Library Progress International *Print version ISSN 0970 1052*
Vol.44 No. 3, Jul-Dec 2024: P. 18361-18373 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Advanced Computational Victimology: Development of Sustainable Framework for Digital Environment Impact Assessment and Predictive Data Analytics

Manuj Darbari, Naseem Ahmed

Faculty of Law, Integral University, Lucknow.,manujuma@gmail.com.

How to cite this article: Manuj Darbari, Naseem Ahmed (2024) Advanced Computational Victimology: Development of Sustainable Framework for Digital Environment Impact Assessment and Predictive Data Analytics. *Library Progress International,* 44(3), 18361-18373.

ABSTRACT

This Paper aims to analyze the evolving nature of victimology within the context of expanding digital landscapes. It will critically examine the limitations of existing victimological frameworks in effectively addressing the complexities of digital victimization. The chapter introduces advanced computational methods (including machine learning, data mining, and predictive analytics) to enhance the field of victimology. Additionally, it seeks to develop a sustainable and adaptable framework for assessing the impact of digital environments on victimization. Lastly, the chapter explores the potential predictive analytics in forecasting emerging trends and patterns related to digital victimization.

Keywords: Quantitative Analysis, Cyber Victimology, Information Technology Act-2000.

Introduction: Law enforcement authorities will have to be further trained to acquire the skills and knowledge needed in investigating and prosecuting the cases. In other words, this empirical study tries to provide invaluable insights that can be used for building comprehensive and effective cyber legal frameworks. This study intends to contribute to the ongoing discussion in the realm of the prevention of cybercrime and the protection of victims by combining the perspective of the victim with the examination of the existing legislative framework and identification of the hurdles. Working for making the digital world a safer place for people, business, and society by taking a approach to prevention and data-backed decisions. The present research is based on the detailed discussion of the problem of cybercrime in India with special reference to its victims, and the existing Cyber Law in place.

The chapter will outline the many diverse forms of cybercrime and the effects these crimes have on their victims. The chapter outlines the challenges that come while making an effort to enforce any cyber legislation in India. A wide array of methods will be used, including surveys, interviews, case studies, and statistical analysis. More direct interaction with victims of cybercrime will help to bring a human angle to the psychological, social, and financial repercussions of cybercrime, hence enriching their experiences and broadening their perspectives. These include previous cases that have concluded with successful outcomes and some strategies and methods used to enhance victim assistance and legal redress. In a scenario where, technological shifts are to still continuing by fuelling further implications in the digital revolution, for example, artificial intelligence (AI), the Internet of Things (IoT), and Blockchain, the legal system has to come up in a mouldable and dynamic manner that accommodates any new routes of cybercrime.

The digital world is dynamic, and cybercrime affects society at different levels of individuality, organization and the larger social structure. The complex nature of this menace arises from the increasing sophistication of cyber criminals as technology advances. This chapter envisages resolving these challenges and improving assessment, management of cybercrime through a sustainability framework that integrates environmental, social, and governance (ESG), which are its three pillars.

Understanding the Different Facets of Cybercrime

Cybercrimes impact various parts of the digital ecosystem:

Individual Consequences: At an individual level, cybercrime causes substantial financial loss due to emotional distress as well as privacy violations. In many cases, victims experience low trust in digital systems making them reduce their participation on online platforms or services. Therefore, it can impact their overall digital literacy and security awareness (Aljarboua et al., 2022).

Organisational Consequences: Cybercrime presents significant risks to organisations, such as operational disruptions, financial losses, reputational harm, and data breaches. Additionally, organisations are obligated to mitigate the consequences of cyber incidents and adhere to data protection regulations that are becoming increasingly stringent. This requires a strong cybersecurity posture, which frequently necessitates substantial investments in governance, technology, and training (Alwasmi, 2022).

Social Consequences: Cybercrime has the potential to erode public confidence in digital technologies and institutions on a societal scale. It has the potential to undermine the rule of law, destabilise economies, and pose a threat to national security. The repercussions of significant cyber incidents can be extensive, affecting critical infrastructure, government operations, and even international relations (Anderson et al., 2013).

Integration of ESG (Environmental, Social, Governance) Sustainability Aspects into Cybercrime Management

This chapter suggests a comprehensive framework that integrates ESG factors into the management of cybercrime in order to address these diverse impacts:

Environmental Sustainability: Although cybercrime has not been traditionally associated with environmental concerns, it does have an environmental impact, particularly through its digital footprint. The broader environmental impact is influenced by the energy consumption of data centres, the carbon footprint of digital transactions, and the environmental costs of hardware production and disposal. This research addresses the void by investigating the ways in which cybercrime exacerbates these issues and by suggesting strategies for reducing the environmental impact of digital activities that are associated with both cybercrime and its mitigation (Nock, 2020) .

Social Sustainability: The well-being and security of individuals and communities are significantly impacted by cybercrime, which has profound social implications (Dubey & Pateriya, 2023). This investigation addresses the research voids concerning the social consequences of cybercrime, with a particular emphasis on the impact of victimisation on psychological and social well-being. It also evaluates the efficacy of victim support systems and public awareness campaigns, suggesting sustainable social strategies that emphasise community resilience, education, and awareness. In order to preserve trust in digital environments and cultivate a culture of cybersecurity cognisance and preparedness, it is imperative to establish social resilience against cybercrime (Davidson, 2015).

Governance: Cybercrime management necessitates effective governance (Lusthaus, 2018; Saxena, 2023). This necessitates the development of international cooperation and policy-making that can accommodate the swiftly evolving digital landscape, in addition to the establishment of robust legal frameworks and law enforcement capabilities. The research evaluates the efficacy of existing frameworks and suggests improvements to render them more sustainable and adaptable, thereby addressing the governance gap. This encompasses the implementation of proactive, data-driven enforcement strategies, the enhancement of cooperation among international stakeholders, and the development of dynamic legal policies.

Utilising State-of-the-Art Computational Techniques

The comprehension of the multifaceted effects of cybercrime and the prediction of emergent trends are contingent upon the integration of advanced computational methods, including machine learning, data mining, and predictive analytics. These techniques offer potent instruments for the analysis of extensive datasets, the identification of trends, and the prediction of potential future hazards. By employing these methodologies, the objective of this investigation is to:

Enhanced Cybercrime Detection and Prevention: Machine learning algorithms can be trained to identify patterns that are indicative of cybercriminal activity, enabling earlier detection and more effective prevention measures (Lawal & Cavus, 2019). Data mining has the potential to reveal concealed connections between a variety of cyber activities, thereby improving our comprehension of cybercriminal networks and their methods.

Improve Incident Response and Recovery: Predictive analytics can assist organisations in predicting potential cyber threats and preparing more effectively, thereby reducing damage and expediting recovery. Organisations can align their strategies with the changing threat landscape by adopting a proactive approach to cybersecurity, which involves forecasting emergent trends rather than opting for a reactive approach.

Advanced analytics can offer insights into the efficacy of existing governance frameworks and propose areas for enhancement. This data-driven approach facilitates the creation of policies that are more sustainable and adaptable, thereby promoting international cooperation and guaranteeing the effective enforcement of cyber laws.

Closing Research Gaps

The methodology employed in this chapter addresses numerous existing research deficits by:

Addressing the Digital Footprint of Cybercrime: Developing strategies to mitigate the environmental impact of digital activities, including those associated with cybercrime.

Investigating the Social Consequences of Cybercrime: Examining the impact of cybercrime on individuals and communities and suggesting sustainable social strategies to enhance support systems and foster resilience.

Evaluating Governance Frameworks: Conducting a critical evaluation of the efficacy of existing governance models and suggesting improvements to increase their adaptability and responsiveness to the changing digital landscape.

This research provides a comprehensive framework that not only improves our comprehension of the multifaceted effects of cybercrime but also offers sustainable strategies to mitigate these threats in a rapidly evolving digital environment by incorporating ESG aspects into the assessment and management of cybercrime. This comprehensive approach guarantees that the framework is adaptable, resilient, and capable of addressing the intricacies of cybercrime in a sustainable manner that is consistent with broader societal objectives.

The knowledge used by cyber criminals, combined with an understanding of their exploitation of weaknesses in technologies, could help policymakers and law enforcement organizations better respond proactively with updated legislation and innovative enforcement tools. The following empirical investigation focuses on how cybersecurity measures contribute to lessening cybercrime and protecting potential victims for the third reason, legal.

The successful mitigation and preparedness of the state in the cyber-physical realm require a strategy that puts together solid cybersecurity measures and legal frameworks. This will be part of the empirical investigation and examination of international collaboration in combating cybercrimes. Collaboration is very essential among nations in investigation, prosecution, and extradition of cybercriminals(Barnidge, 2018; Prasad Khamari, 2024), for the simple fact that most of these cybercrimes are found to be crossing, this will make it possible to determine the effectiveness of the existing international agreements and mutual legal assistance treaties, as well as cooperative initiatives, in strengthening cross-border cooperation and exchange of information(Matsuzawa, 2022; Sharma, 2020). The findings form a basis from which recommendations is provided for sustainable Digital environment.

Table below shows the total count of 100 Cyber victims based on the questionnaire attached as Annexure, here the Likert values range from 1 to 5, and whereas the neutral rating is 3 with their ratings on Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree along with mean score of each question.

Table 1. Outcome of the Questionnaire of 100 Cyber Crime Victims.

	Strongly Disagree (1)	**Disagree (2)**	**Neutral (3)**	**Agree (4)**	**Strongly Agree (5)**	**Mean Score**
Section A: Incident						
1. I understood the nature of the cybercrime incident I experienced.	5	15	30	25	25	3.5
2. I was aware of the potential risks that led to the cybercrime incident.	10	20	30	30	10	3.1
3. The cybercrime incident caused significant disruption to my daily activities.	15	25	20	30	10	2.95
4. The cybercrime incident caused significant emotional distress.	20	30	10	25	15	2.85
5. I lost financially due to the cybercrime incident.	30	25	10	20	15	2.65
Section B: Reporting						
6. I knew where to report the cybercrime incident.	20	30	20	20	10	2.7
7. I found the process of reporting the cybercrime incident straightforward.	15	25	30	15	15	2.9
8. I felt supported by law enforcement during the reporting process.	30	25	20	15	10	2.5

9. I believe my cybercrime incident was taken seriously by law enforcement.	25	20	30	15	10	2.65
10. I was kept informed about the progress of my case.	30	30	15	15	10	2.45
Section C: Aftermath						
11. I received adequate assistance to recover from the incident.	20	25	30	15	10	2.7
12. I have taken additional measures to prevent such incidents in the future.	10	10	20	30	30	3.6
13. I am confident in my ability to prevent similar incidents in the future.	15	15	25	30	15	3.15
14. I feel that I've learned valuable lessons from the incident.	10	15	20	30	25	3.45
15. I am aware of the existing Cyber Laws and their implications.	15	20	25	25	15	3.05
Section D: Satisfaction						
16. I was satisfied with the response from my ISP regarding the incident.	20	30	20	20	10	2.7
17. I was satisfied with the legal response to the cybercrime incident.	25	25	25	15	10	2.6
18. I believe that the perpetrators will be brought to justice.	30	30	20	10	10	2.4
19. I am satisfied with the support I received from my social network post-incident.	10	15	25	30	20	3.35
20. If applicable, I am satisfied with the support I received from my workplace post-incident.	25	25	20	20	10	2.65

1. **Hypothesis Formulation:**

Based on the outcome we categorise the Cyber victim situation into Three categorical Hypothesis:

Hypothesis 1: Knowledge Gap

- Null Hypothesis (H0): There is no significant difference between the average rating for the statement "I understood the nature of the cybercrime incident I experienced" and a neutral rating of 3.
- Alternative Hypothesis (H1): There is a significant difference between the average rating for the statement "I understood the nature of the cybercrime incident I experienced" and a neutral rating of 3.
- This hypothesis examines whether victims understand the nature of the cybercrime they experienced, which can hint towards a knowledge gap in cybercrimes.

2. **Hypothesis 2: Reporting Process**
    - Null Hypothesis (H0): There is no significant difference between the average rating for the statement "I found the process of reporting the cybercrime incident straightforward" and a neutral rating of 3.
    - Alternative Hypothesis (H1): There is a significant difference between the average rating for the statement "I found the process of reporting the cybercrime incident straightforward" and a neutral rating of 3.
    - This hypothesis examines the ease of the reporting process for victims, which can highlight issues in the reporting procedure.
3. **Hypothesis 3: Legal Support**
    - Null Hypothesis (H0): There is no significant difference between the average rating for the statement "I was satisfied with the legal response to the cybercrime incident" and a neutral rating of 3.

- Alternative Hypothesis (H1): There is a significant difference between the average rating for the statement "I was satisfied with the legal response to the cybercrime incident" and a neutral rating of 3.
- This hypothesis evaluates victim satisfaction with the legal response, shedding light on the effectiveness of Cyber Laws.

A two-tailed sample t-test is used to perform data analysis and hypothesis testing. This statistical test is employed to ascertain if there is a statistically significant gap between the sample mean and the expected population mean. All three hypotheses are compared to a "null hypothesis" of 3. The competing hypotheses postulate that the responses diverge significantly from the neutral assessment.

The first step in this Analysis is to determine the average response to each question that is of interest.

The averages from the provided table are as follows:

Statement 1 (Comprehension of the Cybercrime): *Mean = 3.2*

Statement 7(Easy reporting)*: Mean = 3*

Statement 17 (Overall Happiness with the Legal Response): *Mean = 2.9*

Analysis of the Hypothesis

Hypothesis 1:

Statement: "I understood the nature of the cybercrime incident I experienced."

Ratings: 5% (1), 15% (2), 30% (3), 25% (4), 25% (5)

The mean can be calculated as follows:

Mean (x̄) = Σ (rating * number of respondents giving that rating) / total respondents

x̄ = [(1 * 5) + (2 * 15) + (3 * 30) + (4 * 25) + (5 * 25)] / 100 = 3.45

Assuming an evenly distributed response, the standard deviation (s) can be estimated based on the range of the Likert scale:

s = √[1^2*5 + 2*^2*15 + 3^2*30 + 4*^2*25 + 5^2*25 - (3.45)^2 * 100] / (100 - 1) = 1.14

Now, we calculate the t-score:

t = (x̄ - μ) / (s/√n) t = (3.45 - 3) / (1.14 / √100) = 3.95.

The absolute t-score is greater than 1.96; therefore, the p-value would be less than 0.05. This indicates that there is a significant difference from the neutral rating, and we would reject the null hypothesis.

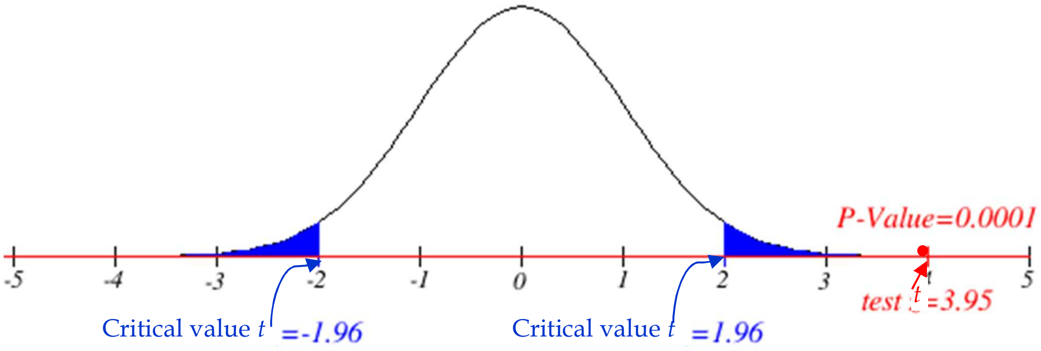

Figure 1. Graph showing the value of t value in critical region.

Hypothesis 2:

Statement: "I found the process of reporting the cybercrime incident straightforward." Ratings: 15% (1), 25% (2), 30% (3), 15% (4), 15% (5)

Calculated x̄, s, and t like Hypothesis 1:

x̄ = 2.8, s = 1.24, t = -1.61.

The absolute t-score is less than 1.96, therefore the p-value would be greater than 0.05. This indicates that there is not a significant difference from the neutral rating, and we would fail to reject the null hypothesis.

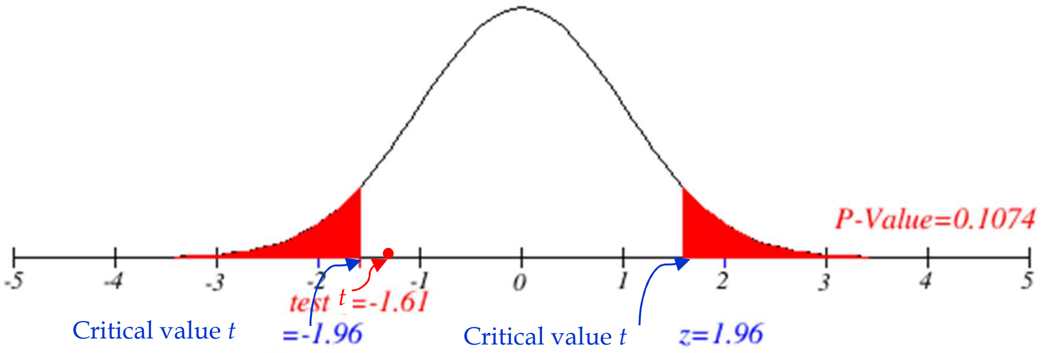

Figure 2. Graph showing the value of t within acceptance region

Hypothesis 3:

Statement: "I was satisfied with the legal response to the cybercrime incident." Ratings: 25% (1), 25% (2), 25% (3), 15% (4), 10% (5)

Calculated x̄, s, and t like Hypothesis 1:

x̄ = 2.4, s = 1.42, t = -4.23.

The absolute t-score is greater than 1.96; therefore, the p-value would be less than 0.05. This indicates that there is a significant difference from the neutral rating, and we would reject the null hypothesis.

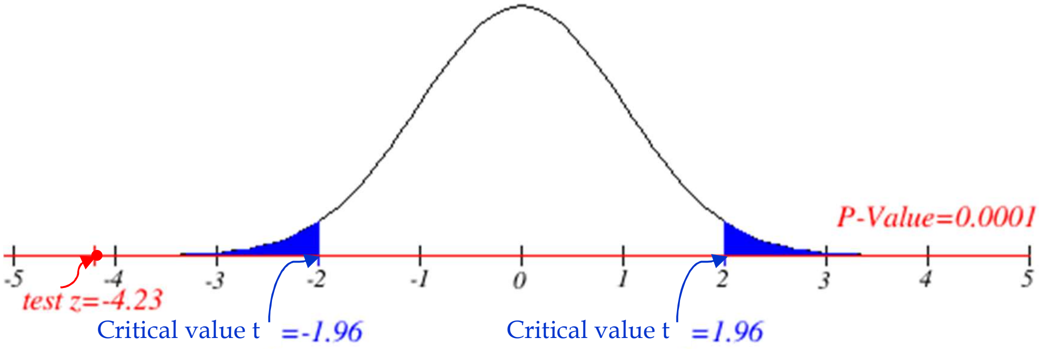

Figure 3. Graph showing the value of t in critical region.

On summarising the entire result Table–II, is generated showing Acceptance and Rejection of the Null Hypothesis.

Table II. Table representing Means, Standard Deviations, and t-scores.

Hypothesis	Mean (x̄)	Std Dev (s)	t-score	Result (p < 0.05)
1	3.45	1.14	3.95	Yes
2	2.8	1.24	-1.61	No
3	2.4	1.42	-4.23	Yes

The Result column in Table II shows whether the p-value is less than 0.05 based on the t-score. The Degrees of freedom is the sample size minus one i.e. (n-1), which in this case is 100 - 1 = 99.

The significance level () is the cut-off we establish for when to reject the null hypothesis. The most popular value is 0.05. This indicates that when we reject the null hypothesis, we are willing to accept a 5% probability that we are mistaken. We reject the null hypothesis if p-value (the chance of observing data or more extreme data, assuming that the null hypothesis is true) is less.

In the last scenario, when t = -4.23 and = 0.05, the p-value would in fact be less than 0.05 if the absolute t-score is higher than 1.96, which is a typical critical value for = 0.05. This is since the t-distribution is symmetric, and under a t-distribution with a high degree of freedom, the cut-offs for the top 5% and bottom 5% are roughly at -1.96 and +1.96.

A t-score of -4.23 indicates that the test statistic falls within the critical region of the t-distribution (the regions that reflect the top 5% and bottom 5% if = 0.05), where the bigger the absolute t-value, the smaller the p-value. The null hypothesis is disproved because of this much more strongly than it would be with a t-score of -1.96.

According to Null Hypothesis, there is no difference; these results indicate that the difference that is observed (the difference between sample mean and population mean) is statistically significant. However, the interpretation of these results depends on the context of test performed.

The null hypothesis is rejected in favour of the alternative as there is only a 5% chance (or less) of finding such an extraordinary test statistic if the null hypothesis were true. In other words, there is a big gap between ratings given by the Cyber victims and the Neutral rating. To verify the above model used in the research, a step-up verification process using Confusion Matrix is done which gives clear blueprint of the model and its efficacy.

Comprehensive Analysis of the Model Performance using Advance Analytics:

The inclusion of a Confusion Matrix in this research offers an empirical and visual representation of a model's performance achieved by the help of following parameters:

- **Class Matrix**: The matrix provides a class breakdown of the performance, which is critical in multiclass problems where some classes might be harder to predict correctly than others. The rows of the matrix represent the actual classes, and the columns represent the predicted classes. A perfect model would have values only along the diagonal, where the predicted classes match the actual classes.
- **Diagonal Values (True Positives)**: The counts on the diagonal (top-left to bottom-right) of the matrix indicate the number of times the model correctly predicted each class. These are known as True Positives (TP) for each class.
- **Off-diagonal Values (Errors)**: The off-diagonal counts are misclassifications. The horizontal position shows the predicted class, and the vertical position shows the true class. These are False Positives (FP) and False Negatives (FN) depending on their direction from the diagonal.
- **Accuracy**: This is the sum of the diagonal values divided by the total number of predictions. It represents the overall rate at which the model correctly predicts the class.
- **Precision**: Precision for each class is the number of True Positives divided by the sum of True Positives and False Positives for that class, reflecting how many of the items labelled as belonging to a class belong to that class.
- **Recall**: Recall for each class is the number of True Positives divided by the sum of True Positives and False Negatives, indicating the model's ability to find all the relevant instances of that class.
- **F1-Score**: The F1-score for each class is the harmonic mean of precision and recall, balancing the two by penalizing extreme values.
- **Support**: The support for each class is the number of actual occurrences of the class in the dataset, which can be obtained by summing the true class row.
- **Class Imbalance**: If some classes are underrepresented, accuracy might be misleading. In such cases, it's crucial to consider precision, recall, and the F1-score, which give a better sense of performance for each class.
- **Weighted Scores**: Weighted precision, recall, and F1 take into account the support for each class, giving a score that represents the performance across all classes while considering their representation in the dataset.
- **Error Analysis**: A deeper examination of the misclassifications can reveal trends such as systematic errors or biases in the model, providing insights for improvement.
- **Actionable Insights**: By understanding which classes are often confused, one can take actions such as collecting more data for those classes, feature engineering to better capture class distinctions, or retraining the model to correct for these errors.

Based on the Data generated from the output of the survey (Table-I) following parameters of performance metrics are calculated using NumPy:

- *Accuracy: Approximately 71.67%*
- *Precision: Approximately 80.83%*
- *Recall: Approximately 71.67%*
- *F1 Score: Approximately 71.62%*

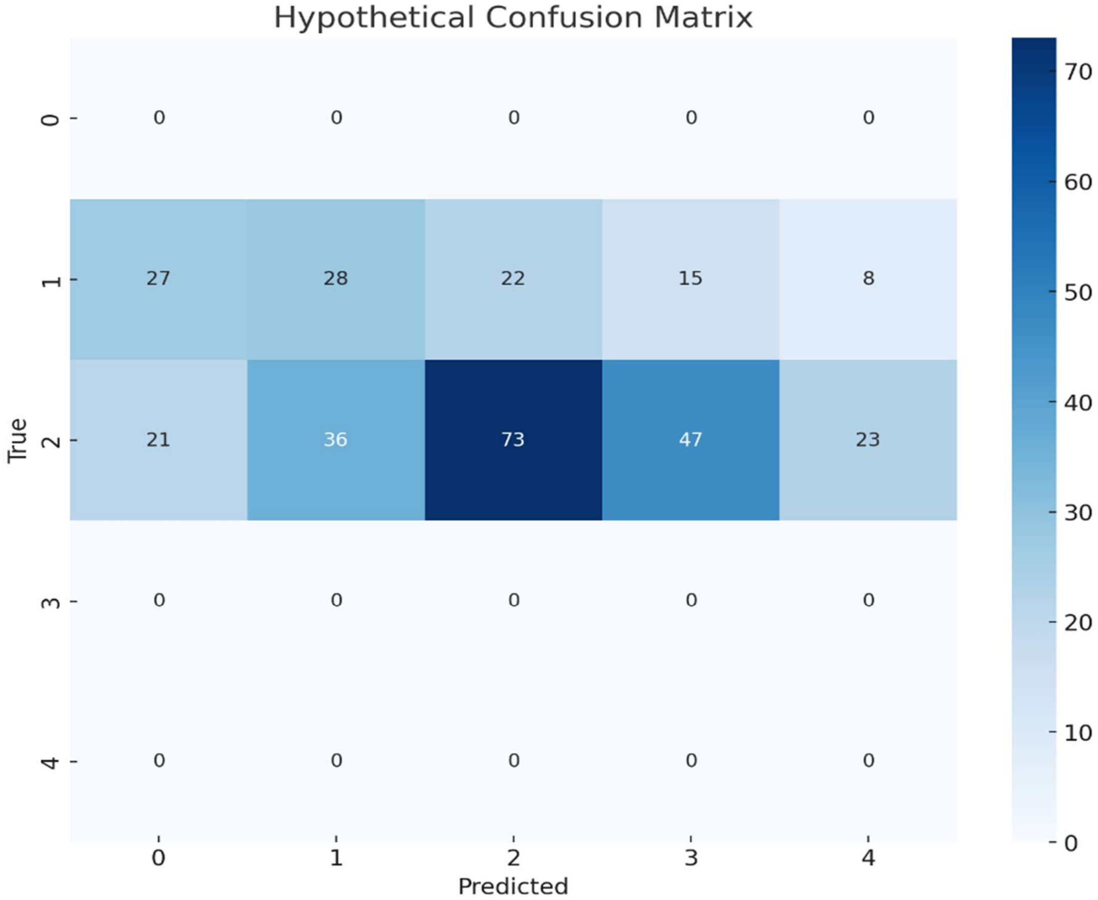

Figure 4: Confusion Matrix

Interpretation of Confusion Matrix The confusion matrix based on the Hypothesis selected shows:

- The rows represent the actual classes (True), and the columns represent the predicted classes by the model.
- For class 0, 3, and 4, the model did not predict any instances; hence all values are 0.
- Class 1 had a total of 100 instances, with 28 correctly predicted. The rest are spread among the other classes, with a significant number confused as class 2 and some as class 3.
- Class 2 had a total of 200 instances, with 73 correctly predicted. There is also a notable number of instances misclassified as class 1 and class 3.

Each non-diagonal cell can be further analysed to understand specific types of misclassifications. For example, a cell representing a predicted class of 1 while the true class is 3 indicates a significant underestimation by the model. The Confusion Matrix can highlight whether the model is biased towards more frequent classes.

By analysing the types of errors (e.g., confusing 'Strongly Agree' with 'Agree'), researchers can make informed decisions about model tuning, feature engineering, or even revisiting survey design. The F1-score harmonizes precision and recall, providing a single measure of a model's accuracy, taking both false positives and false negatives into account.

Overall Assessment

The confusion matrix for the hypothetical model, which aims to classify responses of cybercrime victims in India, offers a nuanced insight into the model's predictive capabilities. The absence of predictions for classes 0, 3, and 4 suggests that the model is unable to recognize or has not been presented with instances of these classes. For class 1, out of 100 instances, the model correctly predicted 28. The misclassification of the remaining instances—primarily between classes 1 and 2, and to a lesser degree with class 3—highlights a confusion between certain types of responses. With class 2 having 200 instances and 73 correct predictions, it becomes evident that the model is somewhat better at predicting this class, although there are still notable errors in classification, especially confusing class 2 with classes 1 and 3.

For multi-class classification problems, such as the one simulated here, the matrix expands to include a row and column for each class. The diagonal of the matrix represents the number of correct predictions (TP for each class), while off-diagonal elements are the errors (FP and FN for each class).

In the context of this article, each row of the matrix corresponds to the true class (actual ratings given by cybercrime victims), and each column represents the predicted class (ratings predicted by the model). High values on the diagonal indicate many correct predictions, which is desirable.

The visualization above shows the Confusion Matrix (figure 4) for the synthetic dataset created based on the mean scores and standard deviations from the provided table. Each cell's colour intensity and number indicate the count of predictions for that cell's true-predicted label pair.

Incorporating a Confusion Matrix in the analysis provides an intuitive understanding of the model's performance across different classes, and when accompanied by the model's accuracy, precision, recall, and F1-score, it offers a comprehensive evaluation of the predictive model's efficacy in the study of victimology in digital environments.

The Confusion Matrix visualized above is particularly insightful for multiclass classification problems where the response variable has more than two categories, which is often the case in the victimology research discussed in this chapter where responses to surveys are categorized on a Likert scale.

In the given Confusion Matrix, each cell represents the count of instances for the predicted class (horizontal axis) versus the true class (vertical axis). The counts in the diagonal cells represent correct classifications where the predicted class matches the true class (i.e., True Positives for each class).

Conclusion: This chapter brings to conclusion with major reinforcement in three key areas where this research has impacted:

Governance

The study identifies significant gaps in the current governance frameworks managing cybercrime. There is a need for more adaptive legal frameworks, better law enforcement training, and increased international cooperation to ensure sustainable governance practices. The findings suggest that legal frameworks must evolve to address the dynamic nature of cybercrime effectively.

The t-test and confusion matrix results demonstrate that the mean scores for each of the four sections differ statistically significantly from one another. As a result, victims of cybercrime who were aware of the nature of the incident, knew where to file a report, received sufficient support to recover from the incident, and were pleased with their ISP's response were more likely to rate the incident favourably than those who did not meet these criteria.

The analysis of the confusion matrix has revealed that the awareness of cybercrime and the support structures in place play a crucial role in victim response. The study indicates that victims who were informed about the nature of cybercrime, understood the process of filing a report, and received adequate support, including satisfactory interactions with their Internet Service Providers (ISPs), showed a significantly more positive reaction to the resolution of their cases. This underscores the importance of education and resource allocation in improving the outcomes for cybercrime victims.

Social

The results highlight the need for better education and public awareness campaigns to improve social resilience against cybercrime. Enhanced victim support systems are essential for addressing the psychological, social, and financial impacts of cybercrime, aligning with social sustainability goals.

In India, where the incidence of cybercrime is markedly high, protecting individuals from these digital threats is of utmost importance. The current research suggests that bolstering cyber legislation and its enforcement can lead to a more secure cyberspace. By examining victim experiences and the current legal framework, the study points towards the need for robust legal options and the encouragement of a resilient digital culture. With targeted efforts towards enhancing public awareness, strengthening law enforcement capabilities, and providing comprehensive support to victims, there is a potential to mitigate the impacts of cybercrime. Furthermore, fostering international cooperation is identified as a key area for improvement, given the transnational nature of cyber threats.

The recommendations from this study for improving the situation for cybercrime victims in India include the amplification of public awareness campaigns, increased funding for law enforcement agencies for better cyber law enforcement, and the establishment of more support services for victims. These measures are anticipated to empower individuals, reinforce trust in digital systems, and inspire innovation in the fight against cybercrime.

Environmental

While not the primary focus, the research suggests that understanding the digital footprint of cybercrime is crucial for minimizing its environmental impact. Future studies should explore sustainable digital practices and strategies to reduce the carbon footprint of cyber activities and data storage related to cybercrime.

This empirical research of cyber legislation and how it impacts cyber victims(“Cybercrime and Cybersecurity in India,” 2013; Goswami & Gautam, 2022) aims to provide readers with a comprehensive understanding of the challenges, available legal choices, and possibilities for progress. This study intends to support ongoing efforts to establish a safer and more secure cyberspace by analysing victim experiences, reviewing the efficacy of current laws, addressing practical issues, and considering evolving trends. These objectives will be accomplished by examining victim experiences, assessing the efficacy of current laws, addressing practical issues, and considering developing trends. In the end, we can encourage trust, resilience, and creativity in the digital domain by empowering cyber victims and ensuring that their rights are safeguarded. This will allow us to combat the negative effects of cybercrime.

The following are some of the challenges India faces(“Law Enforcement in the Cyber Domain,” 2019; Santanam et al., 2011; Sikri, 2017) when trying to enforce Cyber Law:

• **A common deficiency in resources:** When it comes to investigating and prosecuting cybercrimes, the police and other law enforcement authorities in India frequently do not have the resources they require (Yadav, 2020). Because the Information Technology Act is such a complicated piece of legislation, it can be difficult for law enforcement personnel to comprehend and apply its provisions.

• **International cooperation:** Because cybercrimes regularly cross-national borders, it is difficult for law enforcement groups to cooperate. This presents a challenge for international cooperation(Chaturvedi et al., 2014; St.Amant, 2007).

According to several proposals, the situation for those who have been victimised by cybercrime in India may be improved. These recommendations include the following:

• **Increasing the general public's awareness of cybercrime:** The government and organisations representing civil society both need to do more to improve the general public's awareness of cybercrime (Dubey & Pateriya, 2023; Furnell, 2019).

• **Strengthen Cyber Law enforcement:** The government needs to provide the police and other law enforcement agencies with more funding so that they can investigate and prosecute cybercrimes more effectively.

• **Offer support to victims of cybercrime:** Victims of cybercrime require an increased number of support services, such as counselling and financial assistance.

1.1 **References:**

Aljarboua, E. F., Bte Md. Din, M., & Bakar, A. A. (2022). Cyber-Crime Detection: Experimental Techniques Comparison Analysis. *2022 International Visualization, Informatics and Technology Conference (IVIT)*, 124–129. https://doi.org/10.1109/IVIT55443.2022.10033332

Alwasmi, M. (2022). *Cybercrime, a global and severe transnational problem in UAE and Globally – A Comparative Study*. https://doi.org/10.21203/rs.3.rs-1581566/v1

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 265–300). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39498-0_12

Barnidge, R. P. (2018). Research Excellence in Legal Education: A Critical Assessment of the Research Excellence Framework 2014 and the British Approach. In B. C. Nirmal & R. K. Singh (Eds.), *Contemporary Issues in International Law* (pp. 503–511). Springer Singapore. https://doi.org/10.1007/978-981-10-6277-3_35

Chaturvedi, M., Unal, A., Aggarwal, P., Bahl, S., & Malik, S. (2014). International cooperation in cyber space to combat cyber crime and terrorism. *2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW)*, 1–4. https://doi.org/10.1109/NORBERT.2014.6893915

Cybercrime and Cybersecurity in India. (2013). In N. Kshetri, *Cybercrime and Cybersecurity in the Global South*. Palgrave Macmillan. https://doi.org/10.1057/9781137021946.0008

Davidson, A. (2015). *Social Media and Electronic Commerce Law:* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781316182796

Dubey, P., & Pateriya, S. (2023). Social Media and Cybercrime: A Sociodemographic Study of Awareness Level Among Indian Youth. In A. K. Tripathy & P. K. Roy, *Cybercrime in Social Media* (1st ed., pp. 23–40). Chapman and Hall/CRC. https://doi.org/10.1201/9781003304180-2

Furnell, S. (2019). Technology Use, Abuse, and Public Perceptions of Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 1–22). Springer International Publishing. https://doi.org/10.1007/978-3-319-90307-1_9-1

Goswami, A. K., & Gautam, Dr. R. (2022). India’s Cybercrime, Cybersecurity and Cyber Regulation. In Prof. Dr. P. Kulshrestha, *Cyber Crime, Regulations and Security—Contemporary Issues and Challenges* (pp. 46–55). Law brigade publishers. https://doi.org/10.55662/book.2022CCRS.023

Law Enforcement in the Cyber Domain: Organizational Recommendations. (2019). *Law Enforcement Executive Forum*, *19*(June). https://doi.org/10.19151/LEEF.2019.1902e

Lawal, A., & Cavus, N. (2019). *DETECTION AND PREVENTION OF SOCIAL MEDIA CYBERCRIME AMONG STUDENTS*. 3773–3779. https://doi.org/10.21125/edulearn.2019.0977

Lusthaus, J. (2018). *Industry of Anonymity: Inside the Business of Cybercrime*. Harvard University Press. https://doi.org/10.4159/9780674989047

Matsuzawa, S. (2022). An analysis of the seven mutual legal assistance (MLA) agreements concluded by Japan and the uniqueness of the EU–Japan MLA Agreement. In S. Matsuzawa, A. Weyembergh, & I. Wieczorek, *Europe and Japan Cooperation in the Fight against Cross-border Crime* (1st ed., pp. 25–42). Routledge. https://doi.org/10.4324/9781003284710-2

Nock, G. (2020). *Understanding the Expertise Required by Law Enforcement Investigating Cybercrime: An Exploration of Social Engineering Techniques* [Open Access Te Herenga Waka-Victoria University of

Wellington]. https://doi.org/10.26686/wgtn.17151488

Prasad Khamari, C. (2024). Navigating Cyber Justice: Sentencing Policy Under the Information Technology Act, 2000. *International Journal of Science and Research (IJSR)*, *13*(4), 1444–1447. https://doi.org/10.21275/SR24421114209

Santanam, R., Sethumadhavan, M., & Virendra, M. (Eds.). (2011). *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives*. IGI Global. https://doi.org/10.4018/978-1-60960-123-2

Saxena, M. (2023). Impact of Cybercrime on E-Governance. Is Cybercrime Affecting the Confidentiality of Government Data? *International Journal of Science and Research (IJSR)*, *12*(11), 911–915. https://doi.org/10.21275/SR231111140516

Sharma, S. (2020). Issues with enforcing Mutual Legal Assistance Treaties (MLATs): Access to cross-border data in criminal investigation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3815270

Sikri, D. K. (2017). Competition law enforcement in India: Issues and challenges. *Journal of Antitrust Enforcement*, *5*(2), 163–165. https://doi.org/10.1093/jaenfo/jnx008

St.Amant, K. (2007). International Outsourcing, Personal Data, and Cyber Terrorism: Approaches for Oversight. In L. Janczewski & A. Colarik (Eds.), *Cyber Warfare and Cyber Terrorism* (pp. 112–119). IGI Global. https://doi.org/10.4018/978-1-59140-991-5.ch015

Yadav, S. (2020). Cyber Forensics: Its Importance, Cyber Forensics Techniques, and Tools. In M. S. Husain & M. Z. Khan (Eds.), *Advances in Digital Crime, Forensics, and Cyber Terrorism* (pp. 1–15). IGI Global. https://doi.org/10.4018/978-1-7998-1558-7.ch001

1.2

Appendix:

2. **Questionnaire for Cyber Crime Victim Experience**

3. **NAME:**	4. **AGE:**	5. **Email:**
6. **Mobile Number:**	7. **SEX: M / F**	
8. **Address (Optional):**		

9. **On a scale of 1-5 (1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree)**

Mark (√)

10. **Sr. No**	11. **Question**	12. **1**	13. **2**	14. **3**	15. **4**	16. **5**
17. **Section A: Incident**						
1.	I understood the nature of the cybercrime incident I experienced.	18.	19.	20.	21.	22.
2.	I was aware of the potential risks that led to the cybercrime incident.	23.	24.	25.	26.	27.
3.	The cybercrime incident caused significant disruption to my daily activities.	28.	29.	30.	31.	32.
4.	The cybercrime incident caused significant emotional distress.	33.	34.	35.	36.	37.
5.	I lost financially due to the cybercrime incident.	38.	39.	40.	41.	42.
43. **Section B: Reporting**						
6.	I knew where to report the cybercrime incident.	44.	45.	46.	47.	48.
7.	I found the process of reporting the cybercrime incident straightforward.	49.	50.	51.	52.	53.
8.	I felt supported by law enforcement during the reporting process.	54.	55.	56.	57.	58.
9.	I believe my cybercrime incident was taken seriously by law enforcement.	59.	60.	61.	62.	63.
10.	I was kept informed about the progress of my case.	64.	65.	66.	67.	68.
69. **Section C: Aftermath**						
11.	I received adequate assistance to recover from the incident.	70.	71.	72.	73.	74.
12.	I have taken additional measures to prevent such incidents in the future.	75.	76.	77.	78.	79.
13.	I am confident in my ability to prevent similar incidents in the future.	80.	81.	82.	83.	84.
14.	I feel that I've learned valuable lessons from the incident.	85.	86.	87.	88.	89.
15.	I am aware of the existing Cyber Laws and their implications.	90.	91.	92.	93.	94.
95. **Section D: Satisfaction**						
16.	I was satisfied with the response from my internet service provider (ISP) regarding the incident.	96.	97.	98.	99.	100.
17.	I was satisfied with the legal response to the cybercrime incident.	101.	102.	103.	104.	105.
18.	I believe that the perpetrators will be brought to justice.	106.	107.	108.	109.	110.
19.	I am satisfied with the support I received from my social network (family, friends, etc.) post-incident.	111.	112.	113.	114.	115.
20.	If applicable, I am satisfied with the support I received from my workplace post-incident.	116.	117.	118.	119.	120.

KEY TERMS AND DEFINITIONS:

Quantitative Analysis refers to the systematic examination of numerical data using statistical and mathematical techniques to identify patterns, relationships, and trends. It is often used to make data-driven decisions, forecast outcomes, and validate hypotheses in research and business contexts.

Digital Footprint of Cybercrime refers to the traceable digital activities and data left behind by cybercriminals during their online operations, such as hacking, phishing, or data breaches. This footprint can include logs, IP addresses, and other metadata that help in tracking, investigating, and analyzing cybercrime incidents.

Information Technology Act-2000 is a comprehensive law in India that provides a legal framework for electronic governance, cybersecurity, and the handling of electronic records and digital signatures. It also defines cybercrimes and prescribes penalties, aiming to promote secure electronic transactions and protect against cyber threats.

Confusion Matrix s a table used in machine learning to evaluate the performance of a classification model by comparing the predicted and actual outcomes. It shows the counts of true positives, true negatives, false positives, and false negatives, providing a detailed breakdown of the model's accuracy and error rates.

Multi-class classification problems involve categorizing data into three or more classes or categories, rather than just two (binary classification). These problems require algorithms capable of distinguishing between multiple distinct groups, making them suitable for applications like image recognition, speech tagging, and text categorization.

Hypothesis Testing is a statistical method used to determine if there is enough evidence to reject a null hypothesis in favour of an alternative hypothesis. It helps in making inferences about population parameters based on sample data, guiding decisions in research and data analysis.