Measurement of cybercrime severity: A victims' perspective

Binod Kumar[1]
Department of Management Studies,
Indian Institute of Technology Madras,
Chennai, Tamil Nadu, India

Saji K. Mathew
Department of Management Studies,
Indian Institute of Technology Madras,
Chennai, Tamil Nadu, India

Kandaswamy Paramasivan
Department of Management Studies,
Indian Institute of Technology Madras,
Chennai, Tamil Nadu, India

ABSTRACT

Despite the increasing incidents of cybercrimes and their impact on human society, there has been little attention on generating actionable information from cybercrimes, particularly to support investigative action. This research takes the perspective of the victim, who suffers the ultimate adverse impact of cybercrimes. Following prior research on building crime typology and severity, we first classify cybercrimes hierarchically by mapping a set of reported cybercrimes to the formal crime types defined in the Indian Penal Code, IT Act 2000 and the amendments thereof. The crime content of cybercrimes, separated from the technology, would thus give clarity of purpose to stakeholders involved in cybercrime investigation and reporting. Furthermore, we are developing a measurement process to score cybercrimes based on their severity. For this, we will conduct a study and select subjects more than 100 in numbers such as police officers, judges, and university and law students from the southern India. To validate the results, we will perform consistency checks. This process includes pilot testing, establishing baseline scores, formal scoring by various subject groups, and conducting tests for reliability and validity. In order to establish internal consistency, we use two scales, a 1-11 interval scale and a

[1] Corresponding author. ms20d010@smail.iitm.ac.in +91 9472650115

ratio scale with a standard cybercrime item for scoring. To establish validity and reliability through correlations, we engage four different subject groups related to cybercrimes. This research contributes to the IS body of knowledge in cybercrimes by developing a measurement process to generate actionable information.

Keywords: Severity, Scale, Typology, Index, Score

INTRODUCTION

While cybercrimes in the digital era pose a huge threat to humanity, law enforcement agencies face a greater challenge in responding to this category of crimes with relevant information. According to NCRB (2024), the number of reported cybercrimes in India has steadily risen from 5,693 in 2013 to 65,893 in 2022 (https://ncrb.gov.in/crime-in-india.html). In the United States, Federal Bureau of Investigation (FBI)'s Internet Crimes Complaint Center (IC3) received 351,937 reports of cyber, and computer crimes in 2018, amounting to $2,706.4 million in impact (Brunner 2020). However, the FBI admits that IC3 can only receive reports of approximately ten percent of actual cybercrime incidents, while only less than one percent of malicious cyber incidents faced enforcement action (Wexler 2014; Brunner 2020). In cybercrimes against individuals, unfamiliarity with reporting procedures, and a lack of faith of victims in successful investigations have been cited as key reasons for the lamentable under reporting, and inaction on cybercrimes (Broadhurst & Chantler 2006; Brunner 2020). There is also a lack of actionable information that could parse cybercrimes, separating cyber technology from the crime itself. Here technology is a tool used by one user to commit a crime against another technology user (Brunner 2020). In this setting, information to law enforcement agencies on the severity of crimes in cybercrime incidents becomes critical for capacity building to direct resources for action.

In the absence of the capacity to handle cybercrimes, law enforcement agencies often resort to the financial value involved in a cybercrime to determine if an action is required (Johnson et.al. 2020). Wexler (2014) reported that often federal agencies focus on cybercrimes involving high value monetary loss while ignoring low value loss cases. Subsequently, low level offenders continue to commit cybercrimes without facing much legal challenges. Although such measures simplify decision making, neglecting the real impact of cybercrimes on the victims could amount to throwing baby with bath water. In fact, cybercrimes can have much higher impact on the mental health of individuals, which is difficult to quantify (Kerr et al. 2013). It is also known that the criminal actions of the offenders can have more than one effect on a victim. For example, in Predatory Loan Mobile Application (Aggarwal et.al. 2024) that resulted in the suicide of more than 50 people, extortion by cybercriminals led to injury (mental) and monetary loss. The psychological consequence of the cybercrime could be much higher than the monetary loss involved. Further, the psychological impact also depends on how rich or poor the victim is (Kahneman 2011; Borwell et al. 2022). Hence, using financial value of cybercrimes to base investigative decisions, without a clear understanding of cybercrimes and their severity could be highly flawed.

Prior studies have developed cybercrime typologies predominantly based on the nature of the offense, and the technology involved (e.g.: Jamatkhana et al. 2014; Borwell et al. 2022). Additionally, certain literature explores the impact of cybercrimes on users only considering the monetary loss while ignoring the broader impact of cybercrimes on the victim. Hence, it is imperative to classify cybercrimes based on their diverse impact on victims covering aspects of physical and psychological injury, property loss, and property damage. Crime classification in the US began in the 1920s, with Uniform Crime Reporting (UCR) published by the FBI. Subsequently Sellin & Wolfgang (1964) developed a classification scheme for juvenile delinquency, which followed a scientific approach to indexing each crime with a numeric score. Currently the US government has moved to National Incident Based Reporting System (NIBRS), to address the limitations of UCR. To the best of our knowledge, such a classification scheme for cybercrimes based on their impact on victims still has not received due attention in academic research, despite the crucial role such information could play in cybercrime investigative decisions. In order to address this critical gap, we framed the following research objectives: (a) developing a typology of cybercrimes based on victim's perspective (b) mapping the cybercrimes to corresponding crimes as defined in the Indian Penal Code (IPC), and the Indian Information Technology Act 2000, and their amendments thereof (c) measuring the severity of cybercrime after mapping?

Our study follows the scientific scale development process developed by Sellin & Wolfgang (1964), which has been widely referenced to develop crime severity indices in several countries like USA, England, Germany, France and others European countries. This will involve a pilot test to establish the validity of a scale, followed by severity scoring of formally reported cybercrimes by expert groups. We will use two different scales: an interval scale of 1-11, and a ratio scale with a standard cybercrime reference, and score them by multiple subject groups. This will enable us to establish the validity and reliability of the scoring system through correspondence.

The remaining part of the article is organized as follows: The Literature Review section reviews relevant research, followed by Research Design section outlining the procedures we will follow for our study, including selecting subjects to score offenses, determining the types of scales to be used, and conducting the pilot study. The Data Analysis section describes how we will analyze the data for establishing reliability, and validity of the study. Finally, we conclude the paper with future directions.

LITERATURE REVIEW

Cybercrimes have evolved significantly, varying based on the perspectives of both observers and victims, and the geographical development of computer-related offenders (Gordon & Ford 2006). Cybercrimes are committed in the internet as well cyberspace covering the interconnected landscape of the networked systems (Jahankhani et al 2014; Saleem et al. 2022). Cybercrimes could be committed against individuals, organizations, and nations (espionage). The Council of Europe's Cybercrime Treaty defines "cybercrime" as offenses ranging from criminal acts against data to content, and copyright infringement (Krone 2005). Zeviar-Geese (1997) proposes a broader definition, encompassing offences that impact both individuals, and organizations, with a range of activities like fraud, unauthorized access, child pornography, and cyberstalking.

Cybercrime is analyzed through Routine Activity Theory (RAT) and Rational Choice Theory (RCT). RAT suggests that crime occurs when motivated offenders find suitable targets without capable guardians. This aligns with RCT, where individuals weigh benefits against risks when deciding to engage in illegal activities. While Capeller highlights cyberspace's distinct nature (Capeller 2017), Grabosky argues that virtual criminality resembles traditional crime (Grabosky 2017). Leukfeldt and Yar (2016) critique RAT's application to cybercrime, citing complex targets and virtual world dynamics (Yar 2005). However, Miró-Llinares (2011) and Reyns et al. (2011) defend RAT's relevance in cyberspace, emphasizing convergence possibilities. A recent review has highlighted the absence of guardians in the cyberspace as a major reason that explain the growing incidents of cybercrimes, particularly on the social media (Kumar & Mathew 2024). Borwell et al. (2022) reported the significant impact of cybercrimes on victims, yet victims being often unfairly blamed for their own victimization. This paradox leads to blaming the victim instead of addressing the cybercrime.

Crime classification and severity

There are two classifications of crimes developed in the United States, which are applicable to traditional forms of crimes, and are widely used (Sellin & Wolfgang 1964; Douglas et.al. 2013; Brunner 2020). The first, known as the Uniform Crime Reporting (UCR), was developed in 1920's by the FBI. The FBI classified crimes based on the list of crimes frequently reported at police stations. It consists of two crime categories: Part I cover crimes that are frequently reported to the police, including seven types referred to as "Index" crimes, which are considered serious. These include Criminal Homicide, Aggravated Assault, Robbery, Forcible Rape, Burglary, Larceny, and Auto Theft. Part II includes offences other than Part I. The Uniform Crime Reporting transitioned into the National Incident Based Reporting System (NIBRS) in January 2021 (https://www.bjs.ojp.gov/national-incident-based-reporting-system-nibrs). NIBRS mapped the cybercrime cases to offenses like trespass, fraud and among others, while classifying cyberspace for the classification of cybercrime (Tsakalidis & Vergidis 2017). Critics argue that the methods are insufficient for understanding cybercrime due to potential inconsistencies in reporting (Brunner 2020).

The second typology of crimes was developed by Sellin & Wolfgang (1964) to address juvenile delinquency. Based on the crime data provided by Philadelphia Police Department of USA, the Scholars developed a model for classification of delinquency, consisting of two major crime types, Class I and Class II. Class I consists of three major crimes: A. Physical injury, B. Property loss through theft, and C. Property damage. Class II crimes consist of other seven crime types (D-J). They also developed numeric index of severity for each type of crimes through a detailed scale development, data collection and scientific validation process. In this work, 141 crimes types were identified by permuting different crimes that occur among the A, B, C types of Class I, using data from recorded crimes. The US National Survey of Crime Severity also estimated seriousness of complex crimes by employing a magnitude estimation technique, but this method is considered less practical (Parton et al. 1991). In order to accurately assess the severity of cybercrimes, a typology of cybercrimes based on their impact is imperative.

Cybercrime classification and severity

Prior research has examined different classifications of cybercrimes, based on their criminological, technological and the financial aspects (Kumar & Mathew 2024). For example, a recent review of cybercrimes in social media has classified them from a criminological perspective (Faust & Tita 2019). Another recent review of cybercrimes by Drury et al. (2022) provided a typology of cybercrimes, focusing on cybercrime detection technology. Others explore the impact of cybercrimes on users considering the monetary loss (Jamatkhana et al. 2014; Borwell et al. 2022). However, these studies do not sufficiently address the broader impact of cybercrimes on victims which involves physical and psychological harm, property loss, and property damage in addition to monetary loss (Attrill-Smith & Wesson 2020; Ignatuschtschenko 2021; Gupta & Mata-Toledo 2016). Kumar and Mathew (2024) reported that physical or external harm is associated with harmful coping mechanisms, such as smoking, alcohol consumption, and even suicide, while internal or psychological harm results in issues like depression, anxiety, and mental disorders. Cybercriminals not only disrupt the physical and psychological well-being of victims but also instill fear among them. Agrafiotis et al. (2018) identified five broad categories of harm caused by cybercrimes: physical or digital harm, economic harm, psychological harm, reputational harm, and social and societal harm. Cybercrimes affect not only the victims but also their perception of interpersonal relationships and overall well-being (Cheng et al., 2020; Das & Nayak 2013; Brands & Van Doorn 2022). Borwell et al. (2022) emphasized the psychological and financial impacts of cybercrime on victims. For instance, in the case of online banking, victims of fraud or individuals aware of such incidents often experience trauma due to financial loss and the breach of personal information. This can result in significant psychological effects, including intense fear (Lestari et al. 2024).

The evaluation of cybercrime severity requires assessing the seriousness of the crime. The severity of a crime is defined as the level of harm or potential harm caused by a criminal act. Crime severity is traditionally measured based on the extent of financial or physical harm (Felson et al. 1999; Galvin & Safer-Lichtenstein 2018). Harm is closely connected with breaking norms, and negative feelings evoked (Schein & Gray 2018). Kidd's (1979) model, often referred as the labeling theory is a relevant approach when society labels certain behaviors as deviant or wrong, and individuals who engage in those behaviors internalize these labels for the crime. According to the Theory of Dyadic Morality (TDM), criminal acts are judged based on three factors: norm violations, negative emotions, and, perceived harm (Schein & Gray 2018). This harm is dyadic, where an intentional agent inflicts damage on a vulnerable party.

Prior studies have reported contextual relations between perceived severity of cybercrimes, and cybercrime reporting behavior. When actors in the cyber space identify a behavior as deviant, they may attempt to report the cybercrime, which relies on the perceived seriousness of the offense. Reporting of the cybercrime may involve significant physical harm or financial loss, and there is a greater social inclination to report financial fraud externally. This is particularly relevant when victims are organizations, and they do not want to lose reputation, especially when the perceived seriousness of the crime is high, irrespective of the presence of a financial incentive (Andon et.al. 2018; Borwell et al. 2022). If the crime is severe, victims are more likely to report it themselves. Felson et al. (1999) conducted a survey investigating how the victim's relationship to the offender influences reporting of assaults to the police, either by the victim or third parties (guardians). Their findings indicate that while the offender-victim relationship affects third-party reporting, it does not notably impact victim reporting. Gottfredson & Gottfredson (1988) report that the process of reporting a witnessed crime assumes that bystanders make logical decisions. They further assess the relationship of reporting decisions to how unusual the event is considered, how to explain it, take personal responsibility, and weigh the costs and benefits of taking action. An accurate measure of how seriously society views various cybercrime events would greatly aid cybercrime lawmakers, policymakers, and law enforcement agencies (Brunner 2020). It could also help determine suitable penalties, and sentencing practices, as well as guide the allocation of limited justice resources (Wolfgang 1985). Selling & Wolfgang (1968) recognized this potential while developing a measurement scale for delinquency. In the same way a severity score for cybercrime could offer several potential applications.

Our review of literature, though not exhaustive, shows scarcity of studies addressing the classification based on the impact of cybercrimes on victims, and a scale to measure severity of cybercrimes. As in the case of crimes other than cybercrimes, judicial services, public administrators, and social scientists acknowledge the need for clear, and accurate methods to classify, and prioritize cybercrimes. Without such measures, determining the level of cybercriminal activity, and evaluating the severity of cybercrimes remain challenging. In this context, we identify two critical gaps in the cybercrime knowledge space, which has huge implication for practice: a typology of cybercrimes based on the impact of the crime on the victim and a numeric score of severity that could be used to compare cybercrimes. Both the critical gaps motivate us to conduct the study for measure the severity of cybercrime from victim perspective. Research design section below describe detailed about the methodology need to follow to conduct the study. This section address of first research question

RESEARCH DESIGN

The purpose of our research is to develop a typology of cybercrimes based on credible historical data, which is mapped to a standard crime classification system (e.g.: Sellin & Wolfgang 1964), and in turn to IT Act 2000 and the Indian Penal Code (IPC). We further propose to develop a scoring system that will represent cybercrime severity, statistically validated. We follow Sellin & Wolfgang (1964) for methodology (for the survey and data collection, as well as for scale development) , and contextualize to the Indian cyber space by mapping a sample set of cybercrimes to one or a permutation of crimes listed in the IPC and the IT Act 2000. We will use the following offence categories for mapping cybercrime offence (Sellin & Wolfgang 1964; Attrill-Smith & Wesson 2020; Ignatuschtschenko 2021; Gupta & Mata-Toledo 2016; IT Act 2000; Kumar & Mathew 2024): (a) physical injury, (b) adverse psychological impact, (c) property loss, (d) device espionage (IT Act 2000), and (e) social consequences (loss of reputation, stigma, isolation, or strained relationships with family, friends, or colleagues), (f) emotional sufferings, and (g) loss of trust (victims may lose trust in others, including institutions, authorities, or even themselves, as a result of the crime). Here we consider the immediate impact of cybercrimes on the victims, and do not consider long term and potential secondary effects. This section address our second research question.

After the typology is established, the next step will involve creating an instrument or scoring system to assign scores to each cybercrime, facilitating the determination of their severity. This process will aid in indexing cybercrimes, subsequently assisting in assessing their severity. This will be accomplished in two steps: (a) conducting a pilot study to score cybercrime severity on two scales by select subject groups, and (b) establishing reliability and validity of the instrument. Fig (1) provides an illustration of the proposed scale development methodology.

Data source and Subject selection

In order to establish a credible source of reported cybercrime incidents, we refer to the First Information Reports (FIR)s available online (at https://eservices.tnpolice.gov.in/CCTNSNICSDC/CitizenFIRView?0). We downloaded 80 FIRs filed during 2021-2024 (2 years), which are recorded in the vernacular language of Tamil (Tamil Nadu Police. 2024). We subsequently employ the help of a Tamil-English translator to identify the subset of twenty cybercrime FIRs from the FIRs. The number of cybercrimes that can be used for our study was identified in consultation with a senior police official, who was aware of the number of reported cases in one year, in recent times.

In order to conduct the pilot study to arrive at a baseline typology of cybercrimes, we first select a group of experts who could map the cybercrime to one or more categories of crimes in the IPC or the IT Act. We identified a group of 12 experts with minimum ten years of experience in the practice of criminal law or a role in the police department (Inspector or above). Thereafter, we conduct a Focus Group Discussion (FGD) by presenting descriptions of each cybercrime, derived from an analysis of data from FIRs using qualitative content analysis to identify recurring patterns. Experts are then formally asked to provide their opinions on the appropriate mapping of the cybercrime to the relevant crime types in the IPC or the IT Act 2000. During the FGD, the experts will discuss and evaluate these mappings. A consensus will be reached through iterative discussions, and any disagreements will be resolved by a majority vote. Finally, we document the rationale for the mapping.

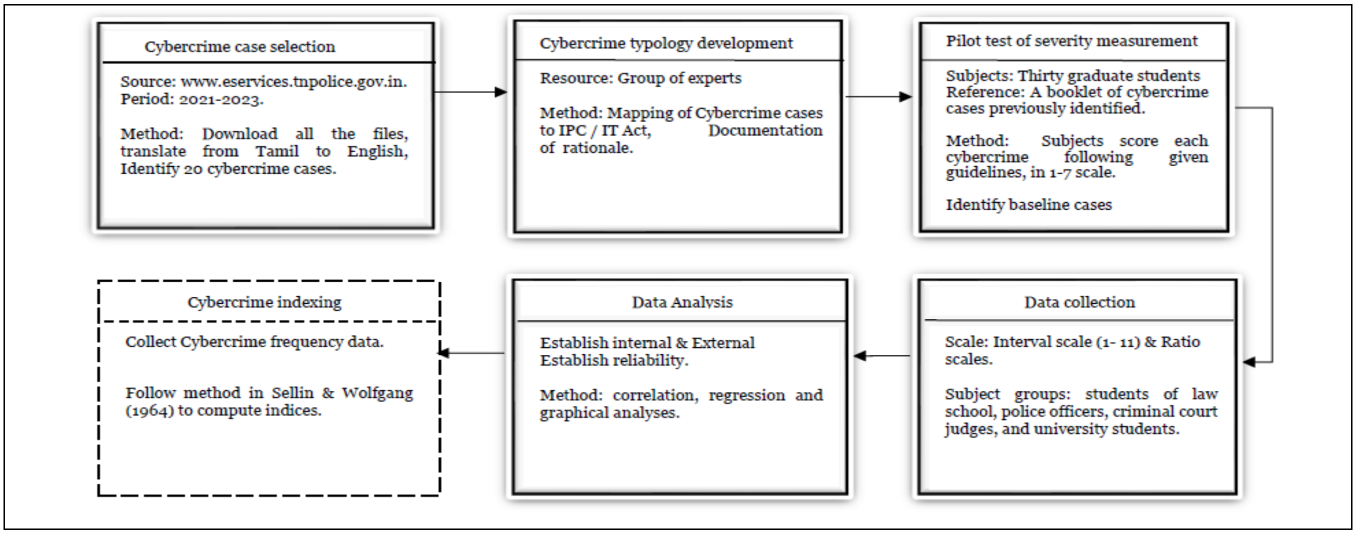
Cybercrime case selection
Source: www.eservices.tnpolice.gov.in.
Period: 2021-2023.
Method: Download all the files, translate from Tamil to English, Identify 20 cybercrime cases.
Cybercrime typology development
Resource: Group of experts
Method: Mapping of Cybercrime cases to IPC / IT Act, Documentation of rationale.
Pilot test of severity measurement
Subjects: Thirty graduate students
Reference: A booklet of cybercrime cases previously identified.
Method: Subjects score each cybercrime following given guidelines, in 1-7 scale.
Identify baseline cases
Data collection
Scale: Interval scale (1- 11) & Ratio scales.
Subject groups: students of law school, police officers, criminal court judges, and university students.
Data Analysis
Establish internal & External
Establish reliability.
Method: correlation, regression and graphical analyses.
Cybercrime indexing
Collect Cybercrime frequency data.
Follow method in Sellin & Wolfgang (1964) to compute indices.

Figure 1 The proposed scale development methodology

Following the identification of 20 cybercrimes, and their mapping to formal crime types, we prepare one booklet for each of the cybercrimes, which contain the details of the cybercrime as in the English translation of the FIR, followed by a scale of 1-7 to score each cybercrime, with 1 indicating least severity and 7 indicating highest severity. A group of 30 graduate students of a premier institution of engineering in Southern India will be engaged to score each cybercrime, using the booklets. This will result in 600 (thirty times twenty) scores. Following Sellin & Wolfgang (1964, p. 247), we will identify two cybercrimes for each of the seven categories of the 1-7 scale, such that the median score of the two crimes matches the midpoint of the scale value, and standard deviation is minimum for the two crimes in that category. This section addresses our third research objective.

Selection of scale

In the next stage of the study, we undertake the scoring of the cybercrimes by a larger representative community. The following subject groups have been identified for the scoring: (a) students of law school, (b) police officers, (c) criminal court judges, and (d) university students.

We have chosen two scales, namely an interval scale, and a ratio scale, to score severity of cybercrimes. These scales are expected to be interconnected in a consistent, and reproducible manner, unaffected by social influences. The interval scale has a defined lower, and upper limit, ranging from 1 to 11, with each division representing an equal distance. In contrast, the ratio scale has no predetermined upper limit, and allows for any number of values with greater than zero as the lower limit. An infinite number of discriminatory points are available for assessing any phenomenon, with each score representing a ratio of a standard cybercrime item positioned at the beginning of the scoring process. The placement of this standard item can be any number, and will be determined with the help of experts.

Prior to scoring, each subject will be informed that their identity will remain anonymous throughout the scoring process. We develop booklets for scoring offenses (Sellin & Wolfgang 1964). Some booklets are designed based on the interval scale, while others are designed based on the ratio scale. Apart from the scale, the information booklet provides instructions for filling out the booklet, examples of the interval or ratio scale, and the offenses to be judged. During the scoring process if the subject will get the interval scale, the subject will circle a number from 1 to 11 on each page to indicate the seriousness of each cybercrime, with examples provided for guidance. The first two violations will demonstrate the most (11) and least serious (1) categories, while the middle seriousness will be marked as 6. Each category represents an equal step in seriousness, and only one circle should be made per page without turning back. Subjects need not write their name on any sheets as they will not be identified. Instructions for the ratio scale will clarify that subjects should indicate how serious they perceive each violation to be, not how the law or courts might judge it. Subjects will write a number in the score box on each page, with the first violation serving as a standard item. Suppose standard item violation will be scored as a 10, then all other violations should be scored relative to this standard. For instance, a violation perceived as ten times more serious than the standard should be scored as 100, while half as serious should be scored as 5. We instruct the subjects to assess each offense based on their personal perspective rather than solely considering the legal aspect. Following the scoring of offenses, we will proceed to analyze the scores assigned by the subjects.

DATA ANALYSIS

Our measurement process follows certain established procedures for analyzing reliability, and validity (Sellin & Wolfgang 1964). First, we use two scales, one interval, and another ratio, simultaneously for scoring. This helps us test consistency of measurement by establishing correspondence between the two scales. Second, we engage four different subject groups in scoring cybercrimes using the two different scales. This enables us to test reliability to establish validity of the measurement system. We establish reliability, and validity by using correlation, and regression (slope) measures between scales and subject groups.

In our study each offense will be scored by a specific group among the four, representing an arithmetic mean in the interval scale and a geometric mean in the ratio scale. Plotting the mean values from the interval scale against the means of ratio scale is expected to reveal a function that is concave downward (Sellin & Wolfgang 1964). For instance, if the mean score for minor harm, such as stress or depression, is higher than the mean score for major harm like suicide, it will be considered an inconsistency. Since no single person will score all offenses, each subject's "field" or range will be randomly generated and limited rather than covering the entire spectrum. For instance, some subjects may only have "suicide" and "minor harm" within their range of cybercrime impact, while others will have "distress and anxiety" as the upper limit to compare with "minor harm". Therefore, to minimize differences between subjects, the following procedure will be implemented: (a) each subject's score obtained in the ratio scale for each offense will be transformed to its logarithm, (b) the transformed score for each subject will be standardized, (c) standard measure scores will be adjusted based on each subject's mean, and variance for each offense score, ensuring uniformity in scoring among all subjects.

Reliability and validity

After normalizing the score in the previous phase, we will test the consistency of the scores across scales and subject groups. If the mean, and variance of the selected groups do not deviate significantly, and exhibit a high correlation value, we will infer internal consistency. After assessing internal consistency, our next step will be to perform external consistency.

In order to ensure external consistency, our next stage will involve selecting subjects from colleges or universities who were not part of the original subject group. After selecting the subjects, our next step will be to use the same booklet that we used previously for the scoring process with some enhancement. For the purpose of establishing reliability, and external validity, some students will receive a completely randomized set of offenses in the booklet, while others will receive a partially randomized set. In essence, some subject groups will follow sequential order, while others will experience a partial random, and simultaneous presentation.

In the sequential ordering, offenses detailing monetary losses will be separated, and randomly distributed among other offenses. In the simultaneous ordering, monetary values will be presented on a single page, arranged from the least to the most value. The same approach will be applied to personal injury, ensuring consistency across sets. Our first task in analyzing the results will be to compare the sequential and simultaneous groups. The comparison will involve computing correlation between both the groups. If the correlation between the groups is high and the variability in mean scores is low, then we could conclude that the scoring system was reliable, and valid. This process will enable us to ascertain the validity, and reliability of the cybercrime severity scores.

CONCLUSION

Our research contributes to the body of knowledge in cybercrimes in the IS field by developing a measurement process for cybercrimes from a victim's perspective, to generate actionable information for stakeholders. The scoring of cybercrime severity simplifies the assessment of cybercriminal activity levels, and the severity of cybercrimes. The rise in cybercrime incidents, along with various victimization factors, highlights the necessity for precise indicators to measure cybercrime severity objectively. This, in turn, aids in initiating action by agencies concerned with law and order in the cyber world.

Despite the potential to generate useful insights to compare and act on cybercrimes, our research has certain limitations. First, as discussed in the introduction, the number of reported and documented cybercrimes are very limited. Second, we accessed only data from one single southern state of India. This will lead to generating scores for a comparatively few cybercrimes, of the order of 20-25, as compared to the 141 crimes considered by Sellin & Wolfgang in their seminal work in 1964. We aim to overcome this limitation by considering cybercrimes for two years instead of the one-year period followed in the prior work. An extension of our work will be the development of cybercrime index as in the case of other crimes. This will require access to records of the police department, to incorporate frequency of cybercrimes in computing index for each type of cybercrimes.

REFERENCES

Aggarwal, V., Aggarwal, N., Dhingra, B., Batra, S., & Yadav, M. (2024, January). Predatory loan mobile apps in India: A new form of cyber psychological manipulation. In 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS) (pp. 1918-1922). IEEE.

Andon, P., Free, C., Jidin, R., Monroe, G. S., & Turner, M. J. (2018). The impact of financial incentives and perceptions of seriousness on whistleblowing intention. Journal of Business Ethics, 151, 165–178. https://doi.org/10.1007/s10551-016-3215- 6.

Attrill-Smith, A., Wesson, C. (2020). The Psychology of Cybercrime. In: Holt, T., Bossler, A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_25

Borwell, J., Jansen, J., & Stol, W. (2022). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. Social Science Computer Review, 40(4), 933-954. https://doi.org/10.1177/089443932098382.

Broadhurst, R., & Chantler, N. (2006). Cybercrime update: trends and developments. In Expert Group Meeting on the development of virtual forum against cybercrime report (pp. 21-56). KICJP & UNODC.

Brunner, M. (2020). Challenges and opportunities in state and local cybercrime enforcement. Journal of National Security Law & Policy, 10(3), 1.

Capeller, W. (2017). Not such a neat net: Some comments on virtual criminality. In Cyberspace Crime (pp. 61-74). Routledge.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. International journal of engineering sciences & Emerging technologies, 6(2), 142-153.

Douglas, J. E., Burgess, A. W., Burgess, A. G., Ressler, R. K. (2013). Crime Classification Manual: A Standard System for Investigating and Classifying Violent Crime. Germany: Wiley.

Felson, R. B., Messner, S. F., & Hoskin, A. (1999). The victim-offender relationship and calling the police in assaults. Criminology, 37(4), 931-948. https://doi.org/10.1111/j.1745-9125.1999.tb00510.x

Ford R (2016) Fraud doubles the number of crimes. The Times, 22 July.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in computer virology, 2, 13-20. https://doi.org/10.1007/s11416-006-0015-z.

Gottfredson, M. R., & Gottfredson, D. M. (1988). Decision making in criminal justice: Toward the rational exercise of discretion (2nd edition). Plenum Press.

Grabosky, P. N. (2017). Virtual criminality: Old wine in new bottles? In Cyberspace Crime (pp. 75-81). Routledge.

Ignatuschtschenko, E. (2021). Assessing Harm from Cyber Crime. The Oxford Handbook of Cyber Security, 127-141.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In Cybercrime and cyber terrorism investigator's handbook (pp. 149-164). Syngress. https://doi.org/10.1016/B978-0-12-800743-3.00012-8.

Johnson D, Faulkner E, Meredith G, Wilson TJ (2020) Police functional adaptation to the digital or post digital age: Discussions with cybercrime experts. J Crim Law 84(5):427–450. https://doi.org/10.1177/0022018320952559.

Kahneman, D. (2011). *Thinking, fast and slow*. New Delhi: Penguin India.

Kerr, J., Owen, R., Nicholls, C. M., & Button, M. (2013). Research on sentencing online fraud offences. London: Sentencing Council.Kidd, R. F. (1979). Crime reporting: Toward a social psychological model. Criminology, 17(3), 380–394.

Kidd, R. F. (1979). Crime reporting: Toward a social psychological model. Criminology, 17(3), 380–394.

Krone, T. (2005). High tech crime brief. Canberra: Austria Institute of Criminology. DOI: 10.1111/j.1745-9125. 1979.tb01303.x.

Kumar, Binod and Mathew, Saji K., "The Dark Side of Social Networking Sites: A Review of Cybercrime Research" (2024). *PAJAIS Preprints* (Forthcoming). 25. https://aisel.aisnet.org/pajais_preprints/25

Lestari, S., Adawiyah, W. R., Alhamidi, A. L., Prayogi, J., & Haryanto, R. (2024). Navigating perilous seas: unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking. Safer Communities, 23(4), 444-464.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3), 263-280.

Miró-Llinares, F. (2011). Criminal opportunity in cyberspace: Application and development of the theory of everyday activities for the prevention of cybercrime. Electronic Journal of Criminal Law and Criminology, 13(7), 1–55.

NCRB (2024). Crime in India. The National Cybercrime Reporting Bureau. Retrieved from https://ncrb.gov.in/crime-in-india.html .

Parton, D. A., Hansel, M., & Stratton, J. R. (1991). Measuring crime seriousness: Lessons from the national survey of crime severity. The British Journal of Criminology, 31(1), 72-85.

Reyns,. B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyber-lifestyle–routine activities theory to cyberstalking victimization. Criminal Justice and Behavior, 38(11), 1149–1169. https://doi.org/10.1177/0093854811421448.

Saleem, S., Khan, N. F., Zafar, S., & Raza, N. (2022). Systematic literature reviews in cyberbullying/cyber harassment: A tertiary study. Technology in Society, 70, 102055. https://doi.org/10.1016/j.techsoc.2022.102055.

Schein, C., & Gray, K. (2018). The theory of dyadic morality: Reinventing moral judgment and redefining harm. Personality and Social Psychology Review, 22(1), 32–70. https://doi.org/10.1177/108886831769828.

Sellin, T., & Wolfgang, M. E. (1964). The measurement of delinquency. New York: Wiley.

Tamil Nadu Police. (2024). Citizen FIR View. Retrieved from https://eservices.tnpolice.gov.in/CCTNSNICSDC/CitizenFIRView?0.

Tsakalidis, G., & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(4), 710-729. DOI: 10.1109/TSMC.2017.2700495.

Wexler, C. (2014). Critical Issues In Policing Series-The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime. In Police Executive Research Forum, Washington, DC.

Wolfgang ME, Figlio RM, Tracy PE, Singer SI (1985) The national survey of crime severity. NCJ-96017. U.S. Department of Justice, Washington, DC.

Zeviar-Geese, The State of Law on Cyberjurisdiction and Cybercrime on the Internet, Gonz. J. Int'l L., 1, 119 (1997-98), available at http://www.across-borders.com.