commit the crime but rather show psychological or emotional qualities. Unlike MO, the Signature is less dynamic and unique; hence it could be proved crucial in the profiling process. In order to recognise a cybercriminal signature, the analyst may look for patterns such as parameter names, command choices, folder names, hidden messages to system administrators, nicknames and similar attributes to extract his/her relevant inferences (Donato, 2021).

Most sources define **motivation** as a component that explains why an attacker committed the crime, and it is considered an essential factor, particularly when evidence is limited or ambiguous (Casey, 2012). Although the motivation element is acknowledged and addressed in most papers, there is a paucity of evidence on theories and approaches that indicate how motivation connects to certain criminal qualities or practices. In contrast to external offenders, internal offenders are subjected to a more analytical view of motivation and different typologies. Shaw and Fischer (2005) highlight the work disgruntlement as the insiders' primary motive for abusive online behaviour. This fact contradicts Verizon's (2019) report, which identifies monetary gain as the most common motivation of cyber offenders for both insiders and external actors.

## C. Cybercrime Groups

Leukfeldt et al. (2017), in their paper, proposed a taxonomy of cybercriminal phishing and banking malware groups based on a review of 18 Dutch police investigations by correlating tech capacity level and geographic distribution to set the relevant conclusions. In every case, distinct group roles were identified, specifically; 'core members, professional enablers, recruited enablers, and money mules'.

In his hybrid model, Warikoo (2014) also uses the skill level as an indicator combined with the attack's methodology and severity, motivation level and structure to describe five discrete cybercriminal teams. Novice Hacktivists, Cyber Criminals, Cyber Crime Syndicates, Cyber Spies and Cyber Terrorists

Broadhurst et al. (2014), based on Gabinsky's FBI report (Chabinsky, 2010), recognised ten different criminal group profiles and compared some real cases in order to assess the validity of these types. Their typology, like Leukfeldt's, contained money mules, but it was more work role-oriented (i.e. Coders, Distributors, Technicians, Fraud specialists). Finally, both papers describe management and recruiting roles denoting the organisational similarity with the non-criminal businesses.

## D. Insider attack profiling

This review discovered a sizable number of studies regarding the internal perpetrators. Given the importance of insider attacks' impact on businesses of all sizes today, this topic could constitute a distinct area of research. Some papers focus on prediction (Magklaras & Furnell, 2001; Kandias et al., 2011; Schultz, 2002), some others on detection or post hoc analysis (Shaw & Fischer, 2005), while the majority uses psychological and behavioural models theories (Maasberg et al., 2015; Nurse, J.R.C et al., 2015). Regardless of the approach,  technical/digital means were used to monitor employees' behavioural patterns to conclude and suggest countermeasures.

## E. Modern tools - techniques

In Colombini and Colella's (2011) paper, users were profiled using digital forensics and data mining approaches based on their electronic devices. The authors created a theoretical method for generating a person's device usage profile and connecting it across devices to predict and prevent criminal occurrences. This was the only document found to have been created in collaboration with the army.

Honeypots, honeynets, IDS (Intrusion Detection Systems), and firewall logs have been used to collect evidence about hackers and patterns of digital crime (Kwan et al., 2008; Odemis et al., 2022; Donato, 2021) and used for statistical correlation and conclusion, combining psychology, behavioural analysis, and information technology

## Conclusion

Cybercriminal profiling appears to be an interdisciplinary endeavour, drawing on theories and methodologies from psychology, sociology, criminology, information security, and forensics. This feature may account for the heterogeneity and complexity of models and approaches; hence, it appears to be a conundrum whether an information technology professional should master behavioural and psychological sciences or the opposite.

The exponential digital evolution, the inherent volatility and complexity of cybercrime, seems to stress more tech-oriented approaches and techniques. On the other hand, the fundamental principles of human behaviour and psychology should remain the centre of every effort, even when the crime scene changes form.

Another issue discovered primarily in studies of cybercriminal groups is the disparate legal systems among the countries where offenders commit crimes. Although some countries have made significant steps to restrict digital crime and adjust their legislations accordingly, further efforts need to be made in a more collective and international framework.

Finally, in studies that focus on insider offenders, there is an evident usage of network and endpoint monitoring in the modern workplace. Although this fact constitutes an efficient and reasonable strategy against cybercrime, it raises serious ethical and privacy concerns. The equilibrium between accepted and abusive usage is expected to be a challenging topic.

## References

Bada, M. & Nurse, J.R.C. (2021) Profiling the Cybercriminal: A Systematic Review of Research. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2021*. Available from: https://doi.org/10.1109/CyberSA52016.2021.9478246.

Broadhurst, R., Grabosky, P., Alazab, M. & Chon, S. (2014) Organisations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, 8(1), pp.1–20.

Canter, D. & Youngs, D. (2005) *Beyond' Offender Profiling': The Need for an Investigative Psychology* . Available from: https://doi.org/10.1002/0470013397.ch7.

Casey, E. (2012) *Cyberpatterns: Criminal behavior on the internet*. Fourth Edi. Elsevier Ltd. Available from: https://doi.org/10.1016/B978-0-12-385243-4.00015-0.

Cohen, L.E. & Felson, M.(1979) Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), pp.588–608. Available from: https://doi.org/10.2307/2094589.

Colombini, C. & Colella, A. (2011) Digital profiling: A computer forensics approach. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6908 LNCS, pp.330–343. Available from: https://doi.org/10.1007/978-3-642-23300-5_26.

Donato L. (2021), 'Computer Criminal Profiling' PhD thesis, De Montfort University, Leicester

European Commission. Convention on cybercrime (2007). Available from: https://eurlex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14560 [Accessed 28 February 2022)

Chabinsky, S. (2010) *The Cyber Threat: Who's Doing What to Whom?* Available from: https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom [Accessed 5 March 2022].

Jahankhani, H. & Al-Nemrat, A. (2011) Cybercrime profiling and trend analysis. *Advanced Information and Knowledge Processing*, (9781447121398), pp.181–197. Available from: https://doi.org/10.1007/978-1-4471-2140-4_12.

Kandias, M., Stavrou, V., Bozovic, N. & Gritzalis, D. (2013) Proactive insider threat detection through social media: the YouTube case. *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society* Available from: https://doi.org/10.1145/2517840.2517865.

Kwan, L., Ray, P. & Stephens, G. (2008) Towards a methodology for profiling cyber criminals. *Proceedings of the Annual Hawaii International Conference on System Sciences*, (2004), pp.1–9. Available from: https://doi.org/10.1109/HICSS.2008.460.

Leukfeldt, E.R., Kleemans, E.R. & Stol, WP (2017) A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change*, 67(1), pp.21–37. Available from: https://doi.org/10.1007/s10611-016-9662-2.

Maasberg, M., Warren, J. & Beebe, N.L. (2015) The dark side of the insider: Detecting the insider threat through examination of dark triad personality traits. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2015-March, pp.3518–3526. Available from: https://doi.org/10.1109/HICSS.2015.423.

Magklaras, G.B. & Furnell, S.M. (2001) Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers and security*, 21(1), pp.62–73. Available from: https://doi.org/10.1016/S0167-4048(02)00109-8.

Morgan, S. (2021) 2021 Report: Cyberwarfare In The C-Suite. *Cybercrime Facts and Statistics* , pp.1–19. Available from: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf.

Nurse, J.R.C., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G.R.T. & Whitty, M. (2014) Understanding insider threat: A framework for characterising attacks. *Proceedings - IEEE Symposium on Security and Privacy*, 2014-January, pp.214–228. Available from: https://doi.org/10.1109/SPW.2014.38.

Nykodym, N., Taylor, R. & Vilela, J. (2005) Criminal profiling and insider cyber crime. *Computer Law and Security Report*, 21(5), pp.408–414. Available from: https://doi.org/10.1016/j.clsr.2005.07.001.

Odemis, M., Yucel, C. & Koltuksuz, A. (2022) Detecting User Behavior in Cyber Threat Intelligence : Development of Honeypsy System. 2022.

Rogers, M. (2003) The role of criminal profiling in the computer forensics process. *Computers & security*, 22(4), pp.292–298. Available from: https://doi.org/https://doi.org/10.1016/S0167-4048(03)00405-X.

Rogers, M.K. (2016) *Psychological profiling as an investigative tool for digital forensics*. Elsevier Inc. Available from: https://doi.org/10.1016/B978-0-12-804526-8.00003-4.

Rogers, M. & Seigfried-Spellar, K. (2014) Using Internet Artifacts to Profile a Child Pornography Suspect. *Journal of Digital Forensics, Security and Law*. Available from: https://doi.org/10.15394/jdfsl.2014.1163.

Schultz, E.E. (2002) Predicting insider attacks. *Computers & security*, 21(6), pp.526–531.

Shaw, E.D. & Fischer, L.F. (2005) Ten Tales of Betrayal : The Threat to Corporate Infrastructures by Information Technology Insiders Analysis and Observations. *Pers-Tr-05-13*, (September), p.66. Available from: http://www.dhra.mil/perserec/reports/tr05-13.pdf.

Steel, C. (2014) Idiographic Digital Profiling: Behavioral Analysis Based On Digital Forensics. *Journal of Digital Forensics, Security and Law*, 9(1). Available from: https://doi.org/10.15394/jdfsl.2014.1160.

Turvey, B.E. & Freeman, J. (2012a) Chapter 14 – 'Case Linkage: Offender Modus Operandi and Signature'. In: *Criminal Profiling An Introduction to Behavioral Evidence Analysis.* (Fourth Ed). Turvey, San Diego: Academic Press, pp.331–360.

Turvey, B.E. & Freeman, J. (2012b) Chapter 3 – 'Alternative Methods of Criminal profiling'. In: *Criminal Profiling An Introduction to Behavioral Evidence Analysis.* (Fourth Ed). Turvey, San Diego: Academic Press, pp.67–99.

Turvey, B.E. & Freeman, J. (2012c) Chapter 5 – 'An Introduction to Behavioral Evidence Analysis '. In: *Criminal Profiling An Introduction to Behavioral Evidence Analysis.* (Fourth Ed). Turvey, San Diego: Academic Press, pp.121–140.

Warikoo, A. (2014) Proposed Methodology for Cyber Criminal Profiling. *Information Security Journal*, 23(May 2015), pp.172–178. Available from: https://doi.org/10.1080/19393555.2014.931491.

Verizon (2019) 2019 Insider Threat Report. Available from: https://www.verizon.com/business/resources/reports/insider-threat-report/ [Accessed 8 March 2022].