Cybercrime Offender Profiles: Psychological Characteristics of Hackers and Online Predators

Shradha Verma[1]

[1]*Department of Forensic Science, MATS UNIVERSITY, Aarang(C.G.)INDIA.*
shradhaverma1242004@gmail.com

Abstract

In rapid-changing digital world, cybercrime has grown into a worldwide danger that ignores borders, cultures, or laws. Because people now rely heavily on linked systems, getting insight into what drives hackers mentally is a key to building smarter defenses, responses, and probes. The research looks at the mindsets and actions of two major types of digital criminals - hackers and online predators - who create different but just as risky issues for safety and fairness online.

Looking at findings from cyber psychology, crime studies, and behavior analysis, this study explores the mindset, drives, and warped thinking behind hacker actions. Smart, tech-savvy individuals who crave learning or proving their skills tend to get involved in hacking - not just for gain but for personal satisfaction. Still, some also show troubling signs like ego-driven attitudes, isolation, lack of concern for others, along with ways of thinking that make breaking rules seem acceptable - framing breaches as clever stunts or defiance against systems. On another side, people who target victims online usually act out of control urges, deception, and cold-heartedness; they carefully build false trust to take advantage of emotional weaknesses. These actions come with twisted reasoning, a need to dominate, trouble managing feelings, made worse because hiding online makes it easier to ignore consequences.

The research combines mind analysis with computer evidence techniques, showing how criminal types might guide sharper investigations, quicker threat spotting, or better danger forecasts. Instead of just reacting, police could predict actions by studying online behavior - like word choices, messaging styles, or tech footprints. On top of that, digging into what drives hackers may shape recovery plans, focusing on personal therapy and responsible internet training rather than one-size-fits-all fixes.

Keywords: - Cybercrime, Psychological Profiling, Hackers, Online Predators, Cyber psychology, Forensic Science

1. Introduction

Cyber Crimes constitute a novel category of offenses that are steadily growing in number because of the widespread use of Internet and IT services. Computer crime has reached the top of the list as one of the fastest-growing illegal activities around the globe. The Internet connects people in a way that has never been done before; at the same time, it also offers criminals the never-ending opportunity to take advantage of those who are weak. [1] With the advent of technology, the illegal activities are also constantly changing.[2] Computer crimes include criminal activities carried out using computers that further perpetrate crimes such as phishing, counterfeiting, cyber-bullying, pornography, bombardment of e-mails, spam, sale of illegal

D. R. Reddy et al. (eds.), *Proceedings of the First International Conference on Advances in Forensics and Cyber Technologies (ICFACT 2025)*, Advances in Computer Science Research 127,
https://doi.org/10.2991/978-94-6239-610-4_8

articles, etc.[3] The internet predators, who are also referred to as online predators, are those individuals who take advantage of the weaknesses of the youth, taking grooming, manipulating, and finally sexually exploiting the victims as the main goals of their actions. They are very good at getting along with young people and using their innocence, trust, empathy and the need for approval to their advantage. These types of people use different online platforms such as social media, instant messaging, chat rooms, etc. to reach out to their victims, and they usually pretend to be friends or understanding people.[4] The practice and implementation of psychological profiling are core to the world of cyber security mostly pertaining to the understanding and handling of behaviors and motivations of cyber criminals.[5] The surge in cyber-crime activities has left the crime investigation agencies perplexed as the criminals behind such activities always invent or utilize sophisticated and unusual means to carry out the cyber-criminal acts. There is a huge gap between the methods used in the traditional crimes and the new age crimes that are technology-driven.[2] Over the past decades, the online behavior has been analyzed through a variety of academic and applied scientific research areas to various extents, among which are communication science, anthropology, economics, psychology, computer science, law, education, medicine, neuro-science, philosophy, linguistics, marketing, politics, sociology, big data and data mining studies, ethics, etc. The list is by no means exhaustive.[35] One of the problem areas in Cyberpsychology is the psychology of human behavior online. This behavior predominantly consists of interaction, cognition, and entertainment (not only playing video games but also listening to music, downloading and watching movies, etc.) which are the main activities in cyberspace, in addition to online shopping, web surfing, using sex/porno applications, and working online. The area of human online behavior is very widely recognized as a major issue and it is even the case that almost everywhere around the world, in every household, people acknowledge its importance and relevance; consequently, the views and opinions expressed by psychologists become topic number one for lively debates. There are billions of IT users and thus researchers can easily find representative samples of the participants for their studies; the concepts of informed consent and the current ethical issues related to the use of the cyberspace are being discussed very thoroughly.[35,41]

2. Materials and Method

2.1Research Approach

The narrative qualitative research method was applied in this review with the aim of combining and then interpreting already existing literature about the psychological traits, the behavioral patterns and the motivational drivers of cybercrime offenders, particularly hackers and online predators. The narrative's method is to offers opportunity for engaging different theoretical viewpoints and empirical results coming from different disciplines such as forensic psychology, criminology, behavioral science, and cybersecurity. With this method, it is possible to have a complete picture of how cognitive, emotional, and situational factors play a role in online criminal behavior.

2.2 Literature Sources

For a strong and trustworthy knowledge base, the relevant studies were collected from high-quality academic platforms like Google Scholar, Research Gate, PubMed, IEEE Xplore, SpringerLink, and Elsevier, ScienceDirect. The databases were chosen based on the fact that they would offer a wide range of peer-reviewed articles, academic books on cyberpsychology and digital criminology subjects. Besides, cybersecurity white papers, government-published

cybercrime reports, and digital forensics manuals were included in the review as additional supporting materials in order to capture real-world insights and broader policy perspectives. This multi-source strategy were not only brought together from the different perspectives of academia and practice but also ensured that the review was of a high scholarly standard and had practical relevance.

2.3 Search Procedure

The literature identification process was via a systematic approach to the literature search using selected keywords and Boolean operators. Included keywords were “cybercrime psychology,” “hacker behaviour,” “cyber-offender profiling,” “online predators,” “cyberpsychology,” “digital grooming tactics,” “motivations of hackers,” and “cybercriminal personality traits.” Boolean combinations were utilized to fine-tune search results and ascertain accuracy. Paper publications between the years 2000-2024 were taken into account to cover the basic research and the latest progress. The search was iterative, which means that further keywords and related studies were added as new themes and patterns were noticed during the analysis.

2.4 Inclusion Criteria

The selection of studies was based on their academic credibility, methodological quality, and relevance to cyber offender's psychology. The sources accepted for inclusion consisted of peer-reviewed journal articles, academic books, government and law enforcement reports, cybersecurity agency publications, and conference papers. Research that offered empirical evidence, psychological theories, behavioural models, or offender profiling data was given priority. Both qualitative and quantitative studies were taken into account to guarantee the coverage of diverse methodological approaches.

2.5 Exclusion Criteria

Non-academic and untrustworthy sources were discarded in order to keep scientific rigor. These may included opinion-based articles, unverified online blogs, popular media content. Studies that dont provide a clear methodological explanation, offered outdated perspectives, or were insufficiently relevant to the psychological aspects of cyber offending were also left out. This filtering guaranteed that only credible and high-quality sources were contributing to the final analysis.

3. Results

3.1 Psychological Behaviour of Cyber Crime Offenders

The main reason why online behavior research has advanced as a multidisciplinary field is that the development is keeping pace with a rapid advancement in computer and web technology very closely.[35]A very complex profile of cybercriminals, showing features like tech-savvy, well-connected, vengeful, focused on goals, greedy, astute, risk-takers, opportunists, rule-breakers, fearless, unemotional, and adventurous was presented by researchers and practitioners. [5-12] The research proposed that the attackers could be redirected from the

crucial assets by presenting to them low-risk, low-reward targets through proper use of algorithms based on cyberpsychology studies.[5]

Psychological profiling, which is based on behavioral analysis and psychological theory, is meant to reveal the patterns and traits that are associated with the bad intentions in the cyber world. The usage of this method takes into consideration the very factors of human behavior that are most difficult to assess, namely language, decision-making and emotions, to identify the psychological types of the malware authors. [5,13-22]. There are always very big differences in behaviour between what people typically do off-line and in cyberspace.[34] Reasonable blame toward the mid-90s sets the precedent of what we now refer to as internet addiction disorder.[35,36] The 21st century has been characterized by the increased attention to social issues like economics, politics, and power in the studies [35,37-38], and this has also been the case with the Presence related research as well as the quick adoption of virtual and augmented reality systems that started around 1990s and have since then significantly increased.[35,39-40] It cannot be anticipated that all the studies on online behavior will soon be clustered and integrated into one specific research field, for then this field would embrace many scientific disciplines.[35]

Anonymity can be interpreted as a double-edged sword when it comes to online interactions resulting in different kinds of activities such as risk-taking, criminal acts, and sharing of person-to-person data along with the proliferation of many and alternative online identities—having multiple online identities can sometimes lead to dissociative disorders. If we consider the case of criminals, they can take on different faces or rather they recently have been hacking the credit cards (such as carders, crackers, distributors of viruses), trolling, and supporting/advocating hate speech while being anonymous at the same time. On the positive side, anonymity encourages online support and favor, volunteer work, caregiving and charity; after all, lurkers may attain competence and/or confidence and stop being 'invisible.' Legislators, ethicists, educators, celebrity bloggers, psychiatrists, security experts have a common ground in taking advantages and disadvantages of the anonymity factor.[35]

Hybrid behavior refers to the mix/augmentation of online and offline multitasking work, such as using avatars for real-life affairs, asking Siri/alexa for advice, having conversations with chatbots, breaking real-life rules, and ignoring possible danger just to take and post selfies online. A lot of individuals are already feeling the pressure of being involved in hidden web communities and of wearing some kind of a badge that signifies their hobby groups.[35]

The behaviors classified as coming from cyber criminals—partly identified by taking chances, wanting to be anonymous, being uninter emotionally, and showing confidence with technology—point out that these people's actions are not unplanned but rather influenced by some strong psychological reasons. In order to grasp the whole picture of why people committing crimes act in such a manner it is required to unravel their mental characteristics, personal backgrounds, and the reasons for their acts. Thus, the following part discusses the psychology and the inherent traits which pave the way of becoming a computer crime perpetrator.

3.2 Mindset and Background of Cyber Offenders

By way of further elaboration on the evolving understanding of cybercriminal behavior, the very importance of intelligence, personality traits, and social skills was; indeed, pointed out as being, among others, the most critical factors in the success of cyber attacks. Also, the research made it known that one of the very important factors that contribute to the behavior of hackers is the environmental factors, which include family relationships and educational background.[5] Certain research that relied on self-report surveys declared that hackers identify themselves with the labels "loners", "psycho-sexual perverts", "under-achievers", "socially inept", and "the offspring of dysfunctional families".[23-26] They are very much like intellectual pupils, bright, quick to grasp, determined, and self-aware, they take risks and at the same time, they do not respect the weaklings, perhaps they have different moral values and hold a mix of world citizen and patriot viewpoints, they are such bad talkers and so argumentative, and on the one hand, they are very much focused on internet-related matters and on the other, they have to a great extent strong interests in real life.[23] Motivations for using hacking combine at seeking revenge, ideology, adventure, thrill, subsistence, gaining notoriety, amusement, and financial gain.[30-33]

The above-mentioned personality traits, mental skills, and motivations directly affect the way cyber criminals conduct their business. The offenders' skills in technology, inquisitiveness, and wish for either control or anonymity are the determining factors for their digital tools and platforms. Thus, it is a psychological understanding of cyber criminals that is held through the knowledge of their specific tools. The subsequent part will outline the key technological resources misused by such people.

3.3 Tools used by the Cyber Crime Offenders

Different cyber criminals use dissimilar tools and techniques in their activities.[28-29]

- Dark net : Being a criminal trial involving black-marketing through the dark net by the sale and purchase of drugs and similar banned things.[2]
- Social media: To attract and entice teenagers and young adults through concern, trust, or some other way.
- Cloud computing: Criminal activity, in response, necessitates various tactics to obscure the criminals' identities, to avoid monitoring and remote detection of them, and to get rid of or repudiate the evidence.
- AI generative platforms: The user generate extremely explicit images of teenage and young adult models in order to exploit them.

The offenders' technological tools and platforms comprise the basis for the different crimes carried out in the virtual world. A specific tool—like the dark net, social networks, cloud computing, or AI-based generators—allows particular forms of abuse to take place, depending on the criminal's motive and expertise. As a result, recognizing these tools inevitably brings about a comprehension of the larger groups of cyber crimes that come into being through their wrong use. The following part thus gives a description of the most important kinds of cybercrimes that get support from these digital means.

3.4 Types of Crimes Happened in Cyber World

- Virus attacks: Well, a virus is software capable of infecting other software and producing its own copies, then moving to a different program. Usually, the viruses affect the computer's data by changing or removing them.
- Spyware : a program that secretly monitors and logs all user activities.
- Software piracy: Software piracy means the infringement of the law, which involves the copying of original software without permission or the concealing and distribution of products that are intended to be the originals. Along with these crimes, copyright infringement, trademark infringement, stealing of computer source code, patent infringements, etc. are also part of the criminals' activities.
- Salami attacks: The attacks of this nature are mostly oriented toward the financial crimes. The idea is to make the changes so trivial that, in one case, it would be entirely unnoticed. To give an example: if an employee working on the bank's server implants a program that deducts a minute sum from each client's account.
- Pornography: Pornography refers to the practice of displaying sexual activities for the purpose of sexual arousal to the internet user. The term also covers such things as pornographic websites, computer-generated pornographic magazines, and Internet pornography offered via mobile phones.
- Child pornography: Child pornography involves acts of pedophiles who, after sharing pornographic images, attempt to meet the children for sexual purposes, including taking nude photos and putting them in sexual positions. Kids are sexually abused by pedophiles who resort to this practice and even record the act to sell the kids' pictures on the Internet.
- Cyber bullying: Cyberbullying is defined as the repeated use of Internet services by the cyber-criminal to harass or threaten the victim.
- Denial of Service attack(DoS): In this type of attack, the offender either overwhelms the network bandwidth of the victim or fills his email with spam such that the victim is unable to access or provide the services he is entitled to.[3]

The classification of cyber crimes offers the precise depiction of the various types of offenses that can occur while, on the other hand, it is very essential to look into the practical ways through which the criminals commit the crimes. Cybercriminals depend on many tactics such as deceit, impersonation, malware usage, and social engineering to realize their aspirations. Knowing these working methods not only uncovers the offenders' psychological traits but also connects them with their actual activities in the virtual world. Hence, the next part describes the general techniques that are often resorted to by cyber criminals.

3.5 Methods used by Cyber Criminals

Hackers were in constant communication with their colleagues in cyberspace and exchanged priceless resources, information, and methods with other groups.[27] Besides, they usually steer clear of sexually explicit materials, and many hacker groups are involved in political actions in a positive way. Therefore, it should be expected that separate hacker boards, chat channels, and so on would be created. Hackers having different drives: the challenge, triumph, and a thirst for knowledge as pure intellectual gratification for the ones on the positive side;

however, the negative side consisted of revenge, sabotage, and theft which also contributed to some hackers' activities.[23,26] Advertising cars for sale on different virtual platforms at lower than market rates results in a good deal. FBI Impersonation these scams.

- E-mail Scam: in their efforts to steal money, fraudsters have exploited court officials through spam attacks.
- Extortion Scams: Intimidation and extortion scams have developed through time to surround scams such as Telephone Calls, Process server, Payday loan, the Grandparent Scam, Hit-man scam.
- Scareware/Ransomware: Extorting money from consumers by intimidating them with false claims pretending to be the federal government watching their Internet use and other intimidation tactics have evolved over the years and included such as Pop-up Scareware Scheme, Citadel Malware, IC3 Ransomware, etc.[1]

Hackers create and/or utilize existing computer software applications to carry out attacks on the targeted system. These malicious individuals have the intention of ruining the system and getting the thrill out of that entire process. Furthermore, there are hackers who trade in personal financial losses, for instance, taking credit card data, conducting illegal transfers of money from various bank accounts to their account, and then taking the cash out.[3]

4. Discussion

4.1 Challenges

Although there are improvements in behavioral profiling and cyber forensics, there are still many challenges that hinder the effective identification and mitigation of cybercrime. The internet's global reach and nature, along with the anonymity, it offers enable criminals to carry out their activities with a high degree of freedom and low risk of getting caught, which makes it more harder for the police to act. The fast-paced technological developments, such as AI-generated content, deepfakes, encrypted communication, and cloud-based tools, continuously make new threats that need constant so.

Adaptation therefore has to be at the forefront of all counter measures taken. On top of that, there is still no common ground for psychological profiling of cybercriminals as the bulk of the models are based on traditional criminal psychology and can therefore only be partially effective at understanding and predicting digital behavior. The barriers to research and intervention that arise from limited access to actual offender data, ethical constraints on performing studies on live offenders, and the underreporting of online crimes, particularly those classified under sexual exploitation and financial fraud, are particularly significant.

4.2 Limitations

At present, the study of accentuation the psychology of cybercriminals is severely restricted due to methodological limitations. A lot of research works depend on self-reported questionnaires, very few participants or external data, which can probably bias the results or not represent the whole cyber offenders population. The distinctions in culture and location are usually ignored, thus, the findings lose their applicability across different societies and

contexts. Besides, the existing criminological theories do not seem to support very well the distinctive behavior of people in cyberspace and therefore, cannot be used. No doubt the longitudinal studies that could eventually uncover the changes in motivations and techniques are still very few in number, thus, the understanding of the evolution of cybercriminal behavior remains greatly lacking.

4.3 Future scopes

Research in the upcoming time should take integrated, technology-oriented ways that merge psychological insights with digital forensics. AI-based tools can improve the behavioral profiling by examining the linguistic clues, decision-making patterns, and digital footprints of individuals to find out if they are behaving suspiciously. The studies carried out in different cultures will be beneficial in recognizing the different ways in which social, economic, and environmental factors affect cybercrime regions. Neuroscience and cognitive psychology can disclose more about the personality traits of sinners such as their tendency for impulsiveness, power of the reward, emotional control, and moral reasoning. Moreover, the use of longitudinal studies, prevention strategies, early detection frameworks, and customized rehabilitation programs might be very effective in terms of strengthening the cybersecurity measures and influencing the policymaking process.

4.4 Implications for Cybersecurity and Forensics

The comprehension of psychological traits and the manner of conduct of cybercriminals is a factor that directly contributes to the improvement of the infrastructures of cybersecurity and the practices of forensic investigations. The offender profiling can map out the foundations of proactive threat detection systems, give information about risk assessment strategies, and support law enforcement agencies in resource allocation based on priorities. Moreover, these observations can stimulate the lawmakers in not only coming up with but also in enforcing more effective regulations and precautionary measures that would harmonically regulate the technological creativity and security requirements.

4.5 Ethical Considerations

The studying and keeping track of cybercriminal behavior is an aspect that is surrounded by difficult ethical dilemmas. The researchers are in a situation where they have to find a way to reconcile the rights of individuals to have their privacy respected with the necessity for monitoring and intervention, thereby making sure that the practices of profiling and data collection do not violate the rights of individuals. There should be ethical standards that will steer the studies that include real wrongdoers or vulnerable groups such as minors, in order to prevent any harm. Besides, the providers of online platforms and the developers of technology are viewed as being accountable for the prevention of exploitation as well as the promotion of secure and friendly digital environments. This signifies that there are broad social and moral responsibilities related to cybersecurity.

5. Conclusion

The hunting ground of cyber criminals has become vast and global, with the digital technology, the internet, and other electronic means they use being the main creators and enhancers of their

criminal activity. Cyber criminals' psychological profile discloses that they are not one type of a group—there are different and sometimes opposing reasons, skills, and ways of behaving within them. Their criminal proclivities are determined by intelligence, personality, the environment, and interaction in online communities. The cyber criminals, including hackers, online sexual abusers, and others, usually take advantage of the digital distance, skills in technology, and psychological tactics to approach the targets that are least likely to resist, particularly children and teenagers. The authors of the paper have pointed out that the cybercrime such as malware infections, financial scams, identity theft, and online child abuse is being carried out by criminals using a sophisticated combination of tools such as, among others, the dark web, social engineering, and the use of cloud technology and AI-created deception. Moreover, the criminals are constantly revising their approaches which makes it harder for the police to catch and prevent them. This situation of vibrant cyber crime events makes it necessary to develop more powerful psychological profiling, early detection systems, and specific interventions. In sum, knowledge of cybercriminals' mind, drives, and morals is a must for the building of working cybersecurity policies, preventive plans, and investigative methods. A multidisciplinary model, involving the collaboration of psychologists, technologists, criminologists, and law enforcement, is the way to go in order to lessen the risk of cyber attacks and safeguard the people in a world growing ever more digital.

Acknowledgement: - The author wishes to thank the conference organizer and mentors for their guidance and support.

Conflict of Interest: - The author declares no conflict of interest

References:

1. Mittal, S., & Singh, A. (2019). A Study of Cyber Crime and Perpetration of Cyber Crime in India. In Cyber Law, Privacy, and Security (pp. 1080–1096). IGI Global. https://www.researchgate.net/publication/332998138_A_Study_of_Cyber_Crime_and_Perpetration_of_Cyber_Crime_in_India.
2. Nagarathna, A., &Sachidananda, K. (2021). *Cyber crime profiling: Quintessential need for cyber-offender detection in India*. Rostrum's Law Review, VI(1). https://www.rostrumlegal.com/cyber-crime-profiling-quintessential-need-for-cyber-offender-detection-in-india
3. Khan, S. A. (2020). Cyber Crime in India: An Empirical Study. International Journal of Scientific & Engineering Research, 11(5), 690-694. https://www.researchgate.net/publication/369559590_Cyber_Crime_in_India_An_Empirical_Study
4. Okpokwasili, O. A., &Onwuatuegwu, I. N. (2023). Online predators: Protecting teenagers from Internet sexual exploitation. International Journal of Modern Science and Research Technology, 1(4), 41–51. https://ijmsrt.com/articles/view/online-predators-protecting-teenagers-from-internet-sexual-exploitation
5. Tshimula, J. M., Nkashama, D'Jeff K., Tshibangu Muabila, J., Galekwa, R. M., Kanda, H., Dialufuma, M. V., … Chikhaoui, B. (2024). *Psychological profiling in*

cybersecurity: A look at LLMs and psycholinguistic features (arXiv:2406.18783v2). arXiv. https://arxiv.org/html/2406.18783v2

6. J. McBrayer. 2014.*Exploiting the digital frontier: hacker typology and motivation*.The University of Alabama.
7. A. Palassis, C.P Speelman, and J.A. Pooley. 2021.An exploration of the psychological impact of hacking victimization.*Sage Open*, 11(4):21582440211061556.
8. R. Saroha. 2014.Profiling a cyber criminal.*International Journal of Information and Computation Technology*, 4(3):253–258.
9. H. Thackray, J. McAlaney, H. Dogan, J. Taylor, and C. Richardson. 2016.Social psychology: An under-used tool in cybersecurity.*BCS Human Computer Interaction Conference*.
10. X. Li. 2017.A review of motivations of illegal cyber activities.*Kriminologija & socijalna integracija: časopis za kriminologiju, penologiju i poremećaje u ponašanju*, 25(1):110–126.
11. G. Yang, L. Cai, A. Yu, J. Ma, D. Meng, and Y. Wu. 2018.Potential malicious insiders detection based on a comprehensive security psychological model.In *2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService)*, pages 9–16. IEEE.
12. T.J. Holt, M. Stonhouse, J. Freilich, and S.M. Chermak. 2021.Examining ideologically motivated cyberattacks performed by far-left groups.*Terrorism and political violence*, 33(3):527–548.
13. H. Thackray, J. McAlaney, H. Dogan, J. Taylor, and C. Richardson. 2016.Social psychology: An under-used tool in cybersecurity.*BCS Human Computer Interaction Conference*.
14. J. Jiang, J. Chen, K.K.R. Choo, K. Liu, C. Liu, M. Yu, and P. Mohapatra. 2018.Prediction and detection of malicious insiders' motivation based on sentiment profile on webpages and emails.In *2018 IEEE Military Communications Conference*, pages 1–6. IEEE.
15. A. Kipane. 2019.Meaning of profiling of cybercriminals in the security context.In *SHS Web of Conferences*, volume 68, page 01009. EDP Sciences.
16. U. Hani, O. Sohaib, K. Khan, A. Aleidi, and N. Islam. 2024.Psychological profiling of hackers via machine learning toward sustainable cybersecurity.*Frontiers in Computer Science*, 6:1381351.
17. S. Budimir, J.R.J. Fontaine, N.M.A. Huijts, A. Haans, G. Loukas, and E.B. Roesch. 2021.Emotional reactions to cybersecurity breach situations: scenario-based survey study.*Journal of medical Internet research*, 23(5):e24879.
18. M. Bada and J.R.C. Nurse. 2021.Profiling the cybercriminal: A systematic review of research.In *2021 international conference on cyber situational awareness, data analytics and assessment*, pages 1–8.
19. R. Montañez, E. Golob, and S. Xu. 2020.Human cognition through the lens of social engineering cyberattacks.*Frontiers in psychology*, 11:528099.
20. J. Gaia, B. Ramamurthy, G. Sanders, S. Sanders, S. Upadhyaya, X. Wang, and C. Yoo. 2020.Psychological profiling of hacking potential.In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.
21. P. Zambrano, J. Torres, L. Tello-Oquendo, Á. Yánez, and L. Velásquez. 2023.On the modeling of cyber-attacks associated with social engineering: A parental control prototype.*Journal of Information Security and Applications*, 75:103501.
22. K. Kioskli and N. Polemi. 2022.Estimating attackers' profiles results in more realistic vulnerability severity scores.In *13th International Conference on Applied Human Factors and Ergonomics (AHFE 2022)*.

23. Woo, H.-J. (2003). *The hacker mentality: Exploring the relationship between psychological variables and hacking activities* [Doctoral dissertation, University of Georgia]. University of Georgia OpenScholar. https://openscholar.uga.edu/record/6869?ln=en
24. Chantler, N. (1996). Profiles of a Computer hacker. Florida: Inforwar.
25. Post, J. (1996). The dangerous information system insider: Psychological perspectives.Retrieved April 3, 2003 from http://www.inforwar.com
26. Taylor, P. A. (1999). Hackers: Crime in the digital sublime. London: Routledge. The Center for the study of Technology and Society. (2001, March 16). Special Focus: Cyberwarfare. Retrievd March 08, 2001 from http://www.tecsoc.org/natsec/focuscyberwar.htm
27. Woo, H. J., Kim, Y. R., & Dominick, J. R. (2002). Hackers: Chauvinists or Anarchists-A content Analysis of Defaced Web Pages. presented at Communication and Technology division, International Communication Association, Seoul, Korea,July.
28. Lickiewicz, J. (2011). *Cyber crime psychology – proposal of an offender psychological profile.* Problems of Forensic Sciences, 87, 239–252. https://arch.ies.gov.pl/images/PDF/2011/vol_87/87_Lickiewicz.pdf.
29. McQuade S. C., Encyclopedia of cybercrime, Greenwood Press, London 2009.
30. Karam, L. (2016). *An Analytical Approach to Psychological Behavior of Hackers' Motives*. Academia.edu. https://www.academia.edu/download/77738580/An_Analytical_Approach_to_Psychological.pdf
31. Niharika1 & Ranjeet Kaur2. Honeypots For Network Surveillance. International Journal of Research in Engineering & Technology ISSN(E): 2321-8843; ISSN(P): 2347-4599 (2014)
32. Wiktionary. geek. [online] Available at: https://en.wiktionary.org/wiki/geek
33. Kennedy, F., Kennerley, H. and Pearson, D. (n.d.). Cognitive behavioural approaches to the understanding and treatment of dissociation.
34. Ancis, J. R. (2020). *The age of cyberpsychology: An overview*. *Technology, Mind, and Behavior,1(*1*)* https://www.researchgate.net/publication/345451549_The_age_of_cyberpsychology_An_overview
35. Wiederhold, B. K., Riva, G., Wiederhold, M. D., & Kirwan, G. (Eds.). (2016). *Annual Review of CyberTherapy and Telemedicine* (Vol. 14). Interactive Media Institute. https://interactivemediainstitute.com/wordpress/wp-content/uploads/2019/04/ARCTT-14.pdf
36. K.S. Young, Caught in the Net: How to Recognize the Signs of Internet Addiction – and a Winning Strategy for Recovery, Wiley & Sons, N.Y., 1998.
37. M. Castells, Communication Power, Oxford University Press, 2009.
38. E. Castronova, Synthetic Worlds. The Business and Culture of Online Games, The University of Chicago Press, Chicago and London, 2005.
39. M.M. North, S.M. North, J.R. Coble, Virtual Reality Therapy: An Innovative Paradigm, IPI Press, 1996.
40. M. Lombard, F. Biocca, J. Freeman, W. IJsselsteijn, R.J. Schaevitz (Eds.), Immersed in Media: Telepresence Theory, Measurement & Technology, Springer, Berlin, 2015.
41. E.A. Buchanan (ed.), Readings in Virtual Research Ethics, Infosci Publ., Hershey, PA, 2004