THE NEED FOR PERIODICAL ADAPTATION OF CYBER LAWS IN RESPONSE TO EVOLVING CYBER CRIMES SUCH AS CYBERSTALKING AND REVENGE PORNOGRAPHY

Giridharan S, BBA LLB, Indian Institute of Management Rohtak

Nagarjun S, LLM, NALSAR University of Law, Hyderabad.

ABSTRACT

This research investigates how people perceive cybercrime, its causes, and ways to lessen it. According to the survey, which gathered responses from 50 participants, many individuals are not completely aware of the rules that are now in place regarding cyberspace or the gravity of crimes like revenge pornography and cyberstalking. It also draws attention to the frequent abuse of technology, such as proxy sites and VPNs. The results imply that in order to combat cybercrime, greater awareness, more stringent legislation, and more robust security measures are required. The study provides valuable insights even if it was restricted to online replies because of practical considerations. The purpose of this study is to increase awareness of the dangers people confront online and to assist in improving legal responses.

1. INTRODUCTION

The introduction of technology has created previously unheard-of possibilities for connection, communication, and information sharing in the quickly changing digital age. But along with these developments has been an increase in cybercrimes that take advantage of the weaknesses in the digital sphere. Cyberstalking and revenge pornography stand out as particularly pernicious risks to an individual's privacy, security, and well-being among the growing concerns. In this digital era, misconduct has become more commonplace. Examples of these include revenge pornography, which is the malicious sharing of intimate or explicit content without consent, and cyberstalking, which is the persistent and frequently intrusive pursuit of an individual online. The legal structures intended to combat cybercrimes must change as these crimes' breadth and complexity continue to expand.

Given the ever-changing nature of cyber dangers, it is imperative that cyber laws be updated on a regular basis. Conventional legal systems frequently find it difficult to keep up with the quick advances in technology and the cunning strategies used by cybercriminals. Thus, it is becoming increasingly necessary to review and revise current laws in order to successfully combat the subtleties of revenge pornography and cyberstalking. This research paper examines the complex factors that make it necessary to periodically evaluate and modify cyber laws in order to combat online crimes like revenge pornography and cyberstalking. It explores the difficulties brought about by these developing offenses, looks at the flaws in the present legal system, and suggests ways to strengthen the legal defense against these online threats. Society can better protect people from the negative effects of cyberstalking and revenge pornography by recognizing the dynamic nature of cyber dangers and the crucial need for legislative adaptation, therefore promoting a safer and more secure digital environment.

2. LITERATURE REVIEW

The paper, "**Cyber Crime and its Classification**[1]", written by Osman Goni, explores about the diverse problem of cybercrime in this modern world thereby highlighting the disruptive effects it has on the society. Cybercrime is carried out with the help of internet, computers and other technologies. Cyber-attacks happen throughout the world and the attacks result from a

[1] O. Goni, Cyber Crime and Its Classification, 10 Int'l J. Elec. Eng'g & Apps. (Jan.–Mar. 2022), https://www.researchgate.net/publication/373556615_CYBERCRIME_PREVENTION_AND_THE_ROLE_OF_THE_ODISHA_HIGH_COURT_LIBRARY_IMPACT_OF_A_LEGAL_USER'S_AND_THEIR_PRIVACY

wide variety of causes. It is also becoming more difficult to reduce cybercrime activities as in this modern society we are modern dependent on computer technology which ultimately results in a wide variety of cybercrime activities such as cyberstalking, Revenge Pornography and etc.

Writers In their contributions to the literature study, Dr. Debarati Halder and Dr.K. Jaishankar define cybercrimes as crimes carried out using contemporary communications networks against specific people or groups. Cybercrime has serious ramifications that include damage to media platforms, military data, and vital infrastructure. Data crimes, network crimes, and associated crimes are the categories into which the study divides cybercrime. While network crimes include unapproved access and the spread of viruses, data crimes entail the interception, alteration, and theft of information. There are many examples of linked crimes like content related crimes like cybersex, cyberdefamation, threats, computer related fraud and forgeries and aiding and abetting cybercrimes. All of these come under the domain of linked crimes.

Several cyber-crimes are discussed in the paper which includes phishing, cyberstalking, hacking, virus distributions and etc. The paper explores each category's nature and implications, emphasizing the difficulties brought on by technological abuse. Unauthorized hardware or software modification, exploitation of vulnerabilities, and access to computer systems without authorization are all covered in the section on hacking. The authors provide a comprehensive description of cybercrime, highlighting its varieties, definition, and challenges posed by people's increasing reliance on computers and the internet. The conclusion of the article emphasizes the urgent need for preventative measures to address the rising danger that cybercrimes represent, considering potential impacts on the national security, the economy, and society.

Cybercrime prevention and the role of the Odisha High Court Library: Impact of a legal user's and their privacy[2]

The abstract looks at how modernization and the Internet of Things (IoT) have affected a number of industries, including libraries. It focuses on how cybercrime has become more prevalent in India and how this has affected information security. It explores how libraries have changed in the digital era and emphasizes the difficulties brought on by online crimes including

[2] M. Karna Singh & B. Maharan, Cybercrime Prevention and the Role of the Odisha High Court Library: Impact of a Legal User's and Their Privacy, 8(4) Int'l J. Info. Movement 36 (Aug. 2023), https://www.ijim.in

phishing, theft, and fraud. To counter cybercrime, the Information Technology Act of 2000 is cited as a legislative framework.

The definition of cybercrime, its various forms, and its possible effects on library operations and the advancement of the country are covered in more detail later in the document. Because libraries handle sensitive information, particularly defense and research-related materials, it emphasizes the need for preventative measures. The importance of preventive measures including cyber laws, internet awareness campaigns, cybercrime units, and educational programs is emphasized.

The article provides libraries with specific tactics to strengthen cybersecurity, including hardware security, firewall implementation, role-based access control, and frequent data backups. It also looks at how the media, educational institutions, and law enforcement may work together to fight cybercrime and raise public awareness. User education, safe online conduct, and the application of cybersecurity measures are emphasized.

The paper examines information security precautions libraries can take to protect their networks, applications, and data. It draws a distinction between privacy and security, highlighting how crucial it is for libraries to protect user privacy while maintaining data integrity and confidentiality. It is highlighted how important libraries are in encouraging information security procedures in higher education.

Cybercrime of Present Era in Society of Asia[3]

This study paper investigates the crucial importance of cybersecurity in East and Southeast Asia, given that the internet is used extensively these days. The report emphasizes the growing threat of cybercrime and the need for enterprises, governments, and organizations to address cybersecurity weaknesses. Cultural diversity, insufficient law enforcement in some states, and a lack of regionally coordinated cyber threat tactics are among the key concerns mentioned.

The emphasis is on cybercrime as a sort of international organized crime made possible by the globalization age and the internet's role as a platform for criminal activity. The study categorizes cybercrimes, with an emphasis on crimes that target networks or devices, as well

[3] R.B. Satter & S.S. Snigdha, Cybercrime of Present Era in Society of Asia (July 2023), https://www.researchgate.net/publication/372134253_Cybercrime_of_Present_Era_in_Society_of_Asia.

as those that use technologies for illicit objectives. Notable highlights include the preference for elderly over 60 as cybercrime victims and the economic losses incurred by numerous businesses, notably healthcare, as a result of cyberattacks.

The study presents thorough information indicating the global rise in cybercrime costs and prevalence, with a focus on the fast expansion and complexity of cybercriminal operations, which frequently use social media for money. The sections address preventative techniques, digital forensics, and significant instances solved by digital forensics, emphasizing its importance in solving criminal cases such as murders and terrorism.

Law enforcement viewpoints on cybercrime are explored, addressing issues in combatting cyber threats and emphasizing the importance of worldwide collaboration and resources. A section on the present cybercrime scenario in Asia discusses the region's susceptibility as a result of its vast internet user population, highlighting the involvement of organized criminal gangs who exploit technical improvements.

Finally, the study advocates for a comprehensive and collaborative approach to addressing the developing cybercrime situation in East and Southeast Asia. It emphasizes the many hazards presented by cybercriminal activities, highlighting the need of international collaboration and the rule of law in combating the world's rising security dilemma.

3. ORGANIZATIONS UNDER STUDY FROM VARIOUS COUNTRIES THAT ARE RESPONSIBLE FOR CYBER LAWS

I. INDIA

- **Ministry of Electronics and Information Technology (MEITy):**

  Formulation: In India, MEITy is the main government agency in charge of creating laws and regulations pertaining to electronics, information technology, and cyberspace. This organization plays a major role in the creation of cyber laws and this organization is important to create and update cyber laws with respect to evolving cyber crimes.

  Implementation: MEITy supervises the application of cyber laws and makes sure that they are followed. MEITy also collaborates itself with organizations like with some government agencies to address the issue of cyber crimes effectively.

- **Cyber Crime Division of the Central Bureau of Investigation (CBI):**

  Enforcement: The main responsibilities of the CBI's Cyber Crime Division are to look into and uphold India's cyber laws It handles many important cases in cybercrime that includes hacking, financial fraud and others. This division is made so to make sure that those who brake the cyber laws will be prosecuted and justice will be served.

II. USA

- **Cybersecurity and Infrastructure Security Agency (CISA):**

  Formulation: CISA is essential to the development and recommendation of cybersecurity plans and policies for the US government. To implement a combined cyber security strategy CISA works with a group of agencies like with government agencies, private agencies and etc.

  Implementation: CISA works with key infrastructure sectors to put cybersecurity policies and procedures into action. CISA does many works like it gives resources, and does risk assessment services and it also gives advices to implement the cyber security posture of the USA in an overall manner.

- **Federal Bureau of Investigation (FBI):**

  Enforcement: One important federal law enforcement organization in the US is the FBI, which plays a major part in upholding cyber laws. It investigates and prosecutes a range of cybercrimes, including online fraud, identity theft, and hacking. In order to counteract cyber threats, the FBI works closely with federal, state, local, and international partners.

  Collaboration: To exchange intelligence, carry out coordinated activities, and efficiently handle cyber incidents, the FBI works in concert with other agencies and organizations. Collaboration with other agencies will help FBI to combat the cyber threats in an effective manner.

III. China

- **Cyberspace Administration of China (CAC):**

Policy Development: CAC is the central authority from China that is in charge of creating the nation's cyberspace policies. It actively works to create extensive rules, regulations, and standards that control several facets of cybersecurity and the internet.

Law Enforcement Coordination: In order to enforce cyber laws, CAC works with law enforcement organizations. This include dealing with cybercrimes, controlling conduct that occurs online, and making sure that organizations that operate in cyberspace follow set rules.

Regulatory Framework: The CAC is essential to the development of a framework governing topics such online content control, data protection, and the general supervision of activities conducted in cyberspace. This entails establishing guidelines to provide a safe and regulated online environment.

Supervision: CAC works in tandem with various government departments, internet service providers, and other relevant parties to supervise the execution of cyber policies. In order to preserve a stable and safe online environment, it keeps an eye on adherence to rules.

Global Engagement: To solve cross-border cyber challenges, CAC participates in international dialogues and teams up with other organizations. This entails taking part in conferences, agreements, and collaborations to advance a common knowledge of cyberspace security and governance.

IV. United Kingdom

- **National Cyber Security Centre (NCSC):**

Cybersecurity policy: The UK's NCSC is a major agency in charge of creating and revising cybersecurity policy. It creates best practices and recommendations to strengthen the vital infrastructure of the nation and guard against cyberattacks.

Risk management: NCSC is involved in the evaluation and reduction of cybersecurity threats. It offers advice to companies, government agencies, and individuals on how to strengthen their cyber defenses and handle effectively to cyber incidents.

Handling Cyber issues: NCSC is essential in handling cyber issues. It works in tandem with different organizations to control and lessen the effects of cybersecurity breaches. This entails exchanging threat intelligence, providing help with technology, and enabling a coordinated reaction.

- **Information Commissioner's Office (ICO):**

The UK's independent authority for data protection and privacy is the Information Commissioner's Office (ICO). Related to the handling of personal information ICO develops and implements rules.

Penalties and Investigations: ICO is able to look into data breaches and instances of non-compliance with data protection regulations.ICO has the power to punish companies that violates people's personal information. ICO keeps a safe and reliable digital environment.

4. RATIONALE

The rationale for researching the need for the periodic adaptation of cyber laws in response to evolving cyber crimes lies in the necessity to maintain the effectiveness and relevance of legal frameworks in the face of technological advancements and changing cyber threats. This research aims to contribute to developing adaptive and robust legal structures that can protect individuals and societies in the digital age. Also, this research speaks about the challenges law enforcement agencies face in solving cyber crime cases, the role of cyber laws, how cyber crime creates economic consequences, and the necessary precautions that internet users should take.

5. STATEMENT OF PROBLEM

From the literature review that was presented by me and from the knowledge that I gained during the research of this project; I developed some questions on this domain which I think a

person will find difficult to answer if he doesn't have a basic knowledge on this domain. These questions are covered under research questions.

While cyber laws have been created to tackle these digital crimes, the dynamic and ever-changing nature of technology creates substantial challenges. Current legal frameworks may fail to keep up with the rapid development of new internet platforms, communication methods, and privacy breaches employed by hackers involved in cyberstalking and revenge pornography. As a result of the mismatch between current laws and expanding cyber threats, there are legal gaps, enforcement challenges, and potential weaknesses in protecting individuals from the harmful consequences of these cybercrimes.

Outdated cyber laws provide significant challenges in combating the evolving world of cybercrime. As technology advances, fraudsters use new methods and techniques for exploiting legal gaps and vulnerabilities in current legislation. Old laws become weak and frequently fail to keep up with new cyber threats, restricting law enforcement's ability to investigate, punish, and deter cybercriminals effectively. Inadequate legal frameworks may fail to confront new forms of cybercrime, such as ransomware attacks, identity theft, and advanced phishing techniques. Furthermore, a lack of solid cyber laws may result in jurisdictional challenges and international legal gaps, making it more difficult to prosecute hackers across borders. Legislative frameworks must be updated and enhanced to equip law enforcement agencies with the necessary instruments to combat cybercrime, which is constantly evolving.

6. OBJECTIVE OF THE PROJECT

The objective of the project is to emphasize the imperative for a continuous and responsive evolution of cyber laws in the face of emerging cyber threats, particularly focusing on cybercrimes such as cyberstalking and revenge pornography. With the rapid advancements in technology, perpetrators of these crimes are adept at exploiting legal loopholes and leveraging the dynamic nature of the digital landscape. The project seeks to underscore the necessity for periodic adaptations of cyber laws to stay ahead of evolving cybercriminal tactics, ensuring that legal frameworks remain robust, comprehensive, and effective. By examining the challenges posed by cyberstalking and revenge pornography, the project aims to advocate for legislative reforms that address these specific cybercrimes, promoting a more resilient legal environment that safeguards individuals from online harassment and exploitation while facilitating efficient law enforcement efforts.

7. RESEARCH QUESTIONS

1. What role does user awareness and education play in mitigating the risks associated with revenge pornography and cyber stalking?

2. What economic consequences and job losses result from intellectual property crime, and how can nations collaborate to address this global issue?

3. Are there gaps in the legal framework that need to be addressed to enhance cybercrime prevention?

4. What role do cyber laws, especially the Information Technology Act 2000(ITA-2000) and its amendments, play in preventing and addressing cybercrimes in libraries in India?

5. What challenges do law enforcement agencies face in addressing cybercrimes especially like that of revenge pornography and cyberstalking, considering the rapid growth of cyber threats, and how adequate are their resources in keeping up with the evolving nature of cybercriminal activities?

8. SCOPE OF THE STUDY OF RESEARCH METHODOLOGY

8.1 RESEARCH DESIGN

In accordance with this project, the study uses both primary and secondary data. Secondary data is useful in a variety of ways in this project. It can be used to identify User awareness and education, consequences of IPC (Intellectual Property Crime), Gaps in legal framework that needs to be addressed to prevent cybercrime prevention and also about the role of the ITA-2000 in addressing cyber-crimes in libraries. The primary data is collected by floating a questionnaire and it reflects views of people regarding cyber-crime activities in modern societies, dangers that cyber-crime activities pose and also about the strategies that can be adopted to prevent cyber-crime activities.

8.2 NATURE AND SOURCE OF DATA COLLECTED

The source of data included are primary and secondary in nature. Secondary data includes the

important articles mentioned in the literature review and online resources that are mentioned in the reference. Important websites are also mentioned at the references. Primary data is collected by floating a questionnaire and people across various age groups and educational backgrounds answered it. The survey included both open ended and close ended questions. Also, Likert scale was also used in the survey.

8.3 THE QUESTIONNAIRE AND OTHER METHODS USED AND THEIR PURPOSE

The questionnaire that was used to collect response from the people is mentioned below:

1. How familiar are you with the title of cyber laws and cyber-crimes?
    - Very Unfamiliar
    - Unfamiliar
    - Somewhat familiar
    - Familiar
    - Very familiar
2. Are the problems associated with cyber crimes, such as cyberstalking and phishing are a serious issue according to you?
    - Yes
    - No
    - Not Sure
3. What are the factors according to you that contribute to the activities of cybercrime in modern societies?
    - Rapid technological advancements
    - Anonymity on the Internet

- Lack of cyber security awareness
- Inadequate cyber security measures
- Economic motivations

4. If you believe that some or other factor contributes to cybercrime activities in modern society, then mention it.

5. What are the significant dangers that cyber crimes pose to modern societies according to you?

- Leads to significant data breaches from protected websites
- Leads to the spread of false information and manipulation of public opinion, thereby impacting societal trust and cohesion
- It can lead to cyber-attacks on critical infrastructure, such as energy grids and healthcare facilities, that can have devastating consequences, impacting citizens' safety and well-being
- Cybercrime erodes public trust in institutions, businesses, and online systems, thereby impacting digital activities and transactions.
- It leads to intellectual property theft

6. If you believe cybercrime poses some or other significant danger to modern society, then mention it.

7. Mark the factors that can be adopted to reduce cyber-crime activities in modern society

- By promoting cyber-security education and awareness
- By investing sufficiently in robust cyber security measures
- By Enacting stringent cyber security laws and regulations
- By Providing Cybersecurity Training for Law Enforcement authorities

- By implementing stronger user authentication and access controls

8. If you believe there is some or other factor that can be adopted to reduce the activities of cyber-crime in modern society, then mention it

9. Mark the factors that the Government of India can work on that will reduce cybercrime activities in modern society

   - Launching nationwide cyber security awareness campaigns
   - By integrating cybersecurity education into school curriculums
   - By regularly viewing and updating cyber laws concerning emerging threats
   - By Allocating adequate resources to cybercrime units will help develop their tactics with respect to emerging cyber crimes

10. Age

    - Under 18
    - 18 – 26
    - 27 – 35
    - 36 – 44
    - 45 – 53
    - 54 – 60
    - 60 and above

11. Gender

    - Male
    - Female

- Prefer not to say

12. Educational qualification

- High school or below
- Bachelor's degree
- Master's degree and / or higher

The purpose of this questionnaire is to gain insights about the knowledge and about the personal opinions that the people have in relation to that of cyber laws and cyber crimes. This questionnaire researches about the strategies that are according to people that are useful to the reduction of cyber crime in modern societies. This questionnaire also speaks about the significant dangers that cyber crime poses in modern society.

8.4 STATISTICAL TOOLS USED FOR DATA ANALYSIS

Tables, pie charts and bar graphs are the statistical tools that were used for data analysis in this research project.

9. USER AWARENESS AND EDUCATION

User awareness and education plays a very important role in managing the risks with respect to cyber crimes like revenge pornography and cyber stalking. It has many uses like it helps in:

I. Recognizing risks:

Revenge pornography: Increased user knowledge helps individuals realize the risks and consequences of sharing sensitive information. Understanding the legal consequences and emotional toll may discourage people from engaging in such acts.

Cyber Stalking: Education teaches users to spot signs of cyber stalking, such as persistent online harassment, unauthorized access to personal information, and unwanted communication.

II. Promoting Responsible Online Behavior:

Revenge Pornography: Awareness campaigns can stress the importance of obtaining express consent before disclosing personal information. Users should be educated on the hazards and breaches of trust associated with non-consensual sharing.

Cyber Stalking: Education encourages safe online behavior, such as respecting others' privacy and refraining from intrusive activities that may lead to cyber stalking.

III. Understanding of Privacy Settings:

Revenge Pornography: To limit who may view their content, users must be informed on the privacy settings on social networking platforms and other websites. Understanding these options will assist you in preventing the illicit distribution of personal images.

Cyber Stalking: Awareness campaigns may teach users how to change their privacy settings on various online platforms to limit the amount of personal information exposed to potential stalkers.

IV. Legal Awareness:

Revenge Pornography: Users should be informed of the legal consequences of engaging in revenge pornography, as well as potential avenues for legal action. This information may act as a deterrent.

Cyber stalking: Education of cyber stalking laws and reporting procedures empowers users to take legal action against criminals, resulting in a safer online environment.

V. Digital literacy

Revenge Pornography: Revenge Pornography requires users to be technologically adept and comprehend the ramifications of publishing content online. This includes being worried about the longevity of digital data and its potential for misuse.

Cyber Stalking: Digital literacy education may teach users how to recognize and defend themselves against common cyber hazards, reducing the likelihood of being a victim of stalking or harassment.

VI. Support Resources

Revenge Pornography: Awareness campaigns can highlight victim support resources such as hotlines, counseling services, and legal assistance, fostering a sense of community and aiding those affected.

Cyberstalking: By educating users about online reporting protocols and law enforcement institutions, victims may seek help as quickly as feasible.

10. CONSEQUENCES OF INTELLECTUAL PROPERTY CRIME AND METHODS TO ADDRESS THIS ISSUE

Intellectual property (IP) crime can have major economic consequences and result in job losses at all levels. Intellectual Property (like patents, trademarks and etc), is a valuable asset for both businesses and individuals, therefore the economic impact is enormous. When these rights are violated by unauthorized use, duplication, or distribution, it can harm artists, inventors, and the economy as a whole. Some of the consequences of it and strategies for addressing them are discussed below:

I. Economic effects:

Lost Revenue: Intellectual property crime costs firms and individual's money since counterfeit or pirated products usually result in reduced sales and market share.

Impact on Innovation: Fear of IP theft may stifle innovation since firms may be afraid to participate in R&D if they believe their intellectual property is not sufficiently protected.

Damage to Brand Reputation: Counterfeit or low-quality merchandise may undermine actual brands' reputations, with long-term economic implications.

II. Strategies to address IP Crimes:

International Cooperation: To effectively combat intellectual property crime, states must collaborate on a worldwide basis. Sharing expertise, best practices, and resources can help the entire response.

Harmonized Legal Frameworks: Developing and implementing consistent and harmonized

legal frameworks across nations can help to streamline efforts to prosecute intellectual property violations throughout the world. This might involve aligning punishments and definitions for intellectual property crimes.

Increased Enforcement: Nations should make more efforts to discover, investigate, and prosecute intellectual property violations. This might include providing funds to specialized units within law enforcement groups.

11. GAPS IN LEGAL FRAMEWORKS THAT NEEDS TO BE ADDRESSED TO ENHANCE CYBER CRIME PREVENTION

There are many gaps in legal framework that needs to be addressed to enhance cyber crime prevention. Some of these gaps are:

Transnational Collaboration: Cybercrime is often transnational, needing international cooperation. There may be flaws in the coordination of legal systems between countries, hindering effective cross-border collaboration in investigating and prosecuting cybercriminals.

Jurisdictional Issues: Determining jurisdiction in cyberspace can be challenging, causing challenges in enforcing laws. Clear legal means for resolving situations involving many jurisdictions are essential to avoid legal voids.

Definition and Classification: The rapid progress of technology may supersede legal definitions and classifications of cybercrime. Legislative frameworks must be continuously revised in order to meet emerging threats.

Handling Digital Evidence: Traditional court systems cannot completely cope up with the unique challenges that digital evidence poses. There may be gaps in the procedures and standards used to collect, preserve, and present digital evidence in court.

Data Protection and Privacy Laws: The legislative framework must find a balance between preventing cybercrime and protecting individuals' privacy. Gaps in data protection regulations may allow hackers to exploit them, whilst stringent restrictions may inhibit effective law enforcement.

The need for capacity building for law enforcement: Law enforcement officials may lack the information and the necessary resources that are needed to adequately investigate and prosecute cybercrime. There might be gaps in training programs and tools to stay up with growing cyber threats.

Corporate and Government Cooperation: Effective collaboration between the public and private sectors is required. Legal frameworks may need to be strengthened to promote information exchange and collaboration between government agencies and private organisations, hence strengthening overall cybersecurity.

Punishments and Deterrence: Some legal systems may lack the required consequences to effectively deter cybercriminals. Improving the legal consequences for cybercrime can act as a deterrent and assist to fill gaps in the current legal system.

International treaties and agreements:

Strengthening and updating international treaties and agreements on cybercrime can help to ensure a more coherent and coordinated global response. Gaps in such agreements may cause delays in the extradition of cybercriminals or the transmission of sensitive information.

12. ROLE OF THE ITA-2000 IN ADDRESSING CYBER CRIMES ESPECIALLY IN LIBRARIES IN INDIA

Legal framework for cyber-crimes: The Information Technology Act of 2000 offers a legal framework to address a wide range of cybercrimes, including unauthorized access, hacking, data breaches, and the dissemination of malicious code. Subsequent updates expanded the Act's scope and effectiveness.

Data Protection and Security: The Act includes provisions for data protection and security. Libraries routinely handle sensitive user information, and the legal framework ensures that proper security measures are adopted to secure this data, reducing the risk of unauthorized access or data breaches.

Electronic authentication: Libraries may use electronic authentication methods to get access to digital resources and services. The Information Technology Act creates a legal framework

for electronic signatures and authentication to ensure the integrity and validity of electronic documents.

Liabilities for Cybercrime: The Act provides liability for certain cybercrimes, holding individuals or businesses accountable for infractions such as unauthorized access to computer systems, data theft, or tampering with computer source code. This helps to prevent potential hackers from entering or attacking libraries.

Cyber security measures: Libraries should take cybersecurity safeguards to secure their digital infrastructure. The Act creates a legal framework for the implementation of security practices and standards, which reduces vulnerabilities and improves overall cybersecurity.

Legal Recognition of Electronic Records: The Act recognizes the legality of electronic records, such as digital documents and transactions. This is significant for libraries, which increasingly rely on digital resources and electronic documentation.

Offenses and punishments: This Act outline certain cybercrime offenses and sets penalties for those found guilty. This acts as a deterrent and provides a legal basis for penalizing people who engage in activities that impair library systems or data.

Changes for addressing growing risks: Subsequent revisions to the IT Act addressed increasing cyber dangers and challenges. These updates ensure that the legal framework remains current and effective in combating new kinds of cybercrime that might harm libraries.

Digital Signatures: The Act makes digital signatures more accessible, which is critical for libraries that handle electronic transactions. Digital signatures provide a secure, legally binding method of authentication and permission.

13. CHALLENGES FACED BY LAW ENFORCEMENT AUTHORITIES IN ADDRESSING CYBER-CRIME ISSUES AND THE ADEQUACY OF THEIR RESOURCES IN COMPARISON TO THAT OF THE EVOLVING NATURE OF CYBER-CRIME ACTIVITIES

Law enforcement agencies face several challenges in fighting cybercrimes, particularly in cases of revenge pornography and cyberstalking, as a result of the sharp increase in cyberthreats.

These challenges are made worse by the dynamic nature of cybercrime activities. Some of the key challenges and considerations are:

Challenges

Anonymity and Pseudonymity: People who perpetrate cybercrimes like revenge pornography and cyberstalking frequently use online anonymity or pseudonymity. Locating and locating persons engaged in these kinds of operations may prove to be difficult.

Underreporting: Victims of revenge pornography and cyberstalking may be unwilling to disclose occurrences due to privacy concerns, social stigma, or ignorance. This underreporting makes it challenging for law enforcement to address the full scale of the problem.

Encryption: The use of encryption by criminals may obstruct investigations since it protects communications and data from unauthorized access. Decrypting secure communications is a significant difficulty for law enforcement.

Resource Constraints: Law enforcement organizations may have limitations in their human, financial, and technological resources. The cost of acquiring and maintaining state-of-the-art cybersecurity methods and systems may put a strain on budgets.

Legislative Gaps: It is possible that certain nations lack the sophisticated legal structures necessary to address emerging forms of cybercrime. These gaps make it more challenging to properly prosecute cases.

Adequacy of Resources

Education and Training: Law enforcement officials' ability to combat cybercrimes can be enhanced by adequate instructional programs. It is essential to keep up with the latest developments in cyberthreat research.

Investment in Technology: Money needs to be set aside for state-of-the-art cybersecurity methods and equipment in order to stay ahead of hackers. Software and hardware need to be updated on a regular basis.

Legislative Reforms: If laws are routinely updated to reflect new types of cybercrimes and

provide clearer instructions, law enforcement authorities will be better prepared to confront cyber threats.

International collaboration: By strengthening their international collaboration through agreements and partnerships, law enforcement agencies may more effectively coordinate their operations and combat cross-border cybercrimes.

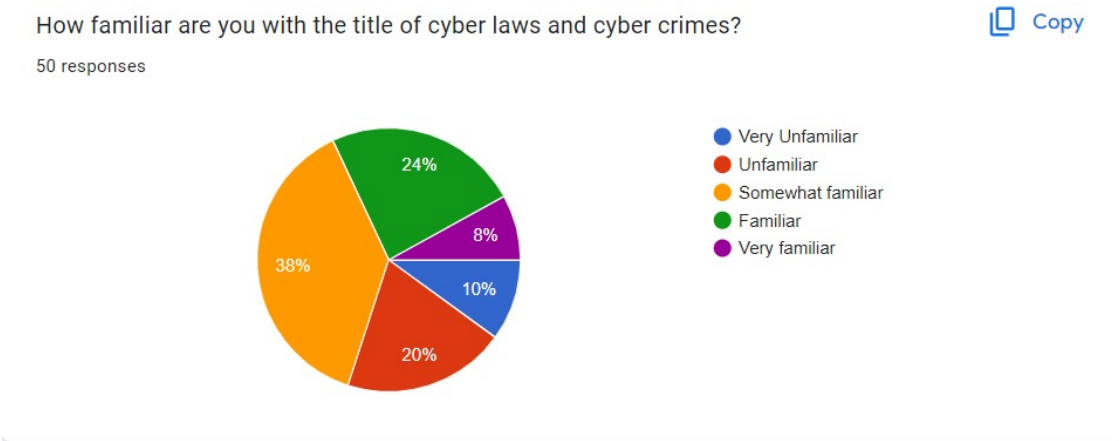
14. DATA INTERPRETATION AND FINDINGS

I conducted a survey by floating a questionnaire and people across various age groups and educational qualification answered it.

Response of those findings:

No of respondents: 50

1.



- Below is the breakdown of the familiarity of the people with cyber laws and cyber crimes:

  - 38% of respondents said they are very familiar with the title of cyber laws and cyber crime.

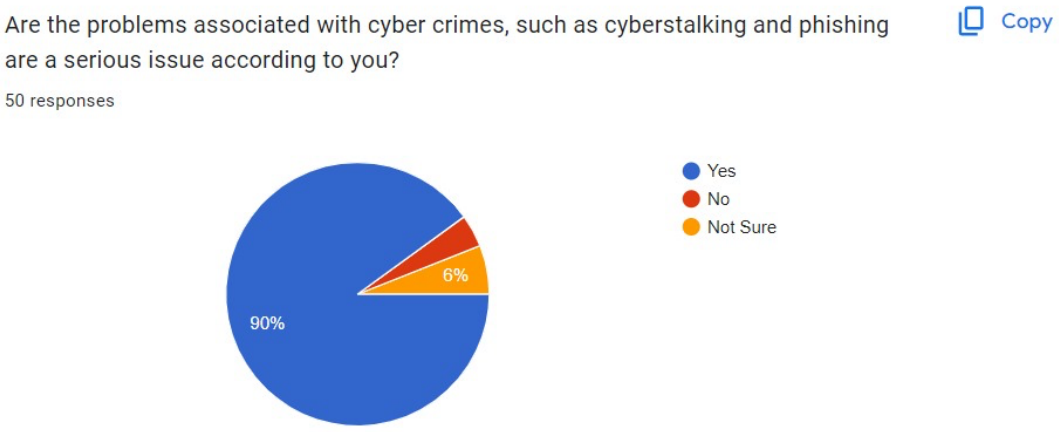
  - 20% of respondents said they are somewhat familiar.

  - 10% of respondents said they are familiar.

- 24% of respondents said they are unfamiliar.
- 8% of respondents said they are very unfamiliar.

This suggests that a majority of people (58%) have at least some familiarity with the titles of cyber laws and cyber crime, but a significant minority (32%) are unfamiliar or very unfamiliar.

2.



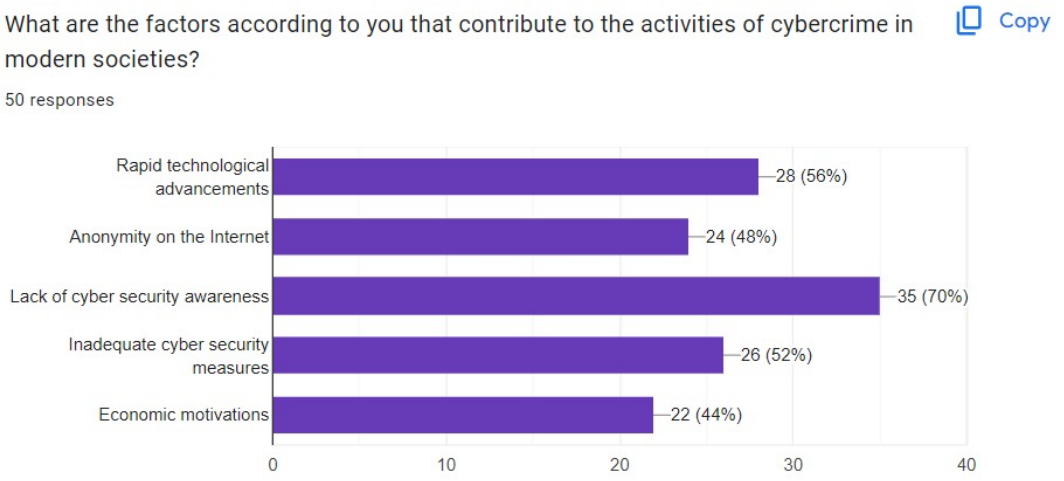
- From this question whether cyber crime is a serious issue or not, we can see the breakdown of the results:
  - 90% of the respondents answered yes
- 6% of the respondents answered no
- 4% of the respondents answered not sure.

There are a few possible reasons why such a high percentage of respondents believe cyber-crimes are a serious issue:

Growing public awareness of cybercrime: The media has regularly portrayed cybercrime as a serious threat, and it has attracted attention in recent years. This may be the reason why people are more concerned about cybercrime now than they were in the past.

Personal experience: Many people have been directly harmed by identity theft, fraud, and other types of cybercrime. Because of this, people might be more likely to consider cybercrime to be a serious issue.

3.



This graph shows the factor according to the people that contributes to cybercrime in modern societies. The findings are:

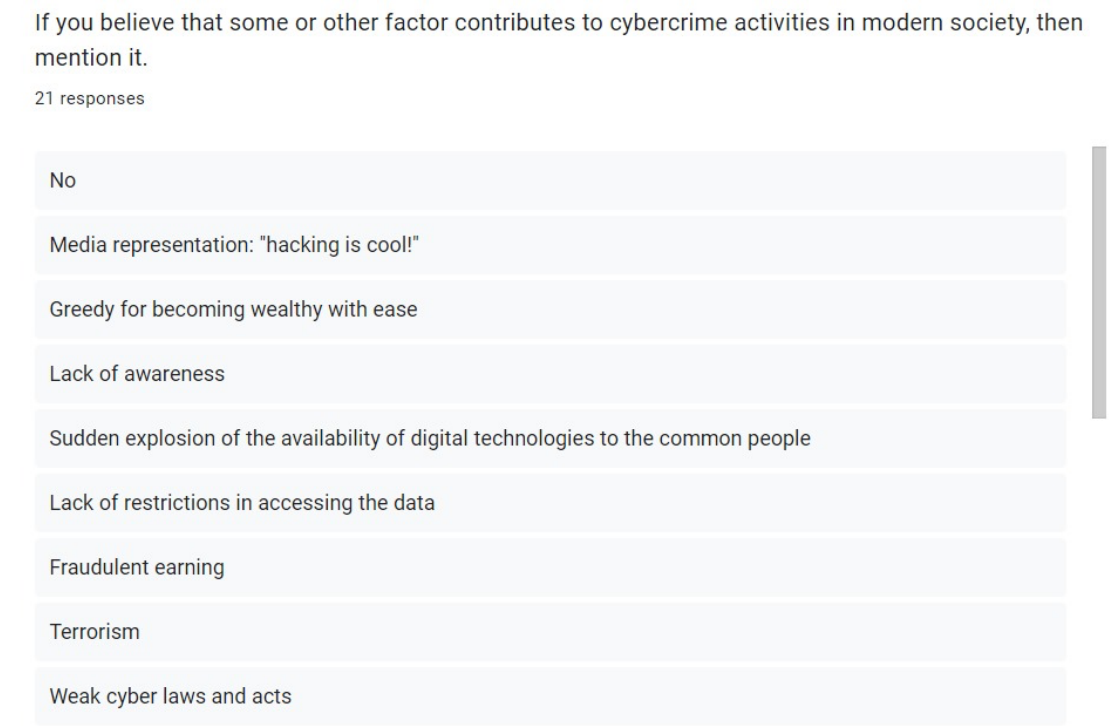
- A major contributing factor to cybercrime, according to 70% of respondents, is a lack of knowledge about cybersecurity.
- According to 56% of respondents, the rapid advancement of technology is one of the primary reasons behind cybercrime.
- Inadequate cybersecurity measures are one of the primary reasons of cybercrime, according to 52% of respondents.
- 48% of respondents said that anonymity on the internet is a major factor in cybercrime.
- Of the participants, 44% believe that financial incentives are a major contributing factor to cybercrime.

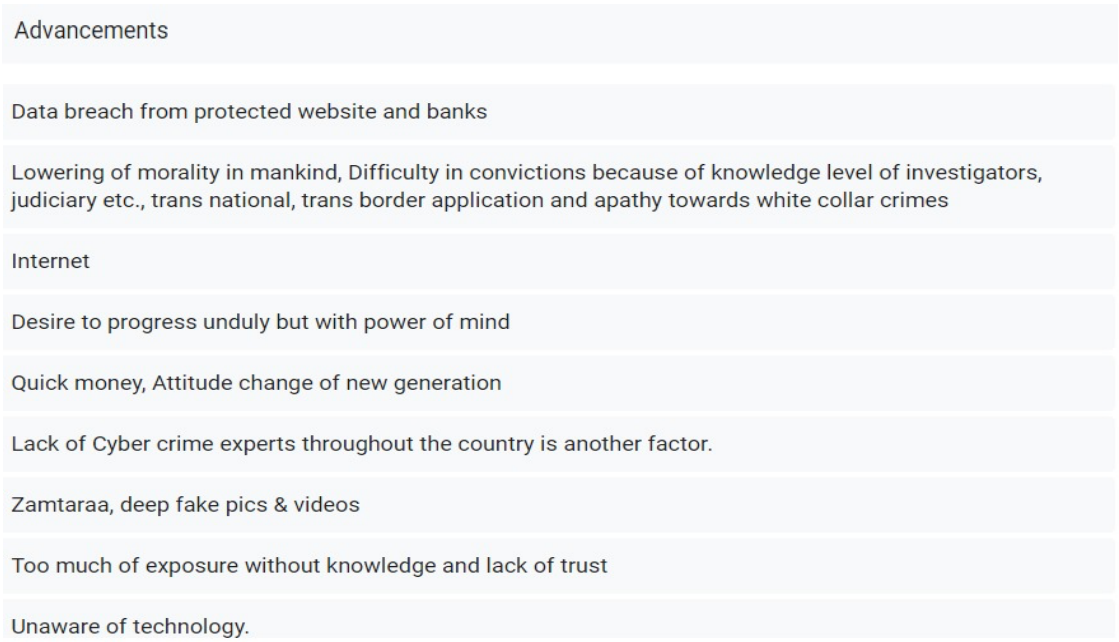
There are a number of reasons why people might have responded in this way:

Lack of awareness on cybersecurity: It's probable that a large number of people are uninformed about the risks associated with the internet activities and how to protect themselves from it. This could make them more vulnerable to cyberattacks.

Quick developments in technology: Rapid advancements in technology have made it possible for thieves to exploit new vulnerabilities. As such, it could be harder to stay up to date on security issues.

4.





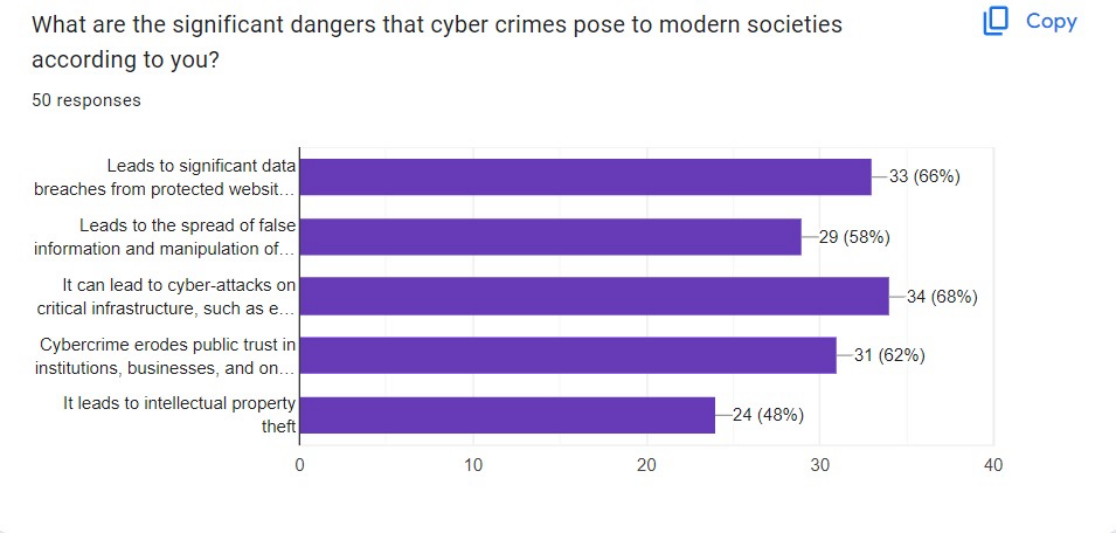
This is an open-ended question and this image of the survey speaks of the factors that the people think that it contributes to the activities of cyber-crime in the modern society. The factors mentioned above are all mentioned by distinct respondents as this was not a compulsory question. That is each and every 1 of the factor mentioned above was typed down by distinct respondents. The summarized findings of the factors that contributes to the activities of cyber crime in the modern societies are:

- Lack of cyber crime experts throughout the country
- Quick money which is resulting from the attitude change of new generations
- Media's representation of hacking is cool
- Lack of awareness among people
- Sudden explosion of the availability of digital technologies to common people
- Lack of restrictions in accessing certain data's
- Weak cyber laws
- Terrorism

- Advancements of digital technology
- Availability of internet
- Lowering of morality in mankind. Difficulty in convictions because of knowledge level of instigators, judiciary etc., transnational, trans border application and apathy towards white collar crimes
- Wide availability of Internet
- Too much exposure to the internet without the awareness of knowledge and the lack of trust

The varied answers to the question of what causes cybercrime reveal a complicated interaction of technological, cultural, and societal processes. First off, ineffective cyber legislation and a dearth of cybercrime specialists point to institutional weaknesses in successfully addressing and preventing cyberthreats. This is made worse by the internet's and digital technologies' explosive growth, which has overtaken awareness campaigns and legal frameworks. Cybercriminal activity is also on the rise due to the temptation of fast money, which is fuelled by the glorification of hacking in the media and shifting views among younger generations. The issue is further made worse by the general public's ignorance of cybersecurity threats and the ease with which some data can be accessed as a result of insufficient constraints. The issue is further made worse by the general public's ignorance of cybersecurity threats and the ease with which some data can be accessed as a result of insufficient constraints. Combating cyber threats is made more difficult by the international character of cybercrimes as well as difficulties in the legal and law enforcement systems. All things considered, these differing answers highlight how complex the problem is and how, in order to effectively tackle cybercrime, a comprehensive strategy addressing technological, legal, educational, and cultural issues is required.

5.



- This graph shows the respondents of the people according to their views of the biggest dangers cybercrime poses to modern societies. Below is the summarized findings:

  - The biggest concern, in the opinion of 66% of respondents, is that it might lead to serious data breaches from secured websites. This could be the outcome of customers realizing the importance of protecting their personal data and the potential consequences of having it stolen or compromised in a data breach.

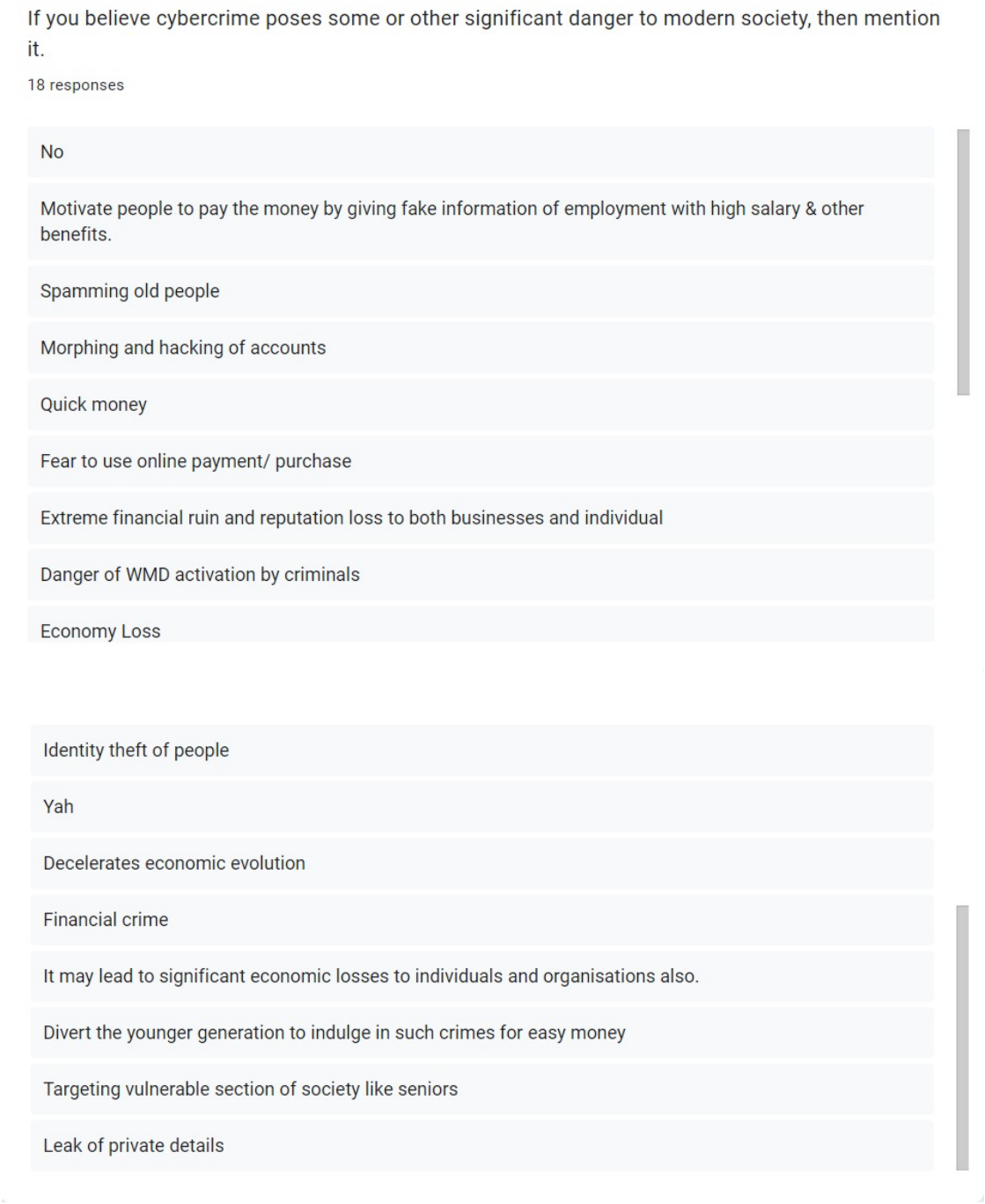
  - 58% of respondents said there was a significant chance that this would distort facts and disseminate false information. This is most likely due to growing concerns about the spread of misleading information on the internet and how it can be used to sway people's opinions and behavior.

  - 68 % of those surveyed said there was a high chance it would lead to cyberattacks on critical infrastructure, such as hospitals and electrical systems. This illustrates how cybercrime has the power to disrupt essential systems and cause significant harm.

  - Cybercrime poses a major risk to the public's trust in businesses, organizations, and institutions, according to 62% of respondents. This demonstrates that people are concerned about how cybercrime can impact society's overall sense of confidence and trust.

- Of those surveyed, 48% felt that there was a significant chance that it would lead to intellectual property theft. This presumably worries companies and organizations that rely on intellectual property to obtain a competitive edge.

6.



This is an open-ended question and this image of the dangers in the modern society that people think that the cybercrime activities posses. The dangers mentioned above are all mentioned by

distinct respondents as this was not a compulsory question. That is each and every 1 of the danger that the cyber-crime activities pose in the modern society was mentioned by distinct respondents.

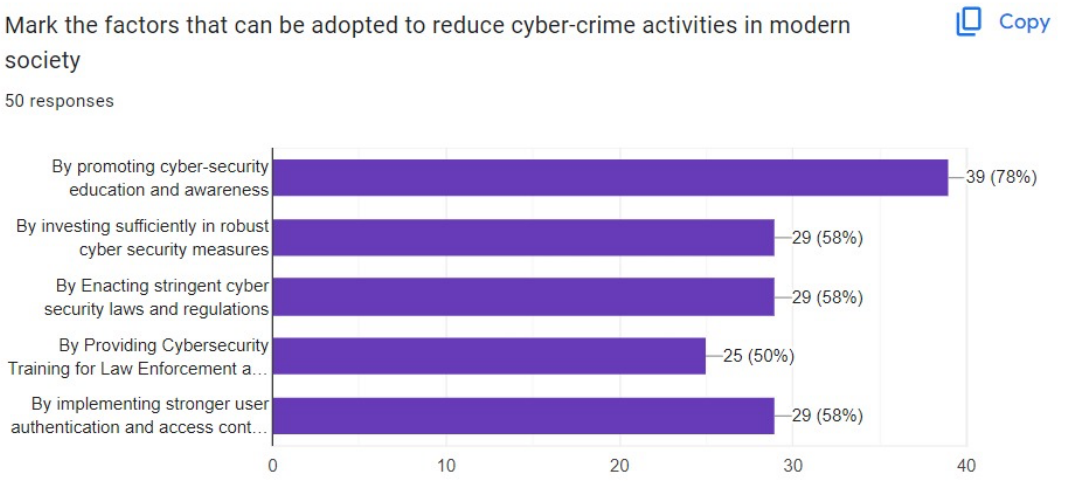
The summarized findings of the dangers are:

- Leads to the leak of private details.
- Leads to the targeting of vulnerable sections of the society like the senior citizens.
- Leads to the diversion of the younger sections of our society to fraudulent activities for easy money.
- It may lead to significant economic losses to individuals and organisations.
- It may lead to the deceleration of economic development
- It may lead to the identity theft of people
- It may lead to the danger of WMD activation by criminals.
- It may lead to extreme financial ruin and loss of reputation for both to both individuals and businesses.
- It may lead to the fear in the use of online platforms for payments / purchases.
- It may lead to the morphing and hacking of accounts.

There are various reasons for the wide range of answers to the question regarding the risks posed by cybercrime in contemporary society. First of all, because the topic was open-ended, respondents were free to freely express their opinions and worries without being limited by pre-arranged answers. Furthermore, the widespread prevalence of cybercrime in contemporary culture has probably increased people's knowledge of and prompted them to think about a wide range of potential risks linked with online activity. Each respondent may have highlighted a particular facet of the risks associated with cybercrime by drawing on their own experiences, insights, or understanding of cyberthreats. Furthermore, the respondents' varied backgrounds and demographics may have shaped their priorities and perceptions of the possible effects of

cybercrime, resulting in a wide range of responses covering topics like financial fraud, privacy breaches, societal vulnerabilities, and the threat of weaponized cyberattacks.

7.



This graph tells to us about the results of the survey according to people based on what factors they believe that can be added to reduce cybercrime activities in the modern society. Below are the summarized findings:

- According to 78% of respondents, raising public awareness and education about cybersecurity is a key component in lowering cybercrime. This is probably due to the widespread belief that one of the main causes of cybercrime is ignorance of cyberthreats and methods for protecting oneself online.

- 58% of respondents think that one important issue is making enough investments in strong cybersecurity defenses. This shows that people think that in order to make it harder for criminals to succeed, businesses and individuals should invest more in cybersecurity procedures and technologies.

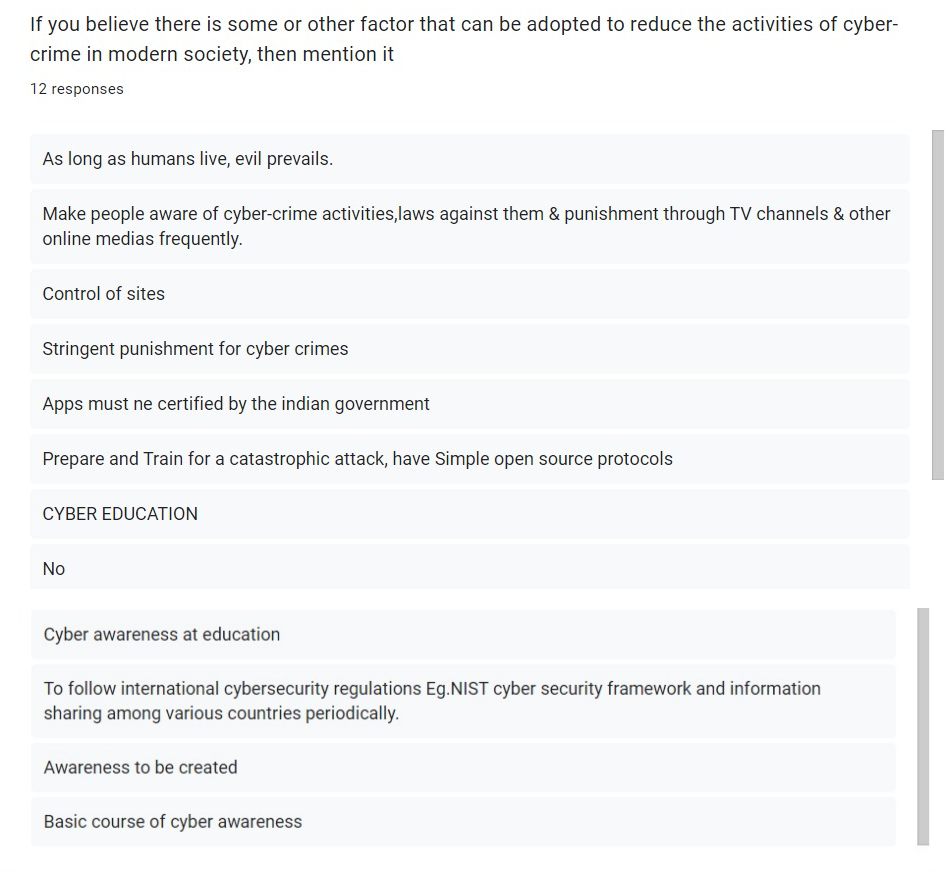
- Adopting strict cyber security laws and regulations is regarded by 58% of respondents as a significant issue. This shows that individuals think that in order to properly punish offenders and discourage cybercrime, more laws and regulations are required.

- 50 percent of respondents think that training law enforcement officials in cybersecurity is a significant impact. This shows that individuals think that in order to investigate and prosecute cybercrimes, law enforcement and judicial professionals need to be better prepared.

- Stronger user authentication and access controls are a big consideration, according to 58% of respondents. This shows that individuals think it can be harder for unauthorized users to access systems and data if there are more stringent authentication procedures and access controls in place.

People would have believed that these were the things that could have been implemented to lessen the activities of cybercrime in the contemporary society, which is why they would have replied in this way. Additionally, while people's opinions vary when it comes to determining the best element to lower cybercrime activities in contemporary society, some of these aspects are similar to one another and some of them are also very distinct from one another.

8.



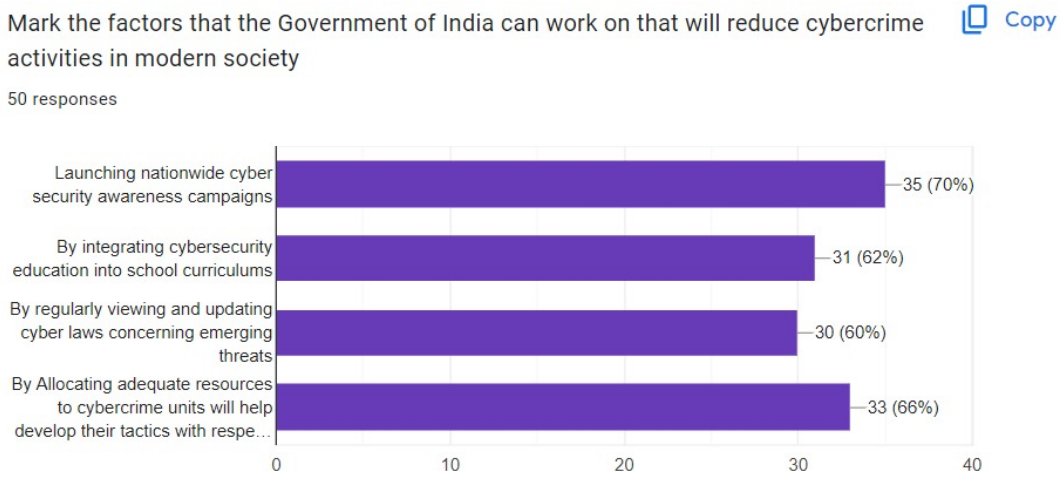
This is an open-ended question and this image of the survey speaks of the factors that the people think that can be adopted to reduce the activities of the cyber crime in the modern society. The factors mentioned above are all mentioned by distinct respondents as this was not a compulsory question. That is each and every 1 of the factor mentioned above was typed down by distinct respondents.

The summarized findings of the factors are:

- To create awareness
- To learn basic courses of cyber awareness
- To follow international cyber security regulation
- To have cyber education
- To prepare and train for a catastrophic attack and to have simple and open source protocols
- All the apps must be certified by the Indian government
- To award stringent punishment for cyber crimes
- To have control of sites
- To make people aware of cyber crime activities that are taking place, laws that can be enforced in case of any cyber crime and to deliver punishments to people who involve in cyber crime activities and to mention their identity in the news channels and social medias frequently

The reason why people responded in this manner was because people would have felt that these were the possible factors that could've been adopted to reduce the activities of cyber-crime in the modern society. Also, some of these factors are similar to each other and some of them are also very different from each other as the views of the people changes in choosing the best factor to reduce cyber-crime activities in the modern society as different people have different views.

9.



- This survey speaks about the image that shows the factors that the Indian government should work upon according to the people that should reduce the cyber crime activities. Below are the summarized findings of it:

1) **Starting national initiatives to raise awareness about cybersecurity:** 70% of respondents said this was a key influence. This may be the result of individuals realizing that one of the main causes of cybercrime is ignorance about cyberthreats and internet safety measures. Campaigns for public awareness could inform individuals about important cybersecurity best practices, such as creating secure passwords, avoiding phishing emails, and updating software.

2) **By integrating cybersecurity education in the curriculum**: According to 62% of respondents, this is a crucial component. Early education could provide kids the information and abilities they need to use the internet safely and responsibly. This might contribute to the development of a generation that is less vulnerable to cyberattacks and more conscious of cyberthreats.

3) **By routinely reviewing and revising cyber legislation in light of new threats:** According to 60% of respondents, this is an essential component. The strategies and instruments used in cybercrime are always changing, thus it's critical that laws and regulations stay up. It is possible to make sure cyber laws are successful in discouraging and penalizing cybercriminals by routinely evaluating and revising them.

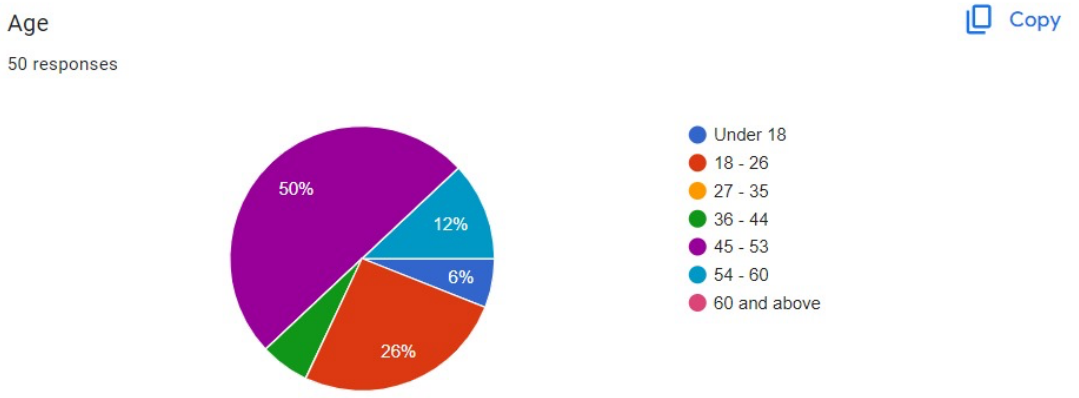
4) **By providing cybercrime units with sufficient resources:** According to 66% of respondents, this is a significant factor. To adequately investigate and prosecute cybercrimes, cybercrime units require an adequate number of personnel, finances, and technological resources. Providing enough resources can help them become more capable and increase their chances of success.

Below mentioned are some of the possible reasons that why people responded in this manner:

- **Cybercrime is becoming a bigger concern**: A significant portion of the Indian population has been directly harmed by identity theft, fraud, and other cybercrimes. Maybe as a result, they are more cognizant of the issue and supportive of remedies.

- **Wish for a safer online environment:** People who wish to feel safe and secure when using the internet may believe that the government has a duty to create a safer online environment for its citizens.

10.



- This project shows about the age distribution of 50 survey respondents. Here's a breakdown of the results:

- 12% of respondents are between 18 and 26 years old.

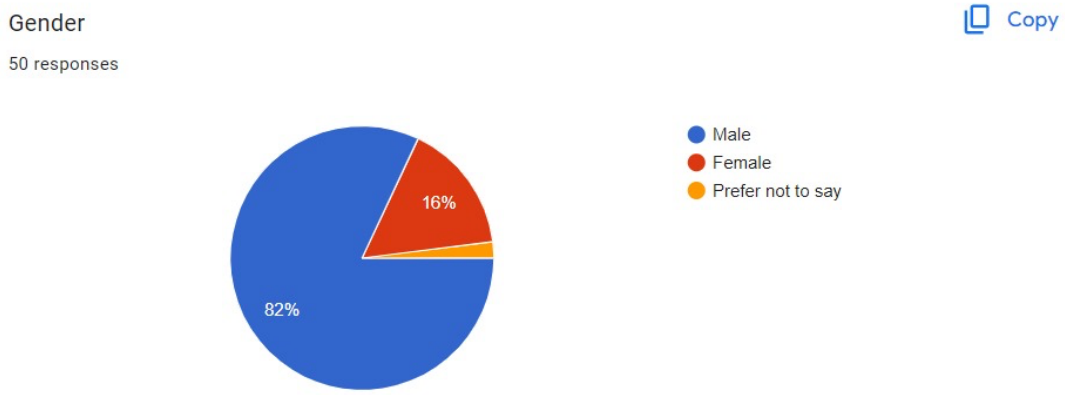
- 26% of respondents are between 27 and 35 years old.

- 6% of respondents are between 36 and 44 years old.

- 6% of respondents are between 45 and 53 years old.
- 12% of respondents are between 54 and 60 years old.
- 26% of respondents are 60 years old or above.

11.

The group is fairly evenly distributed across a wide range of ages.



Gender:

- 82% of respondents identified as male.
- 16% of respondents identified as female.
- 2% of respondents preferred not to say

Educational qualification

High School or below	10 %
Bachelor's degree	46 %
Master's degree and / or higher	44%

From the respondents:

- 10 % of them were high school students
- 46 % of them possess Bachelor's degree
- 44% of them possess Master's degree and/ or higher.

From this we can interfere that most of the respondents were undergraduate students and it is followed by Master's students and finally it is followed by high school students.

15. RECOMMENDATIONS

Recommendations for research question 1:

Comprehensive educational programs can be implemented at schools, universities, workplaces and community centers to raise awareness about the risks of cyber stalking and revenge pornography. People can arm themselves with tactics to defend against cyberstalking and revenge pornography, like utilizing strong and distinct passwords, turning on two-factor authentication, and routinely changing privacy settings. Support groups and online discussion boards can be created so that survivors can interact with other survivors, exchange resources, and, if necessary, seek out counseling or legal guidance. Children, teenagers, and adults can all get age-appropriate education that emphasizes digital literacy, online safety precautions, and the value of respecting the personal space and boundaries of others.

Recommendations for research question 2:

Enforcement procedures can be improved on a national and international scale to successfully address IP Crimes. This might entail giving law enforcement organizations enough funding, creating dedicated divisions to look into IP infringement, and enacting harsher punishments for violators. Increased cooperation and information exchange between law enforcement agencies, governments, business parties, and international organizations can help to address this problem. In order to effectively locate and prosecute intellectual property offenders we can create networks or platforms for exchanging resources, best practices, and intelligence. By ensuring these precautions we can encourage innovation and investments in the research because people will begin to feel that their intellectual properties are protected.

Recommendation for research question 3:

Entire laws that target cybercrimes can be created, with sections addressing new concerns like ransomware attacks, identity theft, revenge pornography, and cyberstalking. The laws must be made flexible enough to accommodate new criminal strategies and technological advancements. Any legal gaps that cybercriminals could try to take advantage of can be found and closed by the government and the courts. This could entail examining current legislation pertaining to cyber stalking, revenge pornography, intellectual property rights, data protection, privacy, and electronic communication to make sure they sufficiently address cybercrimes and offer precise instructions for legal action. International collaboration can be fostered to combat cybercrimes.

Recommendation for research question 4:

Cybercrime activities can be addressed in Indian libraries by offering thorough training and awareness programs to library workers regarding cyber laws, ITA-2000, and its revisions. Employees should receive training on data security, copyright rules, cybercrimes' legal ramifications, and how to handle digital property appropriately. To stop cybercrimes like hacking, data breaches, and illegal access to library systems and networks, libraries can put strong IT security measures in place. Installing firewalls, encryption programs, antivirus software, and access control devices fall under this category to combat cybercrime activities in library. To avoid unauthorized disclosure or misuse, libraries should put up policies and processes for the safe processing, storing, and disposal of user data and digital assets. India can safeguard its libraries by implementing these steps.

Recommendation for research question 5:

By providing specialized training for law enforcement officers like the training should cover digital forensics, cyber laws, victim support, and emerging trends in cybercriminal activities we can investigate and prosecute cybercrimes, including that of revenge pornography and cyberstalking. Multi-disciplinary task forces or cybercrime units can be dedicated to address the specific types of cybercrime activities like that of cyber stalking and revenge pornography especially.

Also, law enforcement agencies must be equipped with the latest technology and digital

forensic tools to effectively investigate cybercrimes. Invest in resources for digital evidence collection, analysis, and preservation are necessary to strengthen prosecution efforts against perpetrators of cyber crimes like that of revenge pornography and cyberstalking.

16. CONCLUSION

This project collected people's views regarding their knowledge of cyber crimes, their contributing factors, and the strategies that could be adopted to reduce cybercrime activities. The outcome of this project is that it would require the government to form stronger cyber laws to reduce cybercrime activities and make people aware of the various factors that contribute to cybercrime activities and the dangers that cybercrime poses in modern society. The outcome includes the improvement of legal response to cyber-crime activities. This topic should be studied as, in this modern time, there is an increased internet use, leading to new forms of cyber crimes and challenges. Cyberstalkers and perpetrators of revenge pornography often exploit new technologies and platforms, making it essential for laws to keep pace with these advancements. Although, in India, watching child pornography is illegal, many people still get access to this content with the help of proxy websites, VPNs, etc. There are reported cases that people who were in relationship threatened their ex-partners with photos or some videos of their relationship to get favors from them and failure in the compliance with them might result in the leak of those mentioned photos or videos. This research project will create awareness among the people of the dangers associated with the internet, and it will also help in the formulation of better cyber laws to combat cyber-crimes like cyberstalking and revenge pornography. By identifying the factors that cause cybercrime activities, the government can form laws to prevent these kinds of cybercrime activities. Also, this project can raise public awareness about the seriousness of cyberstalking, revenge pornography, and other related crimes.

17. LIMITATIONS

This project was completed by the usage of primary data and secondary data. Primary data was collected from people by floating a questionnaire and people answered it according to their own knowledge and it is subjective. The interview was conducted in online mode and the interview could not be conducted in physical mode due to practical limitations like expenses, difficulty in leaving the campus for conducting the interview,etc. For the case of secondary data, facts and authenticity of the information were tried to verify in possible ways. Still, there

are possibilities for some minor technical and human errors, that may be present in this project too. In further reviews, if something is in such a manner, it will be immediately corrected.

REFERENCES

- S. Das & T. Nayak, Impact of Cybercrime: Issues and Challenges, 6(2) Int'l J. Eng'g Sci. & Emerging Techs. 142 (2013)

- M.M. Azad, K.N. Mazid & S.S. Sharmin, Cyber Crime Problem Areas, Legal Areas and the Cyber Crime Law, 3(5) Int'l J. New Tech. & Res. 1 (2017)

- P. Hunton, The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model, 25(6) Computer L. & Security Rev. 528 (2009)

- G.O. Boussi & H. Gupta, A Proposed Framework for Controlling Cyber-Crime, in 2020 8th Int'l Conf. on Reliability, Infocom Techs. & Optimization (Trends & Future Directions) (ICRITO) 1060 (June 2020) (IEEE)

- J.M. Drew, A Study of Cybercrime Victimisation and Prevention: Exploring the Use of Online Crime Prevention Behaviours and Strategies, 6 J. Criminological Res., Pol'y & Prac. 17 (2020)