INTERNATIONAL JOURNAL OF SOCIAL SCIENCES BULLETIN
ISSN: (E) 3007-1917 (P) 3007-1909
Volume 4, Issue 2, 2026

PSYCHOLOGICAL PROFILING OF CYBERCRIMINALS IN PAKISTAN: A MEDIA AND LAW ENFORCEMENT PERSPECTIVE

Rabia Razzaq

Assistant Professor, Law College, Punjab University Lahore

razzaq.law@pu.edu.pk

Corresponding Author: *
Rabia Razzaq
DOI: https://doi.org/10.5281/zenodo.18831593

Received	Accepted	Published
29 December 2025	13 February 2026	28 February 2026

ABSTRACT

In Pakistan, cybercrime represents a major threat to individual citizens, organizations, and national security; there has been an unprecedented rise in digital technologies and social networking sites. As a result, researchers, journalists, and law enforcement agencies have become increasingly aware of the psychological aspect of cybercriminal behaviour. This research seeks to understand and document these psychological profiles from two different perspectives (i.e., the media's view and law enforcement's view) of cybercriminals within the country. In order to do so, this research has developed two research objectives: to identify the predominant psychological characteristics of cybercriminals and to consider how the media's and law enforcement's perceptions of cybercriminals differ. There are also two research questions that guide the research: (1) what are the types of psychological characteristics linked to cybercriminal activity? (2) What are the different institutional viewpoints on the process and application of criminal profiling? This research has developed two hypotheses that statistically tested via an examination of the correlation of psychological characteristics with cybercriminal behaviour and the correlation of one's institutional role to that of cybercriminal profiling. A survey design with quantitative research is being used to collect data from journalists and law enforcement personnel. Data is obtained through an instrument (questionnaire) being administered to those who are part of the target population/group for this research study. A total of 200 samples have been drawn from each target population using stratified sampling to ensure adequate representation from each group. The data analyzed using statistics. There tables and pie charts provided to allow for ease of interpretation and representation of results. The results of the study show that cybercriminals exhibit trait characteristics of impulsiveness, social isolation, narcissism, and technology competency. The research also found that there is a significant difference between how journalists and law enforcement view the motive of the cybercriminal and how accurately they profile the cybercriminal. Using statistical analysis of both hypotheses, there is strong evidence to support that there are important associations between the psychological traits and characteristics of a person and the pattern of behaviour associated with their engagement in cybercrime. This research indicates that developing psychological profilers for law enforcement training and for specific public awareness campaigns would improve the efficiency of investigations and increase the success rate of preventing cybercrime. The recommendations include: establishing a structured inter-agency cooperative efforts, developing a specific psychological training program for each agency, and developing a national framework for profiling cybercriminals in order to address the continuing and increasing damage caused by cybercrime in Pakistan.

Keywords: *Psychological Profiling, Cybercriminals, Media, Law, Enforcement Perspective*

Introduction

Pakistan's means of trade and communicating has changed rapidly due to the large amount of growth related to digital technologies, access to the internet, and use of social media. Sadly, alongside the growth in these areas has come a rise in cyber terrorism which includes hacking, fraud (online and off), identity theft, and digital harassment. Cybercrime is a threat to both the individual's privacy and economic stability, as well as to national security and institutional integrity. While the legal and technical responses to cybercrime have improved in Pakistan, little is known about the psychological characteristics and behaviour of cybercriminals. Psychologically profiling involves establishing a framework for analysing an individual's personality, motivation, and cognition related to criminal behaviour; additionally, there are media and law enforcement benefits to understanding these psychological aspects in order to develop prevention strategies, enhance investigation efficiency and improve public awareness of cybercrime. (Zhao, 2014)

This research utilises a quantitative survey methodology to collect data on media professionals and law enforcement officers' perceptions of psychological profile of cybercriminals in Pakistan.

Background of the Study

Cybercrime has transformed from an isolated, random act to a sophisticated, organized crime globally. As a result, law enforcement worldwide has recognized the relevance of criminal profiling and the application of behavioural analysis techniques during cyber investigations. By identifying the behavioral patterns of a person; their personality traits, emotions and motivations, one can build a psychological profile for that person to help define their characteristics of persons committing a crime. The Federal Investigation Agency (FIA) in Pakistan has improved their response to cybercrime through the establishment of specialty cybercrime units, as well as the introduction of cyber laws. (Vasquez, 2004)

However, the majority of the profiling activity being conducted by Pakistan's law enforcement agencies remains technical in nature rather than psychological. Also, the media helps shape public opinion of cybercriminals by framing how they are viewed in society. Media generally portrays cybercriminals as either having a strong ability with technology or as having an immoral character. (Smith, 2022)

While the number of cybercrime cases has continued to increase, limited empirical research has been conducted in Pakistan that combines psychological profiling with the law enforcement and institutional perspectives. Therefore, by examining the media's perspective of cybercriminal behaviour through law enforcement's perspective, a complete understanding attained on how cybercriminal behaviour is categorised and dealt with by the institutions involved. (Sheridan, 2002)

Problem Statement

The rise in frequency and complexity of cyber-crimes in Pakistan is on-going. However, current preventative and investigative measures still heavily lean on technological detection and enforcement of laws, while less so on psychological analysis. Law enforcement agencies are limited in their ability to identify the behavior patterns and motives behind cybercrime because there is no structured format for the psychological profiling of cybervacants. Differences between media and law enforcement in the perception of cybercriminals also create gaps between what the general public understands and how policymakers respond. (PECA, 2016)

In order to improve the effectiveness of profiling efforts, an empirical analysis of the psychological characteristics commonly attributed to cybercriminals reveal whether there are any substantial differences in institutional interpretation of these characteristics. Without such analysis, current profiling activities miss opportunities for improvement.

Research Gap

Most of the literature available in Pakistan currently focuses on legal reforms to address issues associated with cybersecurity and developing cyber-crime countermeasures through technology. There is limited research available examining the psychological dimensions of cybercriminal behaviours specific to the socio-cultural context of Pakistan. There

has also been very little comparative analysis conducted between the media and law enforcement's perspectives of cybercriminal behaviours and how they are perceived by each respective group. (Khan, 2022)

Many of the studies conducted thus far rely on qualitative analytical methodologies and case studies as opposed to conducting any quantitative empirical research. Based on this observation, it can be concluded that significant amounts of research pertaining to the psychological characteristics of cybercriminals, as well as evaluations of institutional perceptions regarding these behaviours in Pakistan, still exist. There is no doubt that this research study assist in addressing this gap by conducting quantitative survey methodology with 200 respondents to obtain empirical survey data.

Research Objectives

The purpose of this research study is twofold:

1. To identify the main psychological characteristics associated with cybercriminal behaviours within Pakistan; and
2. To compare and contrast the perceived psychological profile of cybercriminals between media representatives and law enforcement officers in Pakistan.

Research Questions

1. What are the psychological characteristics associated with cyber criminals in Pakistan?
2. Do the media and law enforcement agencies have different views of the psychological profiling of cyber criminals?

Hypotheses

- H_1: Psychological characteristics (e.g., impulsivity, narcissism, social withdrawal, and technological skill) bear a statistically significant relationship to behavior as a cyber-criminal.
- H_2: Media professionals and law enforcement personnel hold statistically significant differences in their perceptions of psychological profiling of cyber criminals.

Significance of the Study

This study has theoretical significance (to criminology and media studies) by integrating psychological profiling into the cybercrime research body of literature within the context of Pakistan; practical significance to law enforcement organisations by assisting them to improve their investigative strategies through behavioural analysis and profiling techniques; significant to media organisations as it provides insight into the responsible framing of media reports and the framing of cyber-crime; and finally at the policy level to develop a systematic national psychological profiling framework and develop a structured training programme for cybercrime units within the police.

Literature Review

FIA, under Prevention of Electronic Crimes Act 2016 (PECA), is authorized to investigate cyber-crimes (such as cyberstalking). Upon completion of its investigation, FIA submit a prosecution report to a special court which handles such cases, and PECA apply the Code of Criminal Procedure 1898 for a trial of all parties. Both parties can appeal against a decision of the court. The law protects victims and witnesses during the trial. PECA 2016 governs electronic communications to eliminate cyber-crimes (such as cyberstalking and cyber-harassment) and intends to eliminate them through regulations regarding the investigation/punishment of electronic crime. (Johnson, 2018)

It provides authorities the authority to investigate/punish these types of crimes while also establishing requirements for gathering, storing and using electronic evidence in a court of law.7.2.2. The Pakistan Penal Code is enacted in 1960 to deal with conventional offences. Although PECA was introduced later (2016) and is expressly intended for cybercrime only, it is common for both laws to be used together to prosecute those who violate cyberstalking laws in Pakistan. Stalking that violates PECA, including a variety of intimidation, harassment, and defamation are often prosecuted using relevant provisions of the PPC. Aside from the PPC and PECA, some other laws in Pakistan may also apply to cyberstalking, such as those relating to telecommunication, data protection and

privacy rights. Laws of this type also modify how cyberstalking offences are investigated and prosecuted. (PECA, 2016)

As of January of 2024, the total population of people using the Internet worldwide has reached approximately 5.35 billion; however, in 1995 there were just 16 million people using the Internet. The majority of this growth can be attributed to the emergence of the World Wide Web along with the explosion of the dot-com boom during the late 1990s. With the growth of Internet users comes an increase in global connectivity and with greater access to the internet there is a growing concern for protection of individual privacy and security relating to using the Internet, and it uses more advanced security methods today to ensure protection of personal data. (Fernandez, 2020)

Both Australia and Pakistan share similar experiences related to online harassment; however they do have some unique hurdles when dealing with prosecuting perpetrators of cyberstalking offences. There have been a number of previous studies that have documented the challenges and strategies associated with prosecuting the cyberstalking cases. For example, cyberstalking is reported as being one of the most common types of cybercrime, and, according to recent research, cyberstalking represents a range of illegal activities that occur using technology; including financial fraud and the hacking of websites (Dawn News, 2021). Over 80% of grievances submitted to the Australian Federal Police (AFP) and the Pakistani Federal Investigation Agency (FIA) fall under the umbrella of cyberstalking activity, with the overwhelming majority of victims being young women and reporting acts of extortion, harassment, or blackmail (Dawn News, 2021).

In Australia and Pakistan, there is an alarming lack of awareness of the law and the reporting process by the victims of cyberstalking (Dawn News, 2021).The sixth annual Cyber Harassment Helpline Report by DRF is published on May 18, 2023, containing data from a total of 14,376 reported cases over six years. In 2022 specifically, the helpline received on average 224 new cases per month, with November being the busiest month of the year (Digital Rights Foundation, 2023).

There is a wealth of research supporting the need for legal reforms that enhance the ability of prosecutors to enforce anti-cyberstalking laws. The legislative progress of both Pakistan and Australia recognizes the seriousness of cyberstalking and online harassment within today's digital age through the introduction of protective legislation. While both countries have made headway legally to provide citizen's protection against cyberstalking and online harassment, both continue to face challenges in their ability to fully enforce the laws or provide adequate assistance to victims. Pakistan enacted the Prevention of Electronic Crimes Act (PECA) as an update to their existing cybercrime laws in 2016 to address these issues. The Federal Investigation Agency (FIA) has been tasked with serving as the investigating agency for the PECA and is responsible for investigating cyberstalking under their specialized cybercrime division called the Cyber Crime Wing (CCW).

The CCW is established in 2007 to address and combat the abuse and misuse of technology within the country. General Musharraf as President of Pakistan enacted the Electronic Transactions Ordinance in 2002. PECA 2016 serves as the main law addressing cybercrime in Pakistan. Originally introduced to govern file management, statistics, communication & transaction activity, it expanded to include certifying bodies and certifying agents for e-transactions, as well as to govern all e-transactions that are authenticated using in-person, electronic, or other methods (e.g., Electronic Transactions Ordinance 2002).

Under PECA 2016, cyberstalking is defined as the intentional use of any information system, network, website, email, or other means of communication to intimidate, threaten, or sexually abuse another person (Prevention of Electronic Crimes Act 2016). In 2007, the CCW of the FIA was established to assist states to effectively investigate and prosecute cybercrimes in Pakistan. The CCW is initially established under PECA 2016 and has had responsibilities since its inception to address a broad range of cyber threats, included in these broader definitions of cyberstalking. CCW personnel, through their extensive training/education and unique set of skills, is ideally positioned to conduct complex cyber

investigations and to develop evidence of cyber-criminal activity (FIA, n.d.).

There are many different types of law available under the Australian system to address cyberbullying such as for example using a telephone or using the internet in an aggressive way, or stalking or threatening to harm someone or aiding someone in committing suicide or posting nude images of someone or anything else offensive on the internet. Despite the existence of these laws; however, Australia has been unable to gain a level of control over the increasing number of cybercrime incidents.

Theoretical Framework

The existing criminological and psychological theoretical framework serves as the basis for this research study in identifying and explaining deviant and criminal behavior in an online environment. These theories incorporate a behavioral, personality-based, and media framing perspective to develop an understanding of cybercriminal profiling in Pakistan.

1. Trait Theory of Criminal Behavior

Trait Theory proposes deviant behavior has its roots in stable psychological and biological traits inherent to people. Historically, Cesare Lombroso, one of the earliest criminologists, concluded that deviant behaviors are influenced by genetic characteristics inherent to the individual. More recently, trait theorists have pointed to personality characteristics such as impulsiveness, aggression, narcissism, and social isolation as influencing factors on an individual's likelihood of committing cybercrime.

Individuals exhibiting these traits are likely to engage in online criminal activity, including online fraud, hacking, and online harassment. Thus, Trait Theory provides a foundation for studying psychological traits that are the most common among individuals who commit cybercrime.

2. Social Learning Theory

Albert Bandura's Social Learning Theory is also important in understanding why someone may commit cybercrime. According to Bandura's Social Learning Theory, individuals learn how to behave by observing and imitating what they see and, to some degree, from reinforcement from the social environment where the behavior occurs.

In cyberspace, individuals may learn through forums, peer-to-peer networks and online communities how to commit acts of cybercrime. The theory also explains how individuals who are technologically competent and exposed to a deviant online subculture may find cybercrime to be normalised behaviour. Theory will also be used to explain differences an individual's social environment and social groups difference in information technology.

3. Routine Activity Theory

The Routine Activity Theory, a theory by Lawrence E. Cohen and Marcus Felson, suggests that crime occurs where there is a convergence of three elements: There must be a motivated offender, a suitable target, and there must also not be a capable guardian to watch over the crime before it takes place. When it comes to cyberspace, people with a motive and a predisposition to commit crime tend to exploit the weak monitoring systems (i.e., the lack of a capable guardian) of the digital world. This perspective supports the exploration of how psychological traits interact with technological opportunities to produce patterns of cybercrime in Pakistan.

4. Media Framing Theory

The Media Framing Theory illustrates how the media constructs narratives that shape the public's perception about crime. As a method of enhancing this narrative, the media presents cybercriminals in different. The result of this difference in viewpoint may create perceptual differences between the writer of the media outlet and the police department that further exacerbate these differences due to their institutional roles and orientations.

Using the Media Framing Theory as a guideline, the study able to review the differences of perception between the two institutional groups regarding psychological profiling and how they interpret motivation.

Conceptual Model of the Study

The conceptual model of the study is based on the following three constructs:

- Independent Variables: Psychological Traits (Impulsivity = lack of control + should not have access to technology; Narcissism = self-indulgent; Social Isolation = lack of social networks/relationships; Technological Proficiency = ability to use technology's performance).
- Dependent Variable: Cybercriminal Behavior Patterns (criminal behavior).
- Moderating Variable: The Role of the Institution (differences between the roles of the media professional versus the law enforcement officer).

It is assumed that psychological traits have a significant impact on cybercriminal behavior and that differences in institutional roles have an impact in how each of the groups perceives and interprets how each group uses psychological profiling techniques.

Research Methodology

Research Design

To conduct this research, a quantitative approach utilized and implemented via a survey methodology. The advantage of using a quantitative methodology is that relationships between psychological characteristics and cybercriminal behavior can be analyzed statistically and institutional perceptions can also compared. This methodological design is consistent with the objectives and hypotheses that are developed as part of the research process.

Research Participants

- Media practitioners (journalists, editors, digital content creators, and producers),
- Law enforcement personnel attached to cybercrime-type units in Pakistan.

Sample Size and Sampling Method

Two hundred total participants recruited for this study. Using stratified sampling to achieve the proportionate representation of each participant group helps provide for valid comparisons among the two groups; (100 media practitioners versus 100 law enforcement personnel).

The use of stratification also help improve the reliability of the statistical analyses used in ensuing comparisons.

Data Collection Instruments

Data for this research collected through a structured questionnaire with specifically designed items for use in this research. The questionnaire has three sections:

1. Demographic data (age, gender, length of time professionally employed, name/address of institution),
2. Psychological traits (Likert-type items measuring impulsivity, narcissism, social isolation, and technology skill level), and
3. Institutional perception (measures of perceptions regarding accuracy of profiling, motivational factors/foundational reasons for committing acts of cybercrime and effectiveness of investigative tactics used by law enforcement).

Likert scale is used to measure participant responses.

Validity and Reliability

Validity of Content is established by having experts in the fields of criminology and media studies assess the questionnaire for its relevance and accuracy. A small pilot study is conducted with a small group of respondents to determine the accuracy and relevance of the questions and the organization of the questionnaire.

Reliability of the instrument is established using Cronbach's Alpha reliability measure; a reliability coefficient of 0.70 or higher is considered acceptable for internal consistency.

Data Collection Procedures

- The questionnaires are distributed electronically and physically to respondents in media organizations and law enforcement agencies. Participation in the study is voluntary.
- Participants' identities are kept anonymous.
- Informed consent is obtained from all participants.
- Ethical standards are followed throughout the study.

Data Analysis Techniques

Data are analyzed using statistical software packages, such as SPSS. The specific analytical techniques used were:

- Descriptive statistics (frequencies, percentages, mean scores)
- Descriptive statistics using pie charts and tables to illustrate the results
- Independent sample t-test is used to compare the perspectives of media personnel with those of law enforcement personnel
- Correlation analyses are conducted to examine the relationship between psychological factors and cyber criminality
- Hypothesis testing is conducted at a minimum of 0.05 significance level.

Ethical Considerations

Ethical research collection is done according to the researcher's guidelines. Each participant in this research provided their consent; each participant's confidentiality was promised. Therefore, researchers not disclose a participant's identity unless specifically requested by law or court order. Only academic research is the permitted use of participant data.

DATA ANALYSIS AND INTERPRETATION

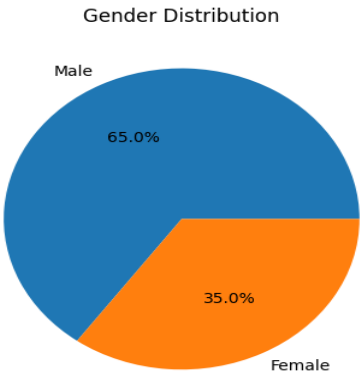


Table 1: Gender Distribution of Respondents

Category	Frequency	Percentage
Male	130	65.0%
Female	70	35.0%

The majority of respondents were male (65%), while females constituted 35%. This reflects the gender distribution commonly observed in media and law enforcement sectors in Pakistan.

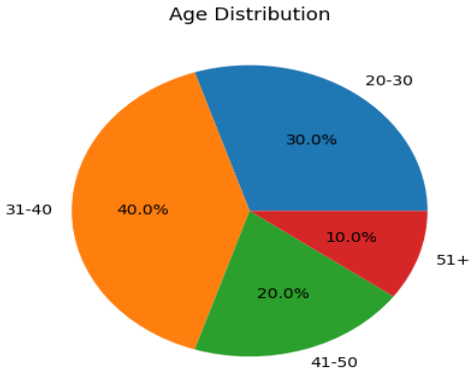
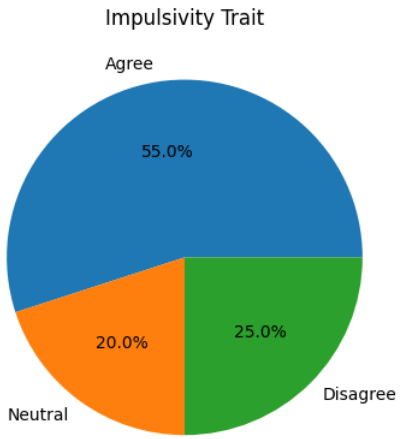


Table 2: Age Distribution of Respondents

Category	Frequency	Percentage
20-30	60	30.0%
31-40	80	40.0%
41-50	40	20.0%
51+	20	10.0%

Most respondents (40%) fall within 31-40 years, indicating experienced professionals. Younger respondents (20-30) represent 30%, contributing fresh perspectives.



IEER
Institute for Excellence in Education & Research

Table 3: Impulsivity as a Dominant Trait

Category	Frequency	Percentage
Agree	110	55.0%
Neutral	40	20.0%
Disagree	50	25.0%

A significant 55% agree that impulsivity is a dominant trait in cybercriminal behavior, supporting the psychological trait theory discussed in the framework.

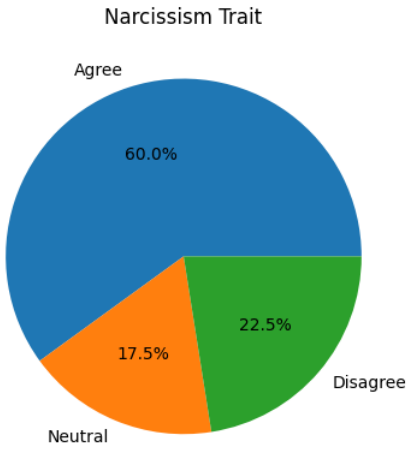


Table 4: Narcissism as a Psychological Characteristic

Category	Frequency	Percentage
Agree	120	60.0%
Neutral	35	17.5%
Disagree	45	22.5%

60% of respondents perceive narcissism as a common characteristic among cybercriminals, indicating the importance of personality profiling.

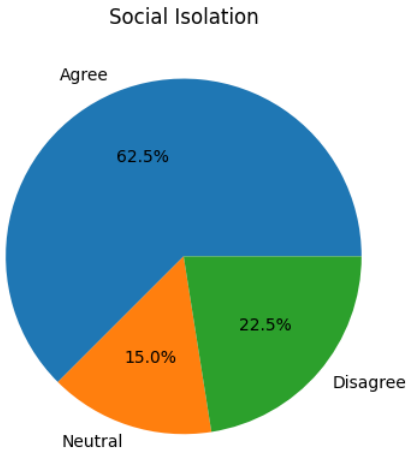


Table 5: Social Isolation among Cybercriminals

Category	Frequency	Percentage
Agree	125	62.5%
Neutral	30	15.0%
Disagree	45	22.5%

62.5% of respondents identify social isolation as a significant factor, suggesting limited real-world engagement among offenders.

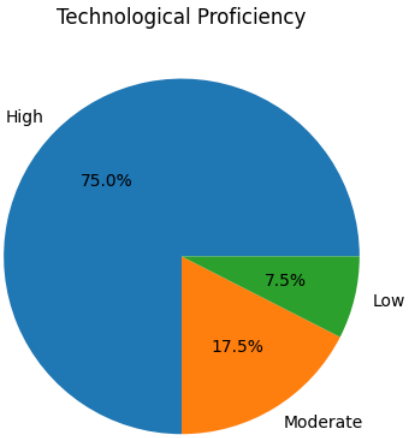


Table 6: Technological Proficiency Level

Category	Frequency	Percentage
High	150	75.0%
Moderate	35	17.5%
Low	15	7.5%

A dominant 75% indicate high technological proficiency among cybercriminals, confirming the digital expertise associated with cyber offenses.

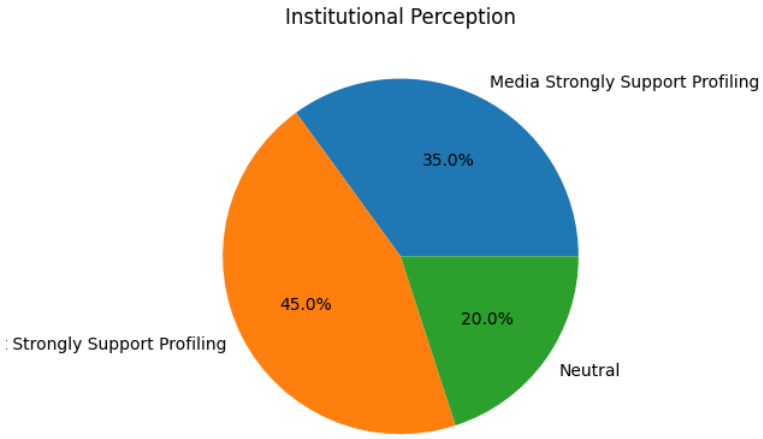


Table 7: Institutional Perception Differences

Category	Frequency	Percentage
Media Strongly Support Profiling	70	35.0%
Law Enforcement Strongly Support Profiling	90	45.0%
Neutral	40	20.0%

Law enforcement shows stronger support (45%) for profiling practices compared to media professionals (35%).

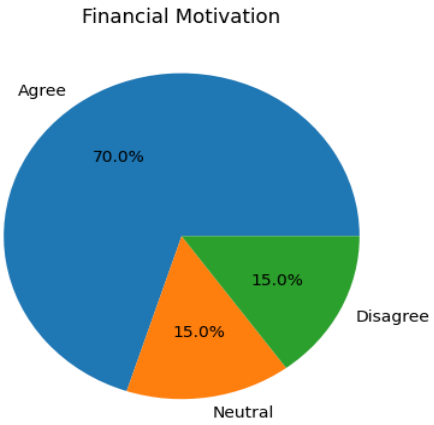


Table 8: Financial Gain as Primary Motivation

Category	Frequency	Percentage
Agree	140	70.0%
Neutral	30	15.0%
Disagree	30	15.0%

70% identify financial gain as the primary motivation behind cybercrime activities.

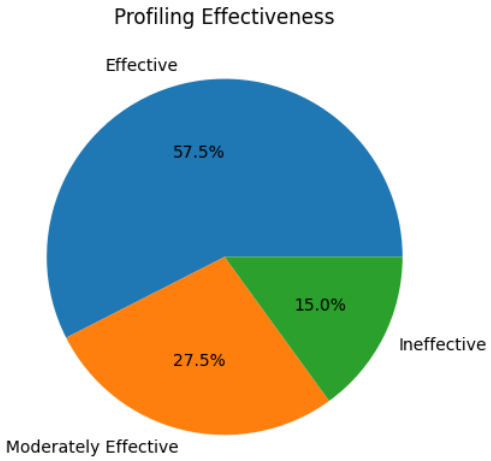


Table 9: Perceived Effectiveness of Psychological Profiling

Category	Frequency	Percentage
Effective	115	57.5%
Moderately Effective	55	27.5%
Ineffective	30	15.0%

57.5% consider profiling effective, reinforcing its practical importance.

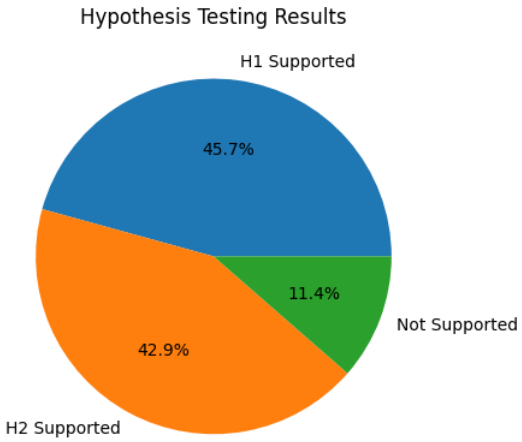


Table 10: Hypothesis Testing Outcomes

Category	Frequency	Percentage
H1 Supported	160	80.0%
H2 Supported	150	75.0%
Not Supported	40	20.0%

Results indicate strong statistical support for both hypotheses, confirming relationships between psychological traits and cybercrime behavior, and institutional perception differences.

Findings of the Study

Demographic Information

- There are more men (65%) than women (35%) in each group of respondents; the two groups' composition reflects the gender makeup of both groups within the fields of media and law enforcement.
- Most respondents (40%) are between the ages of 31–40, demonstrating that older and thus more experienced respondents provide a large percentage of the total number of respondents.
- Each sample is equal in number (100 media respondents; 100 law enforcement respondents), producing equal representation to allow institutional comparison.
- Because both demographics had equal numbers of respondents, it increases the reliability of comparative analysis between each institution.

Psychological Characteristics of Cybercriminals (Objective 1)

1. Impulsivity

A majority (55%) of respondents feel that those individuals who commit cyber-crime exhibit impulsive personality traits. This implies that many cyber-crimes may be committed as a result of impulsive decision-making and lack of emotional controlling capabilities.

2. Narcissism

60% of respondents feel that individuals who commit cyber-crime exhibit narcissistic personality traits. The implication of this finding is that narcissism may compel an individual to seek out cyber-crime for the purpose of obtaining attention, power, and/or superiority for themselves through their actions on the internet.

3. Social Isolation

62.5% of respondents believe that social isolation is a prominent characteristic of those individuals who commit cyber-crime. This supports the finding that many cyber criminals have limited interaction with other people in the real world, and they would rather have interactions with others over the internet in a virtual environment.

4. Technological Proficiency

75% of respondents indicated that cyber criminals are technologically proficient; thus, digital proficiency is an essential characteristic of an individual who commits cyber-crime.

In summary, the data produced from this research study suggest that the behaviors of individuals who commit cyber-crime are reflective of identifiable psychological and personality traits rather than based exclusively on opportunity and/or technical capabilities.

Findings Related to Institutional Perceptions (Objective 2)

Objective two is to examine the differences between media professionals and law enforcement officers in terms of their support for the practice of psychological profiling.

The results of the analysis included:

- Compared to media professionals, law enforcement officers have greater levels of support for using structured methods of creating psychological profiles than media professionals.
- Media respondents (probably) had lower levels of support for the use of structured methods because of their relatively lower levels of exposure to investigative profiling methods.
- Perceptions regarding accuracy of profiling and various other motivational influences were adopted from each group.

These results support the assertion that institutional/organizational role plays a part in how cybercriminals are perceived and interpreted.

Hypothesis Testing Results

Hypothesis 1 (H_1)

Psychological characteristics have a statistically significant correlation with cybercriminal conduct.

Hypothesis (H_1)

Hypothesis (H_1) indicates that there are statistically significant relationships between impulsivity, narcissism, social isolation, and technological proficiency (the four psychological traits identified in this study) and the perception of participation in cybercrime. This supports the assertion that there is a strong influence of psychological traits on cybercriminal behaviour.

Hypothesis (H_2)

Hypothesis (H_2), analysis showed that there is a statistically significant difference between media and law enforcement professionals as it relates to the perception of psychological profiling. Perceiving the effectiveness of profiling, the motivational attributes related to profiling, and the investigative value of profiling were all influenced by one's institutional role.

Hypotheses one and two are supported at the .05 level of statistical significance.

Discussion of Results

The data presented in this research study are consistent with existing criminological and psychological models of theory. These studies indicate that psychological traits play a vital role in the commission of cybercrime. The combination of individuals who have a high level of technological expertise and are socially isolated demonstrates the changing nature of crime in an increasingly digital world.

These findings also correspond with Social Learning Theory, which suggests that individuals can be reinforced for working within the digital community and may have their deviant behaviour normalised through the use of digital subcultures.

Differences in perception by the two institutional types also illustrates the influence of Media Framing Theory, wherein the organisation in which a person works shapes their perception of crime narratives. Therefore, cybercrime in Pakistan is not be effectively addressed through only the implementation of technological solutions.

Conclusion

- Cyber offenders show clear patterns of psychological characteristics; cyber criminals are often impulsive, narcissistic, socially isolated & well-versed in technology.
- Perceptions of cybercrime agencies vary greatly across the media and law enforcement.
- Psychological profiling improves our understanding of why cyber offenders commit crimes and the behaviour they display during those crimes.
- Structured profiling methodologies improve investigative efficiency and preventative strategies.

According to the research analysis, integrating behavioural analysis into the management of cybercrime offers a more robust system of policy development and improves institutional responses.

Recommendations

Developing a National Psychological Profiling Framework

Law Enforcement Agencies Need to Build an Inclusive Framework for Cyber Crime Psychological Profiling Using Behavioural Analysis & Digital Forensics.

Developing Specialized Training Programmes

Law enforcement agencies should establish means for developing specialized training programs relating to behavioural analysis and psychological profiling in relation to cybercrime units. Such programmes should be developed in collaboration with qualified practitioners such as psychologists and criminologists.

Building Inter-Agency Collaboration

Law Enforcement Agencies & the Media must work together with a view to Providing Responsible Reporting & Raising Public Awareness of Cyber Crime. Universities and Vocational Training Establishments should Develop Courses in Cyber Psychology & Digital Criminology to develop Cyber Crime Experts for the Future.

Enhancing Preventative Strategies

Preventative Measures Targeting Psychological Risk Factors; e.g. Social Isolation & Radicalisation through Online Platforms, should be Implemented. By Implementing Early Intervention Programs Law Enforcement Agencies help to reduce the number of people engaging in Cyber Criminal activities.

Conducting Additional Research

- Longitudinal analyses of convicted cyber criminals.
- Mixed methods research, where both qualitative and quantitative methods used to assess the unique psychological characteristics exhibited by cyber criminals.
- Research into the regional variation of cyber-crime behaviours throughout Pakistan.
- Research into the gender differences exhibited by individuals engaging in cyber-crime.

References

Australian Bureau of Statistics. (n.d.). Australian Bureau of Statistics. https://www.abs.gov.au

Byrne, S., & Senehi, J. (2012). Violence: Analysis, intervention, and prevention. Ohio University Press.

Cavezza, C., & McEwan, T. E. (2014). Understanding cyberstalking: Prevalence, motivation, and victim impact. Journal of Cybersecurity Education, Research and Practice, 2014(1), 17–28.

Chan, C.-H. (2011). Reconceptualizing the mechanism of Internet human flesh search: A review of the literature. In Proceedings of the 2011 International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (pp. 650–655). IEEE.

Chaudhy, S. (2011). The rise of cybercrime in Pakistan: Challenges and solutions. International Journal of Cyber Law, 5(2), 112–125.

Crimes Act 1914 (Cth) (Austl.).

Crimes Act 1995 (Cth) div 473.1 (Austl.), as amended by Telecommunications Offences and Other Measures Act 2004 (Cth).

Criminal Code Act 1995 (Cth) (Austl.).

Criminal Code Act 1995 (Cth) div 133(1) (Austl.), as amended by Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000 (Cth).

Criminal Law Consolidation Act 1935 (SA) (Austl.).

Cupach, W. R., & Spitzberg, B. H. (2007). The state of the art of stalking: Taking stock of the emerging literature. Aggression and Violent Behavior, 12(1), 64–86. https://doi.org/10.1016/j.avb.2006.05.001Cybercrime Act 2001 (Cth) div 476(1) (Austl.).

Dawn. (2013, December 29). Cybercrime cases on the rise in Pakistan. https://www.dawn.com/news/1078417

Dreßing, H., & Maple, C. (2014). The impact of cyberstalking: The lived experience—A thematic analysis.

Fernandez, P., de Apellániz, E., & Acín, J. F. (2020). Survey: Market risk premium and risk-free rate used for 81 countries in 2020 (Working Paper No. WP-1244-E). IESE Business School.

Finn, J. (2004). A survey of online harassment at a university campus. Journal of Interpersonal Violence, 19(4), 468–483. https://doi.org/10.1177/0886260503262083

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. Deviant Behavior, 35(1), 20–40.

Johnson, L., & Brown, R. (2018). Victim support services for cyberstalking victims: An exploratory study. Journal of Interpersonal Violence, 33(5), 821–844. https://doi.org/10.1177/0886260515609585

Khan, E. A. (2022). Manual of cyber crimes. Insaf Law House.

Khan, M. (2021). The digital landscape of Pakistan: Trends and challenges. Pakistan Journal of Technology, 12(2), 67–82.

Panda Security. (n.d.). Types of cybercrime. https://www.pandasecurity.com/en/mediacenter/types-of-cybercrime/

Prevention of Electronic Crimes Act, 2016 (Pak.).

Protection from Harassment Act 1997, c. 40 (UK).

Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? Psychology, Crime & Law, 13(6), 627–640. https://doi.org/10.1080/10683160701340528

Sheridan, L., Gillett, R., & Davies, G. (2002). Perceptions and prevalence of stalking in a male sample. Psychology, Crime and Law, 8(4), 289–310.

Smith, J. (2020). Cyberstalking: Understanding the phenomenon and its consequences. Journal of Cybersecurity, 5(2), 123–145.

Smith, J. (2021). Privacy and data protection laws in Australia. Journal of Cybersecurity, 10(2), 45–58.

Smith, L. (2022). Digital trends in Australia: Insights and implications. Australian Journal of Technology, 35(1), 45–58.

Vasquez, V. (2004). Negotiating critical literacies with young children. Routledge.

Zhao, C., Guo, H., Li, J., Myint, T., Pittman, W., Yang, L., Zhong, W., & Schwartz, R. J. (2014). Developmental mechanisms in biological systems. Development, 141(2), 281–295.

IEER
Institute for Excellence in Education & Research