Tackling Cyber Crime Against Women in India: An Effort to Build a Resilient Society

Dr Shalini Prasad[1] *& Dr Abhay Kumar*[2]

ARTICLE HISTORY
Received on: 16/04/2025
Revised on: 22/05/2025
Accepted on: 15/07/2025

ABSTRACT

In the digital age, we mostly rely upon the internet and data-based technology, which has positively revolutionised our lives by bringing a plethora of opportunities in the areas of health, education, and information and communication systems. Digital freedom instilled confidence to break orthodox barriers and explore various options that were earlier not easily accessible. Simultaneously, the evil side of digital technology has introduced new avenues for cyber threats and disinformation operations that can not only disrupt state politics and undermine trust between states but also violate individual rights of privacy and the right to life. In this scenario, the paper is an overall assessment of the rampant cyber-based crimes against individuals with special reference to women. Women are more prone to cybercrimes than men, and their issues are mostly unaddressed. It explores cybercrimes against women from a feminist perspective and discusses their impact on social life within the Indian context. The study revealed that women's targets are nearly imperceptible in the realm of domestic cyber-related laws and international cybercrime conventions. It critically analyses various initiatives and policies that the Indian government has developed over time and how these issues are addressed at the global level.

Keywords: *cybercrime, laws, information technology, victimisation*

INTRODUCTION

Telecommunication systems and computers are essential for digital voice and data transmission across international borders. This capability facilitates the open exchange of thoughts and ideas, fostering a spirit of freedom that empowers individuals to participate in their political processes.

[1]Assistant Professor, Department of Political Science, Faculty of Arts, University of Allahabad. (**ORCID ID :** 0009-0007-1456-9889)
[2]Assistant Professor, Department of Political Science, Faculty of Social Sciences, Banaras Hindu University. (**ORCID ID :** 0009-0007-5896-4215)

The accessibility of information technology and knowledge has greatly improved our daily lives. However, along with these advancements, negative consequences have also arisen, affecting society today.

As we entered the 21st century, there has been an emergence of new variants of threats. The main security challenges for individuals, states, and societies now go beyond traditional military forces. Today, the focus is on cybercrime. There is a concerning development with the increasing number of cybercrime incidents that specifically target women. To identify the rising trends, this research paper aims to identify cyber threats specifically affecting women and to evaluate various policies and initiatives at both national and international levels that promote a resilient system to counter these threats. It highlights the increasing incidence of crimes against women and examines the underlying causes and motives behind these acts. The paper concludes that women are particularly vulnerable in cyberspace and recommends a specific framework for addressing the limitations of India's cybersecurity policies and universal legal frameworks.

CONCEPTUALIZING CYBER-CRIMES

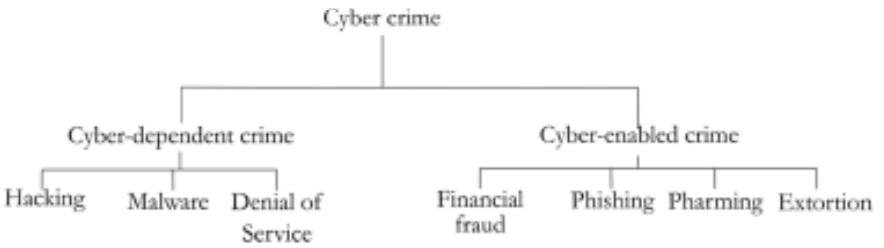
Cybercrime represents the intersection of criminal activity and technology, encompassing various illicit behaviours. Cybercriminals may perpetrate offences without direct interaction with their victims, often concealing their identities. Computers and data serve as both targets and instruments in these offences. McConnell International published a report on cybercrimes, which are defined as dangerous actions committed through or against a computer or network. Furthermore, computer crime can be characterised as using computers to facilitate either direct attacks on technological systems or the execution of traditional crimes (McConnell International, 2000).

Cybercrime can be categorised in two primary ways. First, it occurs when computer files or programs are accessed without authorisation, disrupted without consent, or when an individual's saved or stored information is stolen (Katyal, 2001). In the second instance, cybercrime manifests when computers are employed to commit traditional crimes, such as the creation or distribution of child pornography, or engaging in white-collar crimes like insurance fraud and copyright infringement related to popular songs (Katyal, 2001). These definitions collectively illustrate that "cybercrime" encompasses any criminal activity that is enabled by cyber technology.

“The UK’s Crown Prosecution Service (CPS) categorises cyber-crimes

into two broad categories: cyber-dependent and cyber-enabled crimes (CPS, 2020)". A cyber-dependent crime is a crime that can only occur with the help of a computer, its networks, or any variant of information technology or communication technology (McGuire and Dowling, 2013).

"Cyber-enabled crimes are traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT)" (McGuire and Dowling, 2013).



Source: (McGuire and Dowling, 2013).

It generally involves targeted invasions of computer networks aimed at stealing, altering, or damaging information and systems. Viruses, often referred to as dangerous code and worms, actively spread from one computer to another, causing significant disruption to their functionality and operations. This spreading action not only limits services but also has the potential to destroy networks through deceptive communications, ultimately rendering them completely non-functional.

There are many reasons why attacks happen. Attackers can include hackers who want to show their skills, criminals who steal credit card numbers, foreign spy services that acquire military or economic secrets, as well as terrorists who aim to cause damage to the security of the nation (Knop, 2008).

In simple language, cybercrimes can be defined as acts committed through information technology and the internet that aim to undermine an individual's identity or violate their privacy, often through stalking or disrupting operations with malicious intent (Reddy & Reddy, 2008). Additionally, cybercrime encompasses the theft of intellectual property, which involves violations of patent and intellectual property rights, the disclosure of financial secrets, or espionage to obtain classified documents (Dayson, 2002). Examples of cyber-crimes include:

Hacking is an openly conducted online activity to uncover, manipulate, or exploit vulnerabilities in computer software. Where terrorists' larger goal is to achieve their political objectives, hackers do not typically pursue political objectives. They primarily utilize methods to circumvent computer-generated barriers: attacks on email, theft of computers, and the creation of viruses and worms.

A Distributed Denial of Service (DDoS) attack is a serious cybercrime that deliberately overwhelms computer servers, effectively making vital resources such as websites completely inaccessible to legitimate users. These attacks disrupt access, preventing regular users from reaching the targeted services. A prime example of this occurred in February 2000 when Michael Calce, known as "*Mafiaboy*," executed a round of highly calculated denial-of-service attacks that successfully incapacitated major viable websites, including Facebook, Flipkart or (X)Twitter (Thomas & Hopper, 2008).

Phishing uses online correspondence like email or phone messages to lure victims to a fraudulent website. Once on the site, personal data may be collected, which can be used for financial fraud. Alternatively, the site might install malware, particularly ransomware, to facilitate extortion. These messages are often sent by the culprits who convince individuals to share their private information or visit a website while pretending to be legitimate organisations. While email is the most common medium for these scams, SMS and WhatsApp messages, known as "smishing," are also occasionally used (Lallie, Singh, Lynsay, Jason, Arnau, Gregory, Carsten & Xavier, 2021).

Vishing, or voice phishing, involves illicit calls or voice messages that manipulate people into revealing confidential information like online details, including passwords, or any sensitive bank information. Scammers can misuse this information for illegal activities such as stealing not only money but also personal data. They often pretend to be from known organisations, such as the victim's bank or any identified source. Mostly, they use toll-free numbers or voice over internet protocol (VoIP) technology to prove their credentials (Cisco, n.d.).

Ransomware is another kind of offence that breaks into a person's data and information and demands an unusual ransom of any kind to reinstate access to the files and networks. Generally, once the attacker receives the payment, the attacked regain access to their data. However, if the ransom is not paid, the perpetrator may either disseminate the data on online websites or permanently disable access to the files (Baker, 2025).

A whaling attack is a specialised form of phishing aimed at high-profile individuals within an organisation, such as the Chief Executive Officer (CEO). The foremost objective of these attacks is to deceive the person into authorising substantial wire transfers to the attacker, thereby compromising sensitive company information. They are more likely to be caught and prevented than standard phishing due to their targeted nature (Scott, Robinson, Ben & Clark, 2024).

Tabnabbing is one of the forms of phishing attack only but it specifically targets inactive tabs in your web browser. While the person is focused and working on the current tab, the link to a previous one can be hijacked, redirecting you from the intended website to a malicious site that closely resembles the legitimate one (Washington, 2023).

A man-in-the-middle (MITM) attack occurs when an attacker deciphers the connection between a user and an application. The goal is to involve in theft of personal data like online login credentials and the sensitive CVV numbers of credit cards and debit cards. Targets often include users of trade and finance, like online retailing sites, or any access that requires a password entry (Imperva, n.d.).

Pharming is a similar type of phishing. The attacker fools the operator by redirecting them to fraudulent websites by compromising the user device. This type of attack is inflicted by highly trained technical experts, and therefore, it happens less in numbers as compared to other crimes (Lallie et al., 2021).

To scam someone financially involves misleading individuals or organisations to obtain financial gain through various technological means. On the other hand, extortion involves compelling individuals to take certain actions, often related to financial transactions, through threats or coercion. It is important to raise awareness about these practices to better protect ourselves and our communities (Lallie et al., 2021).

One example of cybercrime is "swarming." This happens when many people try to access a website simultaneously, causing it to crash. Swarming can also make email bombing campaigns more effective. Email bombing is when a hacker sends thousands of messages to overwhelm a target (Weimann, 2004).

After this thorough discussion, it is high time to accept that cybercrimes have been a threat for many years. However, as more people are using the Internet now and spend more time online, they are more prone to these cyber

threats. The lockdowns have also added feelings of anxiety and confinement to this scenario. This situation has given cybercriminals more chances to trick people, make money, or cause problems. Electronic crimes have increased as our lives change and we rely more on the Internet. Cyber-crimes infringe on people's privacy and make them vulnerable to advanced computer technology. The following section addresses cyber-crimes against women, emphasising how technology has created opportunities while also exposing them to significant vulnerabilities that impact their lives.

CYBER-CRIMES AGAINST WOMEN

The National Crime Records Bureau (NCRB), a division of the Ministry of Home Affairs, published a report detailing that "four out of every one lakh individuals are exposed to cybercrime in some form, and out of four, one is a woman" (National Crime Records Bureau, 2020). It also stated that, as of 2019, there was an "18.4% hike in cybercrime incidents overall in India, whereas cases of cybercrime against women increased by 28%" (National Crime Records Bureau, 2020).

This includes a constructive exploration of why women are disproportionately targeted in cyberspace and the strategies that offenders often use in these attacks. By examining these factors, we can work towards developing effective solutions and support systems that mitigate the impacts on women's mental and physical health. Fostering awareness and resilience in the online community is essential for creating a safer digital environment for everyone.

Cyber technology has emerged as a significant tool for perpetrating various forms of victimisation, now facilitated through digital channels. In particular, cyberspace has become the most extensive platform for the cruel harassment of women, as millions of online users can witness these acts. The main targets of cybercrimes occur through a range of digital platforms. These include sending fake links via email, public and private chat rooms like WhatsApp, social networking sites like Facebook or Instagram, to target women. The predominant reason for this kind of behaviour remains similar to that of the pre-technology era: to malign a woman's image and reputation and instil a sense of terror in her mind (Citron, 2009).

Victims of financial fraud are safeguarded by various laws that address identity theft, online scams, and anti-phishing measures. However, women who fall victim to these crimes often do not receive adequate assistance

from the government, as their specific experiences are overlooked and overshadowed by broader trends in cybercrime (Citron, 2009).

The impact of victimisation is different for men and women. When a man's email or personal data is accessed and changed without permission, he can usually move on by notifying the police and his friends. He may not face the same level of humiliation from society as a woman would. His situation is often seen mainly in terms of financial loss. In contrast, a woman who is victimised may face social ostracism. The online humiliation can be harder for her to handle, leading to shame and self-hatred. She risks being viewed sexually, and it can be much more difficult for her to restore her social and professional reputation. Men usually fall victim to hacking and phishing, but they experience less cyberbullying, harassment, or online defamation compared to women (Frank, 2009).

Here are some observations to support this: Cyberbullying and trolling can lead to sexual attacks on women, but this is not a common issue for men. In cases where men harm women, it is the women who suffer; however, when women harm other women, both the perpetrator and the victim experience negative effects.

Women's victimisation undertakes both physical and mental devastation (Dekeseredy, 2010). As society increasingly relies on the internet, the way people experience victimisation has shifted more toward emotional abuse. Instead of physical attacks, we now see high-tech emotional torment. Victims can feel brutalised, horrified, and even suicidal from this emotional abuse, which often affects women more than men.

Unwillingly, women may forcefully join pornography, sometimes without their knowledge, through voyeurism. This situation leaves them vulnerable and can lead to social isolation. Men are less often targets of such voyeurism compared to women. The main differences between male and female cyber victimisation are the reasons behind the abuse, the methods used, and the lasting effects on the victims (Halder & JaiShankar, 2012).

Cyberspace offers women a powerful platform to assert their rights, access information, and express themselves freely, often even anonymously. However, cybercrime has become a global issue, and women are frequently the primary targets of this emerging form of crime. The vulnerability and safety of women are significant concerns within criminal and penal law, yet women often remain defenceless online. Cybercrime against women has reached its heights and poses a serious threat to personal security (Chaudhary

& Sood, 2024).

However, the existing measures and infrastructure to combat cybercrime, including the distribution of cybercrime police stations, may not adequately address the unique challenges faced by women victims (Gurumurthy, Anita & Menon, 2009). This raises concerns about the effectiveness of the current response mechanisms in providing timely support, ensuring justice, and securing digital space for women.

Cybercrime against women encompasses various forms of social media harassment, stalking, identity theft, revenge porn, financial fraud, and other malicious activities specifically targeting women. These crimes not only violate individuals' privacy, safety, and emotional well-being but also contribute to gender-based violence and discrimination in the digital space. Women's unique vulnerabilities online require focused attention and concerted efforts to address these challenges effectively (Chaudhary & Sood, 2024). Below are some different types of cybercrimes against women.

CYBER CRIMES AGAINST WOMEN: HOW?

Cyberstalking: Cyberstalking is a method of using the Internet to harass and abuse someone online. A cyberstalker typically avoids making direct physical threats. Instead, they monitor their victims' online activities, tracking social media interactions to gather personal information. They have sufficient technical knowledge, which is used in various forms of verbal intimidation, issuing threats through messages and posts to instil fear and anxiety, leaving the victim feeling vulnerable and unsafe.

India reported its first case of cyberstalking in 2001, involving a woman named Ritu Kohli. In this case, the defendant stalked her for four consecutive days by illegally chatting under her name and using obscene and abusive language. He also shared her contact number with others, inviting them to engage with her, which resulted in her receiving numerous calls at odd hours. This harassment left her in a state of shock, prompting her to report the incident to the Delhi Police. Under Section 509 of the Indian Penal Code, the attacker was charged with damaging the modesty of a woman (Beliraya & Abhilasha, 2020).

Harassment through emails: It has been happening for years, much like harassment through letters. It includes actions such as blackmail, threats, bullying, and even deception via email. E-harassment resembles letter harassment but often creates additional problems when it is sent from fake

identities.

Cybercrime has become one of the easiest and cheapest forms of harassment towards women. Women become easy prey due to their naïve knowledge and lack of technical expertise. It entails the use of online social platforms to threaten, abuse, or send offensive messages and comments. A study conducted by the National Commission for Women reveals that 54.8% of women have faced incidents of cyber harassment (Sharma & Singh, 2018).

Defamation: Cyber defamation occurs when someone uses cyberspace to publish shameful content or sends it via email to others. This type of information is shared online, damaging a person's image and, consequently, harming their reputation (Mishra, 2018).

E-mail spoofing -This text typically describes an email that seems to originate from one source but is dispatched from a different one. Such emails can lead to financial losses and are a common method used in online scams. By altering specific properties of the email, such as its header, "From" address, “Return-Path,” and “Reply-To” fields, malicious users can make the email appear to originate from someone other than the true sender (Mishra, 2018).

Trolling refers to the act of deliberately provoking disagreement, animosity, or arguments in online social networks. Trolls often target platforms like YouTube's online comment sections, forums, and chat rooms. Additionally, trolling can intersect with cyberbullying and may escalate into mob lynching, either virtually or physically. This can occur through various platforms, such as WhatsApp and Facebook, where large groups may bully individuals or communities based on their religious, racial, political, or national beliefs (Pathak & Tripathi, 2022).

Cyber Pornography: Cyber pornography is one of the heinous cybercrimes on the internet. This includes pornographic websites and magazines created with computers and the internet. Pornography means a projection of sexual acts, mostly through obscene or illegal websites in the dark web world of computers. It includes actions like downloading or sharing pornographic videos, pictures, and writings. The Indian Penal Code, Section 292, defines obscenity and addresses child pornography in Section 67B of the Information Technology Act, 2000 (Yadav, 2022).

Cyberbullying involves Cyberbullying is when someone uses technology to bully or intimidate others. It is a common type of online crime, especially affecting young girls and women. Cyberbullying can happen in many ways,

such as making fun of the person by spreading false rumours, fake messages, or sharing private photos or videos. The Cyber and Media Cell of the Delhi Police surveyed that "forty per cent of cyberbullying victims in India are women" (Misra, 2013).

Revenge porn is a grave cybercrime that specifically targets women in India. It involves the unauthorised sharing of private and personal sexual photos and videos as a means of blackmail or personal grievances. A report from the Cyber Peace Foundation reveals a staggering 148% increase in revenge porn cases in India over the past year. This heinous violation inflicts severe mental and emotional trauma on victims and irreparably damages their reputations (Yadav, 2022).

Sextortion—a term derived from the words "sex" and "extortion"- refers to the act of using an individual's sexual imagery to blackmail or threaten them. In essence, it occurs when a person coerces another into taking undesired actions, such as sending additional compromising photos, maintaining contact, or transferring money, by threatening to release their sexual imagery. Victims of sextortion can be targeted by both online strangers and former romantic partners, who seek to harass, embarrass, and manipulate them (Thorn, 2024).

Cyber-financial fraud has become an increasing concern for women in India. The surge in online transactions has provided cybercriminals with new opportunities to exploit unsuspecting victims. This type of fraud encompasses various schemes, including phishing, credit card fraud, and other online financial scams (Yadav, 2022).

The term **morphing** refers to the means of using an image of a person, either from personal images shared online or taken by the individual, and altering its content with software. This software can be misused to create inappropriate images, particularly of women, by combining certain elements of the original picture with parts from other images (Seth, 2018).

Voyeurism: Section 354-B of the Indian Penal Code specifies that if any person peeps into the personal life engaging in any private act of another person and too without his/her knowledge is termed as voyeurism. Furthermore, if that image is shared online, it unequivocally constitutes a cybercrime (Seth, 2018).

Various behavioural factors contribute to victimisation, such as sour relationships, harassment by ex-partners, workplace rivalries, gender biases and chauvinism, unauthorised exposure to digital technologies, and a playful

intent to enjoy online adult entertainment (Citron, 2009a). Additionally, the pursuit of monetary gains can also play a role (Bartow, 2009). Traditional society and a patriarchal attitude prevent many crimes from being reported (Beliraya and Abhilasha, 2020).

CYBER CRIMES AGAINST WOMEN: WHY?

Cybercrimes against women in India are a multifaceted issue and are shaped by several significant underlying factors. Gender-specific violence, patriarchal beliefs and a lack of awareness about cybersecurity.

Gender-based violence is one of the prime reasons contributing to the startling rise of cybercrimes aimed at women in India. Women are subjected to a range of violent acts, including domestic abuse, sexual harassment, and physical assaults that frequently spill over into the digital realm. In cyberspace, aggressors exploit technology to inflict harm, employing tactics such as online harassment, stalking, and blackmail against their victims. Disturbingly, in many cases, these perpetrators are individuals known to the victims, often intimate partners or even family members, who leverage their existing relationships to further perpetrate these crimes (Yadav, 2022).

Gender violence in Indian society can be attributed to deeply ingrained patriarchal attitudes that greatly contribute to the occurrence of cybercrimes targeting women. The society and the system reinforce patriarchal control, inflicting a culture characterized by misogyny, victim-blaming, and suppression. These discriminatory attitudes often expand into the digital domain, where women face online harassment, trolling, and various forms of abuse more than men. Those who dare to raise their voice against such harassment or violence often face negative repercussions by bringing shame to their families or communities to which they belong. This unsupportive response from family and society is also one of the important factors discouraging many women from reporting incidents of cybercrimes (Kapoor, 2023).

Additionally, a lack of awareness about cybersecurity plays a crucial role in the prevalence of cybercrimes against women in India. Many women lack basic knowledge in the protection of their data, such as creating strong passwords and being familiar with any online scams like phishing, ransomware, etc. This digital gap in understanding makes them vulnerable to any malware attack. Furthermore, women's awareness of privacy policies and safety tips for social media is also limited and influenced by prevailing power dynamics and societal norms, as many online issues are handled by males in the family. Gender and technology are interrelated due to many factors,

such as traditional beliefs, educational background, and approach, with men typically demonstrating greater proficiency in computer usage due to more exposure to the outer world (Saha & Srivastava,2014).

Women are often less informed or aware, or even if they know their rights, there is always an apprehension to fight, as the inaccessibility of the legal framework makes it harder for them to achieve justice for violations in cyberspace. The inadequacy of comprehensive cybersecurity policies and laws, especially for women, further complicates women's ability to seek justice and protection.

The issue of cybercrime was largely ignored until the first cybercrime convention held in Budapest in 2001. At the same time, international conventions and legislation in many countries have been established to protect society from the negative aspects of cyber technology. Even today, crimes like online bullying, stalking and defamation have not received full attention, especially from the perspective of women's victims. Despite women often being more likely than men to become victims of interpersonal cybercrimes, these issues remain inadequately addressed.

Online sexual crimes and abuses tremendously need stringent laws to combat them, but the real problem lies in the accountability of the offenders, who have mostly escaped due to the inappropriate execution of the laws.

A key step is to ensure that women are informed about their rights and the laws that protect them. Increasing awareness can empower victims and contribute to a safer online environment. Many women hesitate to report cybercrime due to fears of retaliation, ignorance of the First Information Report (FIR) process, or doubts about the effectiveness of legal remedies. The government needs to recognize that the rise in cybercrime and online victimization changes the nature of crime itself (Sanze, Catherine, Sheree & Helen, 2018).

The impact of the crimes turns out to be brutal and miserable for the women. Society predominantly blames women for issues related to digital violence, which exacerbates their struggles. This form of violence infringes upon fundamental human rights as outlined by both national and international provisions (Nigam, 2024). Various types of cyber abuse inflict detrimental immediate and long-term effects on an individual's whole psychological and mental well-being, physical health, socio-cultural engagement, and overall economic and social life. Victims of online harassment often encounter dramatic feelings of shame, exclusion, and ostracization (Citron, 2014).

Continuous exposure to cyberviolence can inflict a sense of fear and

self-censorship, ultimately reinforcing and perpetuating male dominance. The survivors of such mental abuse experience results in withdrawal from public spaces due to fear, depression, anxiety, trauma, and even self-harm (Balabantaray, Mishra & Pani, 2023).

BUILDING A STRONG RESILIENT SYSTEM: PREVENTION & PROTECTION

The internet has two main characteristics: it removes geographical barriers, allows users to connect anywhere, and provides anonymity. In India, two key laws address cybercrimes against women: the Indian Penal Code (IPC) and the Information Technology (IT) Act. The IPC serves as a general criminal law, defining various offences and their punishments. In contrast, the IT Act specifically targets issues related to information technology, including cybercrimes.

The IT Act 2000 (amended in 2008) and the National Cyber Security Policy (NCSP) of 2013 try to keep pace with the continuous changes in cyberspace, as the NCSP is now being updated and reorganised as the National Cyber Security Strategy. “The National Security Advisor within the Prime Minister’s Office. Apart from the NCSC, at present, cybersecurity issues are handled by different ministries at technical (MEITY), financial (Ministry of Finance-Mof), security (Ministry of Home Affairs-MHA) and defence (Ministry of Defence-Mod) levels” (Patil, 2021).

The Information Technology Act of 2000 (IT Act) serves as India's apex legislation for addressing cybercrimes. It was enacted to recognise electronic transactions and foster e-governance legally. The IT Act encompasses specific provisions aimed at combating cybercrimes against women, including electronic theft, stalking, trolling, etc. Additionally, the Act mandates the establishment of cybercrime investigation cells in each state to facilitate the effective investigation and prosecution of these offences.

INFORMATION TECHNOLOGY ACT, 2008 (AMENDED)

With the passage of time, the Indian government introduced several amendments to the Information Technology Act of 2000 in 2008. Sections 66 and 67, after amendments, made offensive messages illegal under Section 66A. Section 66 b punishes receiving stolen computers or communication devices through illegal means. Section 66C deals with identity theft and sets a penalty. Section 66D addresses deceiving a person by pretending to be someone else.

Section 66 e punishes for invading someone's privacy. Section 66f punishes serious threats to national security, which is cyber terrorism. It implies that when terrorists use cyber technology for their purposes, like recruitment, propaganda, etc. Section 67A sets punishment for sharing or publishing sexually explicit materials, and Section 67 b adds children under this purview. Additionally, it also established the Cyber Appellate Tribunal to hear appeals regarding decisions made by adjudication officers under the Information Technology Act.

The Indian Penal Code (IPC) addresses various laws in India. It handles crimes against women, including dowry, rape, or violence of any kind, and amendments have expanded its domain by adding voyeurism, cyberstalking and the sharing of sexually explicit material (Jain, 2017). Several ministers have also come up with their own system of combating cybercrimes.

The Ministry of Home Affairs (MHA) is authorised to monitor and combat cybercrimes. Under the aegis of the MHA, the "Cyber and Information Security Division" addresses issues related to cybercrimes and the implementation of the National Information Security Policy and Guidelines. The Intelligence Bureau (IB) plays a pivotal role in internal security information gathering in India, with a focus on monitoring cyberspace. Furthermore, the National Crime Records Bureau (NCRB) maintains detailed records of cybercrimes and incidents, supporting national crime data collection efforts (MHA, 2020).

The MHA is also the prime regulator of the Indian Cyber Crime Coordination Centre. This centre plays a crucial role in combating cybercrimes across India. Among its various components is the National Cybercrime Reporting Portal, a platform established to streamline the reporting of cybercrimes, those targeting women and children (MHA, 2020).

"In 2018, the Ministry of Home Affairs (MHA) launched the Cyber Crime Prevention against Women and Children (CCPWC) scheme" (MHA, 2018). This initiative provides financial assistance to states and union territories for the establishment of specialised cybercrime units focused on addressing cases involving women and children. Furthermore, the scheme also aims to set up dedicated cyber forensic laboratories in each state and union territory, enhancing the capability to investigate incidents of cybercrime.

The Ministry of Electronics & Information Technology (MeitY) supervises all policy matters related to information technology. It works in cooperation with "CERT-IN, the apex agency for cyber threats, along with other agencies like the National Informatics Centre, Centre for Development of Advanced Computing (C-DAC), Unique Identification Authority of India (UIDAI), and the Standardisation, Testing and Quality Certification Directorate. The

Ministry of Electronics and Information Technology (MeitY) has established Cyber Forensics Training Labs" in different cities, including northeastern states. These labs train police and judges on handling cybercrime and handling evidence (Beliray K & Abhilasha, 2020).

To empower Indians digitally and enhance the knowledge-based economy, the government launched Digital India. This programme underscores the significance of fostering digital competence and raising awareness about cybersecurity, especially among women and girls. It also includes efforts to improve the accessibility and quality of technological establishment and facilities, thus bridging the digital gap by enhancing access to technology for women (Yadav, 2022).

Ministry of Finance (MoF): "In 2017, Reserve Bank Information Technology Private Limited (Rebit) was created by the Reserve Bank of India (RBI)" as a subsidiary to provide its various information technology needs. Rebit was established to enrich the proficiency of RBIs in areas such as cybersecurity, which is essential for protecting sensitive financial data, as well as conducting thorough research and audits (Department of Economic Affairs, 2020).

The Indian government is making significant steps in enhancing law enforcement capabilities by implementing awareness programs, launching training initiatives, and advancing skills in cyber forensics. While progress is evident, there remains an opportunity to further counter the challenges posed by the growing scale of cyber threats in the everyday lives of people.

A significant problem lies in the no or poor reporting rate of cybercrimes against women. This behaviour can impede the state agencies from accurately assessing the frequency of cybercrimes against women and enacting laws to combat these crimes. The allocation of resources proved to be ineffective due to inadequate data and information.

To effectively address cybercrimes, it is essential to focus on resource allocation and provide law enforcement agencies with the specialised knowledge and advanced technology they need. Although current efforts face hurdles, such as resource limitations and staffing shortages, these challenges can be tackled with dedicated investments in training and tools. By prioritising these areas, we can improve the efficiency of investigations, enhance the overall response to cyber incidents, and work towards increasing conviction rates in cybercrime cases. With continued commitment and strategic initiatives, the future of cyber safety in India can be significantly strengthened.

While the Indian Penal Code and the Information Technology Act of 2000 and its several amendments offer legal provisions aimed at addressing such offences, their implementation and enforcement are inadequate. The ambiguities and inconsistencies in the interpretation and implementation of laws brought distinct outcomes for similar cases.

Cybercrime against women in India remains a grave and critical offence that must be dealt with stringently by law enforcement agencies. To combat these crimes, it is hindered by complicated challenges, which include inadequate resources, minimal reporting rates, discrepancies in the legal framework and unskilled handling of computer knowledge, which requires technical training and expertise. As mentioned above, capacity enhancement of law enforcement agencies and the judiciary remains the utmost importance. Lastly, every crime must be dealt with by eradicating ignorance among women and making them recognise their rights. (Pathak & Tripathi, 2012).

INTERNATIONAL FRAMEWORK: COMBATING CYBER-CRIMES AGAINST WOMEN

In 2000, the United Nations held the “Convention on the Prevention of Crime and the Treatment of Offenders” in Vienna, highlighting the necessity of stringent laws and universal prevention measures against cybercrime. This was followed by the European Council's adoption of the "Convention on Cybercrime" in Hungary in 2001, which defined cybercrimes as crimes against the secrecy and validity of information systems (Council of Europe, 2001).

Cyber-crimes are a global crime, and this Convention becomes the first international treaty to combat crimes undertaken with the help of the internet. It includes not only copyright violations, online fraud but also heinous crimes like child pornography and crimes undertaken on the dark web. The convention introduced the procedures and provided power to the state agencies to intercept data and internet networks (Council of Europe, 2001). India has yet to ratify the Convention on Cybercrime, which is the single international treaty aimed at combating cybercrime. Accepting this convention could significantly benefit the country by improving and aligning its national cybercrime laws with global standards (Rai & Bano, 2024).

In 2004, the United Nations (UN) established the Group of Governmental Experts (GGE) to address issues related to cybersecurity. However, this initial effort ended without significant progress due to disagreements among the three states: the United States, China, and Russia, which obstructed any consensus on the proposal recommendations. In 2009, the second GGE process was

convened, and its report, submitted in 2010, marked the necessity for the UN member states to inculcate cooperation with diplomatic tools and avoid the risk of cyberspace crimes. While countries acknowledge the importance of global issues like climate change, terrorism, and nuclear escalation, it is high time that they collaborate to combat emerging cyber threats and take action to avoid any cyber risk escalation. Consequently, a universal agreement or consent on cyber security remains elusive for the international community (Patil, 2015).

"The Global Commission on the Stability of Cyberspace and the Global Commission" on Internet Governance are actively working to define essential principles for reliable performance among states in the digital realm. They achieve this by bringing together a diverse group of stakeholders, including politicians, former diplomats, scholars, online rights advocates, and legal specialists. This collaborative approach aims to establish a framework that promotes stability and accountability within cyberspace (Centre for International Governance Innovation, 2020).

We can derive an analysis that not much has been done at the international level, even if cyber crimes are not limited to one country but encompass each country in this digital age. Although several initiatives are being taken at the regional level, like those by BRICS and Quad, adequate measures are still lacking at the universal level. A collective approach is needed to seriously discuss this crime, which not only violates an individual's human rights but also threatens the national security of the nation.

EFFECTIVE STRATEGIES FOR EMPOWERING WOMEN AGAINST CYBER CRIMES

The foremost strategy should be the use of Strong Passwords. The passwords should be strong and cannot be easily detected. It is also very necessary to maintain secrecy about their personal information. Social media should be used vigilantly, as the content is public and anything could become viral in a scratch of time. People should always be alert about phishing emails, vishing, and sharing any personal information in the public domain. There is an urge to keep the software up-to-date. It should be updated regularly, and an effective antivirus must be used (Gupta & Kapoor, 2018).

There is an urgent need for robust measures to enhance individuals'-particularly women's-abilities and capacities in the face of cybercrime. There is a need for the development of a comprehensive response plan, establishing a cybersecurity improvement roadmap, enhancing detection and response capabilities, an effective legal framework, and actively fostering awareness

through user education. It is critical to raise awareness among women about the careful and smart use of internet facilities and to train them on how to respond when they encounter cybercrime.

There is a critical necessity for knowledge and technical advancement to prevent harassment of women in India. To effectively counter cybercrime targeting women, not only are stricter legal reforms required, but a significant reform in the education system is also important, where the usage of computer technology and its negative consequences are also taught.

This change will successfully occur in collaboration with individuals, government agencies, non-governmental organisations (NGOs), and other stakeholders are significant to implement these necessary reforms. Women must be trained to learn and embrace preventive measures, such as exercising caution in sharing their private or personal photographs and videos online, staying vigilant in communications with strangers, and safeguarding passwords and other sensitive information that could be harmful to their security and privacy, (Kumar, 2019)

CONCLUSION

Cybercrime is an irrefutable threat that interrupts social order and inflicts significant damage. To effectively tackle this issue, we must establish a robust and resilient system of universal jurisdiction for cybercrime incidents, with unwavering support from both the international community and specific nations. We must establish an apex authority to oversee and enhance cybersecurity mechanisms within each country. Cybercrimes targeting women in India represent a formidable challenge that demands an immediate and unanimous response from the state, its enforcement agencies, technical skills and expertise, and most importantly, a well-versed, knowledgeable society. Through decisive collaboration and effective strategies, we can and must create an impregnable cyberspace for women in India.

REFERENCES

Baker, K. Introduction to Ransomware. (2025, March 4). https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/

Balabantaray, S.R., M Mishra, & U Pani. (2023). A Sociological study of cybercrimes against women in India: Deciphering the causes and evaluating the impacts on victims. *International Journal of Asia and Pacific Studies*, *19(1)* 23-49.

Bartow, A. (2009). Internet defamation as profit center: The monetization of online harassment. *Harvard Journal of Law and Gender*, *32*, 384–428.

Beliraya, K., Nilesh & Abilasha. (2020). Cyber Crime against Women in India: Legal Challenges and Solutions. *International Journal of Law Management & Humanities*. *3*

(5). 1012–2

Centre for International Governance Innovation. (2020). *Global Commission on Internet Governance,* Retrieved From, http:// www.cigionline.org/activity/global-commission-

Chaudhary, S., & Dr. R. S. (2024). Prevention of cyber-crime against women in India. *International Journal of Law, Justice and Jurisprudence*, *4*(1), 38-49.

Cisco (n.d.) What is vishing?. https://www.cisco.com/site/in/en/learn/topics/security/what-is-vishing.html

Citron, K. D. (2009). Cyber civil rights. *Boston University Law Review. Boston University. School of Law*, *89*(61), 69–75.

Citron, K. D. (2009a). Cyber civil rights. *Boston University Law Review. Boston University*

Citron, K.D. (2014). Hate Crimes in cyberspace, *Harvard University Press*, Cambridge.

Council of Europe. (2001). Convention on cybercrime, Budapest. Retrieved From, <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

CPS. (2019). Cybercrime - prosecution guidance," The Crown Prosecution Service (CPS), T ech.Rep., 2019. Retrieved from https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance.

Dayson, J. D. (2002), *The Myth of_Cyber-Terrorism, Retrieved From,* http://www.treachery.net/articles_papers/tutorials/the_myth_of_cyberterrorism/The_Myth_of_Cyber-Terrorism.pdf.

Deepika R. & Sabina B. (2024). Cyber Police Stations and Cybercrime against Women in India. Economic and Political Weekly, LIX (31), 22-25.

Dekeseredy, S. W. (2010). The hidden violent victimization of women. In S. G. Shoham, P. Knepper, & M. Kett (Eds.), *International handbook of victimology* (pp. 559–584). Boca Raton, FL: CRC Press, Taylor and Francis Group.

Department of Economic Affairs, Ministry of Finance. (2010). *Report of the Working Group for setting up of Computer Emergency Response Team in the financial sector* (CERT-in). Retrieved From, http://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf.

Franks, M. A. (2009). Unwilling Avatars: Idealism and Discrimination in Cyberspace. *Columbia Journal of Gender and Law*, Retrieve From, http://ssrn.com/abstract=1374533.

Gupta, S., & Kapoor, M. (2018). Cyber Crime in India: An Empirical Study on Cyber Crime Awareness among Women. *International Journal of Management Studies*, 5(4), 106-111.

http://www.aarf.asia/images/short_pdf/1538513964_12.%20PAPER%203

Gurumurthy, A. & Nivedita M. (2009). Violence against Women via Cyberspace. *Eco- nomic & Political Weekly,* 44 (40), 19–21.

Halder, D., & Jaishankar, K. (2012). *Cyber Crime and the Victimisation of Women*. IGI Global.

Imperva, (N.D.). Man in the middle (MITM) attack. https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

India Ransomware Report. (2022). Computer Emergency Response Team (CERT-IN). Retrieved from, https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2022.pdf

Jain, M. (2017). Victimisation of women in cyberspace in Indian Upbringing. *Bharati Law Review*. Retrieved From: http://docs.manupatra.in/newsline/articles/Upload/786274E9-B397-4610-8912-28D6D03230F9.monika_jain_pdf_1-1111.pdf

Katyal, N. K. (2001). Criminal law in cyberspace. *University of Pennsylvania Law Review, 149*. Retrieved from http://ssrn.com/abstract=249030 or doi:10.2139/ssrn.249030

Knop, von K. (2008). Institutionalization of a Web-Focused, Multinational Counter-Terrorism Campaign—Building a Collective Open-Source Intelligent System. In Centre of Excellence Defence Against Terrorism (ed.) *Responses to the Cyber Terrorism.* IOS Press: Netherlands.

Kumar, S., & Priyanka. (2019). Cyber Crime against women: right to privacy. *Journal of Legal Studies and Research.5,* (5), 154-166.

Lallie, H., S., Lynsay A. S., Jason R. C. Nurse, Arnau, E., Gregory, E., Carsten, M., & Xavier, B. (2021). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *Computers and Security,* 105. https://doi.org/10.1016/j.cose.2021.102248

M. McGuire & S. Dowling. (2013). *Chapter 1: Cyber-dependent crimes, Home Office, Tech.* RetrievedFromhttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment data/ file/246751/horr75-chap1.pdf

M. McGuire & S. Dowling. (2013). *Chapter 2: Cyber-enabled crimes fraud and theft, Home Office, Tech. Rep.,* Retrieved From https://assets.publishing.service.gov.uk/government/uploads [83] /system/uploads/attachment data/file

McConnell International. (2000). *Cybercrime...and punishment? Archaic laws threaten global information- A report*. Retrieved, from http://www.witsa.org/papers/ McConnell-cybercrime.pdf

Ministry of Home Affairs. (2020). *Indian Cybercrime Coordination Centre (I4C) Scheme.* Retrieve From, www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division.

Ministry of Home Affairs. (2020). *Cyber and Information Security (C&IS) Division.* Retrieve From, www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division.

Mishra, S. (2018). Dimensions of Cybercrime Against Women in India- An Overview. *International Journal of Research and Analytical Reviews. 5*(4). 966-975.

Misra, R. (2013). Cyber Crime Against Women. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2486125

National Crime Records Bureau. (2020). Crime in India. Retrieved from https://ncrb.gov.in/en/crime-india.

Nigam, S. (2024, April 22). Ending online violence against women in India: Calling for an inclusive, comprehensive, and gender-sensitive law and policy framework. https://www.impriindia.com/insights/ending-online-violence-against-women/

Pathak, A., & Prateek T. (2012). Digital Victimisation of women in cyberspace: An analysis of the effectiveness of Indian cyber laws. Retrieved From, https://nluassam.ac.in/docs/Journals/NLUALR/Volume-7/Article%207.pdf.

Patil, S. (2015). US-China: No More Spy Games? *The Diplomat*. Retrieve From: https://thediplomat.com/2015/10/us-china-no-more-spy-games

Patil, S. (2021). *Securing India in the Cyber Era*. Taylor & Francis.

Press Information Bureau. (2020). *Raksha Mantri Reviews Defence Cooperation Mechanism*. Press Release. Retrieve From https://pib.gov.in/Pressreleaseshare.aspx?PRID=1573610.

Reddy, G. Nikhita & Reddy, G.J.U. (2014). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies. *International Journal of Engineering and Technology*, *4* (1): 1–5.

Saha, T., & Srivastava, A. (2014). Indian women at risk in the cyber space: A conceptual model of reasons of victimisation. *International Journal of Cyber Criminology*, 8 (1), 57-67.

Sanze, Catherine, Sheree, M., Sheree & Helen Yu (2018). "Transforming Law Enforcement by Changing the Face of Policing," *Police Chief,* https://www.policechiefmagazine.org/trans- forming-law-enforcement-by-changing-the- face-of-policing/.

Scott, Robinson, Ben, L., & Clark C. (2024, November 18). What is whaling attack (whaling phishing)?. https://www.techtarget.com/searchsecurity/definition/whaling

Seth, K. (2018). *Combating cybercrimes against women*. Retrieve from, https://www.sethassociates.com/wp-content/uploads/2008/08/Women-and-Cyber-Crime.pdf

Sharma, A. & Singh A. (2018). Cyber Crimes against Women: A Gloomy Outlook of Technological Advancement. *International Journal of Law Management & Humanities*, 1(3), 2581-5369.

Tanu K. (2023). Cybercrime against women in India: Identification and Mitigation. *Indian Journal of Integrated Research in Law Indian Journal of Integrated Research in Law, III* (1). Retrieved From: https://ijirl.com/wp-content/uploads/2023/01/cybercrime-against-women-in-india-identification-and-mitigation.pdf

Thorn. (2024, November 4). Sextortion: What it is, How it happens and Who's at risk? https://www.thorn.org/blog/the-growing-threat-of-sextortion/

United Nations General Assembly. (2020). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* Retrieved From, https://undocs.org/A/65/201.

Washington, J. (2023, October 16). What is tabnabbing and how to prevent it?. https://www.freecodecamp.org/news/what-is-tabnabbing/

Weimann, G. (2004). *Cyber Terrorism—How Real Is the Threat? Special Report 119*. http://www. usip.org/files/resources/sr119.pdf

Yadav, H. (2022). Unveiling the dark side of cyberspace: a study of cybercrimes against women in India, *International Journal of Food and Nutritional Sciences*, *11* (1), 3408-3421.

ETHICAL CONSIDERATION:

Plagiarism and AI Declaration: The author declares that this article is an original work. All sources used have been properly cited, and no part of the content has been plagiarized. Any use of AI-assisted tools was limited to language support and did not replace the author's original ideas, analysis, or conclusions.