UCP Journal *of* Law & Legal Education
Vol. 3, Issue 2 (January – June 2025)

Gendered Dimensions of Cyber Security: Risks, Impacts, and Solutions in The Digital Era

Imtiaz Hussain*, *Hadiqa Qureshi*

Abstract

Cybersecurity, a foundation stone of the digital age, affects individuals across all demographics, yet its connection with gender is often unnoticed. From online harassment to cyber-stalking, from cyber-bullying to hate speech, from threats to image-based abuse, from revenge pornography to discrimination, women and other marginalised genders experience heightened risk of cybersecurity. This research focuses on the unique sensitivity these groups face in the digital era, highlighting the sociocultural and systemic factors that worsen their exposure to online platforms. Initially, the paper explores the prevalence and forms of gender based online harassment, analysing its psychosomatic, social, and professional impacts. The study examines how the digital divide and the lack of comprehensive cybersecurity policies contribute to these challenges, drawing on the experiences, perceptions, and responses of vulnerable groups to online risks. The paper also suggests that various stakeholders, including governments, tech companies, and civil society organisations, adopt precautionary and receptive strategies to create safer online atmospheres. Comparative analyses of case studies from different countries and legal systems enlighten the best practices and persistent gaps in resolving this concern. The researchers used doctrinal methodology, relying on both primary and secondary sources. This study aims to contribute to the universal discourse and thoughtful understanding of cybersecurity and to inform strategies to enhance digital safety, equity, and inclusion.

Keywords: Cyber Security, Online Harassment, Gender Perspectives, Digital Safety.

* Final Year Student of Sindh Mehran Institute of Law (SMIL), Jamshoro. email: balouchimtiaz786@gmail.com ** Final Year Student of Sindh Mehran Institute of Law (SMIL), Jamshoro. email: hadiqaqureshi6@gmail.com

Article History: Received: 11 May 2025; Received in revised form: 21 September 2025; Accepted: 17 October 2025.
Available online: 20 October 2025
DOI: https://doi.org/10.24312/ucp-jlle.03.02.550

Introduction

Cybersecurity is a defensive system which protects the risks to computers, information, servers, devices and data from any harm or digital attack (NIST, 2013). The gender approach to cyber security is interconnected with the other aspects; complexities and needs of people based on gender, religion, race and sexual orientation. A gendered approach to cybersecurity is all about understanding and addressing the facts related to the vulnerable groups and individuals, which fall within the ambit of online harassment. According to the Dart Centre for Journalists and Trauma, online harassment can be defined as "any unwanted verbal or nonverbal behaviour that occurs online" which "violates the dignity of a person" and "creates a hostile, degrading or offensive environment**" (**Ahn, J, 2020**).** Women in society face online harassment in different forms: threats, trolling, doxxing, hate speech, etc. The cyber world has become an arena for women, where they are being compelled to fight gender bias and hackers. Cybersecurity is a critical, broad-level issue which is a universal phenomenon, with an average of 97 cybercrime victims per hour; this means there is a victim of cybercrime every 37 seconds (Aiken, M, 2016).

The rapid revolution in the IT industry, with a cornerstone of Artificial Intelligence, has affected the lives of individuals at large. People are more connected and engaged with each other on online platforms compared to physical interactions. These developments have assisted in some instances, but put privacy in danger. Especially, women in our society are targeted by online harassment and cybersecurity issues. Women fear giving any of their details on any online platform due to the lack of security and privacy.

Gender and cybersecurity are two correlated terms which have gained popularity in recent years. Privacy and security are still questioned in this era. In 1999, Scott McNealy, CEO of the computer manufacturing company Sun Microsystems, reportedly remarked, "Privacy is dead. Get over it" (Amnesty International, 2018). His words show a clear view of modern times that how technologies have been transformed, and can be heard in today's echoes. Numerous studies have shown that women experience more cybersecurity issues than men. The absence of gender specific

policies in cybersecurity exacerbates the issue. The interests of men and women differ at large, which can be shown in the behaviour of both with regard to cybersecurity (Bailey, J., & Steeves, V., 2015). While arguing about equality and justice, we ignore the crucial aspect of women's lives, which is privacy and security. The lake of this recognition makes women suffer. This gap worsens the situation in today's realm, where such policies should be made, considering the necessity and confrontation of the present generation, which sticks with the laws and rules relating to the privacy concerns of women.

Women suffer from privacy fear, as the time is evolving and a digitalised way has made it easier to threaten or harass women at large. Additionally, there exists a digital literacy gap which needs to be addressed by training or educating women about this developing era in terms of technology. In the early decades of computing history, programming was so female-dominated, it was seen to be a "pink-collar profession" (Cole, 2014). Even in World War II, women played a crucial role in decoding the messages (Wilcox, 1998). As time passed, women's skills were underrated just because of being women and women were discouraged from pursuing further in the field. Now, the differences arise between men's and women's tech knowledge, expertise and access. In this digital age, these are crucial aspects to be dealt with, and welcome women in a safe online environment. Although UN Women Asia Pacific has developed an eLearning project in 2024 for promoting women's security and learning, it remains a challenge for women around the world (Brown, C. S. 2018).

The laws need to be strong enough to tackle these situations, which are escalating with the period of time and advancement in technologies. Furthermore, women are not trained or educated enough in Tech fields to deal with cyber issues or online violence. There is no focus towards any Tech- Campaign or awareness sessions for the vulnerable groups, due to a lack of these skills, women are likely to be targeted more in the online environment. Cybersecurity policies need a gender-based perspective. Moreover, cybersecurity education needs to be enhanced for the better participation of women in the field.

Though numerous studies have been made concerning cybersecurity issues with women, cybersecurity being a vast field, new technologies still lack some aspects which need to be focused

on. The research gap lies between academic training to the current policies and laws of cybersecurity. There is a dire need for strong academic training and learning for women, which could lead women to deal with these issues even if they are not experts. Basic knowledge of the internet is becoming a necessity in this developing time. Additionally, considering the new cases and issues faced by the people, especially women, the policies should be strong enough to provide justice and remedies to the victims.

This research employs doctrinal methodology to analyse the intersection of cybersecurity and gender within contemporary legal and policy frameworks. The study uses primary sources, including case law, statutes, constitutional provisions, government regulations, and official reports. It examines how existing legal systems address gender-based online harms such as cyberstalking, image-based abuse, and online harassment. In addition to this, secondary sources like commentaries, theoretical analyses, and interpretive writings are used to inspect and critique these legal responses. The research adopts a comparative approach, drawing on case studies from multiple jurisdictions to identify global best practices and recurring shortcomings in legal protection and policy implementation. Through interpretation, synthesis, and evaluation of these materials, the study seeks to understand gendered cybersecurity risks and to propose informed strategies for enhancing digital safety, equity, and inclusion.

Cyber-Security & Gender Disparity in Pakistan

The disparities refer to gaps between men and women in the digital world, reflecting inequality between them. Overviews of some essential aspects are mentioned below: The concept in our society that Tech jobs are for men only, as men possess a higher intelligence level, has created a gender gap. Women make up to 20 to 25 per cent of the workforce in Tech fields. Even though they are discouraged from pursuing higher education in any such field. This misconception has led society to the notion that women do not have any expertise or wisdom, which could amount to professionalism or a career path. This creates self-doubt in women. This reflects even gender stereotypes, which have been declared unlawful by the US Supreme Court and the European Court of Human Rights (Balkin, J. M., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., &

Zarsky, T., 2019). Diversity in cyber security means embracing different genders, races, ages, sexes and colours while hiring them on board. Industries prefer hiring men compared to women (Barlow, J. P. 1996). According to a report published by**.** Cybersecurity in 2023, women make up 26 per cent of the cybersecurity workforce globally. It is a male-dominated field. This diversity has become a tool for industries to make their brand image (Bartle, R. 2004). The online violence against women has rapidly escalated in recent years. According to the survey in 2023 of American adults in the United States found that 31 per cent of women face online harassment (Bhattacharya, S. 2021). The widespread use of the internet and AI has led to cyber violence against women. This includes online harassment, sexual abuse, hate speech, revenge porn and other privacy issues.

When women don't find other women to look up to in the industry, they may begin to entertain doubts about their capabilities and sense of belonging. Women in cybersecurity have no key positions or role models for the young generation to enter the field. Women hold 26 Per cent of AI jobs worldwide. ISC2, 2023, survey only 17 per cent of women took part, which shows the lower amount of female workers in the Tech Industry (Blum, A. 2012). Women mostly avoid being engaged online or participating online due to the fear of harassment and low security levels Bocij, P., 2004). Women's freedom of expression and online participation should be promoted so that they may lead the profession. Research shows that Women and men exhibit different levels of interaction with technologies. For instance, if comparing men and women, women show fewer capabilities and less interest in using computers (Boudreau, B., & Petley, J., 2022). This is due to the lower ratio of women being encouraged to join the Tech field (Boyd, d. 2014).

In Pakistan, like other countries, there is an increased reliance on digital activities nowadays. The pillar of Pakistan's legal framework regarding cybercrimes is the Prevention of Electronic Crimes Act (PECA) 2016. The sole purpose of this legislation was to enhance the protection of individuals 'data and to curb cybercrimes. Furthermore, the establishment of the Cyber Crime Wing by the Federal Investigation Agency (FIA) serves as a dedicated body to combat and investigate cyber offences. Despite these laws, Pakistan still fails to provide a safer environment to women. Cyber issues rose higher in Pakistan after the Covid19as

millions of people were engaged in the online environment. Soon after the pandemic, in 2021, the cyber harassment helpline received 4,441 online harassment complaints, with the majority of complaints coming from women (Buchanan, R., 2017). In 2022, women constituted the highest percentage of victims, accounting for 58.6 per cent of complaints, at the Digital Rights Foundation helpline. In 2023, a total of 2473 new cases were reported by the helpline and women complaining were aged between 18 to 30 (Burke, K. 2019). There is still a rapid growth in cybercrime cases in Pakistan, which needs to be tackled wisely.

Impacts of Cyber Security Threats on Women

The digital era has transformed communication, access to information, and social interaction, but it has also introduced new risks, particularly for women and marginalised genders. Cybersecurity threats disproportionately affect women, exacerbating gender-based inequalities and creating new avenues for harassment, discrimination, and abuse. From cyber stalking to image-based abuse, the risks associated with online presence can have far-reaching consequences on women's mental, emotional, and professional well-being. This paper explores the risks and impacts of cybersecurity threats on women, examining the sociocultural and systemic factors that contribute to their vulnerability, and proposing solutions to enhance digital safety and equity.

Cyber Security Threats Faced by Women

Women are often exposed to online harassment, including derogatory comments, threats, and targeted hate speech (Cyber Civil Rights Initiative, 2020). Social media platforms, forums, and digital spaces often become grounds for misogynistic attacks. Studies show that female public celebrities, journalists, and activists are unreasonably targeted, deterring them from participating in digital discourse (Demos, 2017). Cyber-stalking involves a determined and unwanted digital attention that can intensify into real-world threats to the woman. Women, particularly those in abusive relationships, often experience digital stalking by their partners. Perpetrators use spyware, GPS tracking, and unsanctioned access to personal accounts to monitor and control victims, restricting their self-sufficiency and freedom (Duggan, M. 2017). The victims sometimes

become blind in relationships and give out their private pictures. The broadcasting of private images, commonly referred to as revenge pornography without consent, has become a widespread form of cyber violence against women. Victims face disgrace, emotional distress, and, in severe cases, professional and social exclusion, sometimes by their own families (European Commission, 2021). Many legal systems lack full-bodied frameworks to address this issue, leaving victims with no alternative option. The cybersecurity threats extend beyond personal harm, affecting women's economic and professional opportunities. Workplace cyber harassment, identity theft, and data breaches disproportionately affect the work of female entrepreneurs and professionals, deterring them from leveraging digital platforms for career progress and financial independence. Sometimes this results in females quitting work and being dependent upon their families (Finkelhor, D. 2021). Doxxing is the act of broadcasting private information online without consent, and that excessively affects women, exposing them to cybersecurity threats such as stalking, harassment, and acts of violence (Franklin, K. 2019). Public figures, journalists, and activists advocating for gender rights are especially defenceless, facing coordinated attacks designed to quieten their voices and to deter them (Gill, R. 2017).

Psycho-social and Professional Impacts of Cyber Security Threats

The psychological clang of cybersecurity threats on women is thoughtful. Victims often experience anxiety, misery, and posttraumatic stress disorder (PTSD). The constant fear of online attacks and reputational damage leads to self-censorship, withdrawal from digital spaces, and lower self-esteem (Halder, D., & Jaishankar, K., 2011). Many women limit their online presence or completely disengage from digital platforms to avoid harassment (Henry, N., & Powell, A., 2018). This digital omission limits their ability to access opportunities, network professionally, and participate in social and political discourse, strengthening gender-based inequalities. The specialised significance of cybersecurity threats can't be understated. Women who experience workplace harassment or digital attacks may miss out on job opportunities, face reputational damage, or face difficulties in career development. Fear

of cyber threats deters women from management roles and entrepreneurial undertakings in digital spaces (Internet Governance Forum, 2021). The lack of inclusive legal frameworks to address cyber threats against women worsens the problem (Jenkins, H. 2006). Many countries do not have obvious laws protecting against online harassment, reprisal pornography, or cyber-stalking, leaving victims vulnerable. Even where laws exist, enforcement is often insufficient, and victims face legal barriers in seeking justice.

Socio-Cultural Factors Contributing to Vulnerability

Patriarchal norms and systemic gender biases manifest in digital spaces, reinforcing misogyny and discrimination (Kim, K. J. 2022). Women who challenge traditional roles or express opinions on gender rights face intensified cyber-attacks. The normalisation of online misogyny discourages reporting and accountability. Women in developing regions face higher risks due to limited digital literacy and access to cybersecurity resources. A lack of awareness about online safety measures, coupled with restricted access to technology, makes women more susceptible to cyber threats (Kim, K. J. 2022).

Governments and tech companies often fail to prioritise gender sensitive cybersecurity policies. Many digital platforms lack stringent moderation policies to curb online abuse, and reporting mechanisms are inefficient, discouraging victims from seeking redress (Klein, R. 2019). Addressing these challenges requires a multifaceted approach, including legal reforms, corporate responsibility, digital literacy, and gender inclusive policies. By always arranging and making gender sensitive cybersecurity measures, societies can create safer digital spaces, ensuring that women can contribute freely and securely in the digital world. Strengthening global collaboration and knowledge sharing can also contribute to mitigating cyber risks and nurturing an inclusive society.

Role of Technology in Mitigating Cyber Threats

In the digital age, cyber-related threats excessively affect women, making technology a crucial tool in addressing these challenges. The proper use of artificial intelligence (AI), encryption, cybersecurity tools, and online safety contrivances has evolved to

challenge gendered cyber threats such as online harassment, cyber-stalking, and image-based abuse. The following section explores the technological developments and use that help in mitigating cyber risks and fostering a safer online environment for women.

AI and Machine Learning in Cyber Threat Detection

The Artificial Intelligence-powered systems can effectively examine online interactions and help us to identify harmful content, such as hate speech, cyber harassment, and threats in real time. Social media platforms like Facebook and Twitter use AI to flag and remove abusive content before it spreads, but this is only done for publicly posted things (Kshetri, N. 2019). This can be a recommendation to use it in private conversations too, in order to avoid such issues. Machine learning models can detect cyber threats by analysing past patterns of abuse on the online platform. These predictive analytics may be used by law enforcement agencies and cybersecurity firms to proactively address the potential cyber threats targeting women, which is a marginalised gender. The rise of deep fake technology has also amplified the risk of image-based abuse and misinformation, which is directed towards women (Lam, A. 2018). AI-driven deep-fake detection tools can help to identify the deployed content and prevent its misuse (Lessig, L. 2006).

Encryption and Digital Privacy Tools

The encrypted messaging apps like WhatsApp protect users from unauthorised access and ensure private communication. The women facing cyber threats can securely exchange messages without the fear of interception, as they cannot be viewed by anyone other than the intended recipient (Lievens, E. 2010). The Virtual Private Networks (VPNs) allow users to mask their IP addresses, making it difficult for cybercriminals to track their location. This is especially useful for politicians, activists, journalists, and women facing cyber threats. MFA adds an extra and important layer of security by requiring multiple verification steps for account access, which includes biometric recognition, face recognition, two-factor recognition, etc (Manne, K. 2018). This decreases the risk of unauthorised access to social media, email, and financial accounts.

Online Safety and Cybersecurity Tools

Social media platforms often employ AI-driven content moderation tools to detect and remove offensive and harmful content, protecting women from harassment and cyberbullying (Matias, J. N. 2020). Doxxing is the act of publicly skimpy private information that can have severe consequences for women (Nissenbaum, H. 2010). Anti-doxxing tools help in sensing and removing personal material from online platforms; such tools are used in social media handles. Several organisations provide cybersecurity training programs tailored for women, refining them on digital self-defence, privacy surroundings, and recognising cyber threats (Phippen, A. 2017).

Ethical Considerations and Challenges

While technology plays a crucial role in justifying cyber threats, it also raises decent concerns: Many AI moderation systems fail to distinguish gender specific threats effectively due to unfair training data (Rainie, L., & Wellman, B., 2012). Excessive intensive care for cybersecurity purposes can lead to desecrations of digital privacy rights (Reardon, M. 2020). Advanced cybersecurity tools are not always accessible to marginalised societies due to cost and digital knowledge gaps (Salter, M. 2017).

Future Technological Innovations in Cybersecurity

The future of cybersecurity solutions should focus on AI models must be trained on diverse datasets to identify and address gendered cyber threats effectively. Decentralised identity confirmation can help women protect their digital individualities from cyber criminals. Facial recognition and fingerprint verification can provide more secure access to online accounts and decrease identity theft. Technology can serve as both a safeguard and a test in the fight against gendered cyber threats. While AI, encryption, and cybersecurity tools increase online safety, their ethical employment and approachability must be guaranteed. A combined effort among governments, tech companies, and civil society is necessary to leverage technology efficiently and create a safer digital space for all.

Comparative Legal Framework on Gender Justice and Cyber Security

The digitised world has transformed the meaning of data protection. This change has altered the way people used to cooperate and connect. The advancement in technologies has raised the necessity for a comprehensive legal framework addressing data protection and cybersecurity. The study of comparative legal frameworks shows valuable analysis of how different jurisdictions deal with the issue. The framework of different legal systems may vary according to their culture, privacy concerns and individual rights.

Global Standards

General Data Protection Regulation: GDPR is a European Union Regulation for the information privacy made on 14 April 2016 and implemented on 25 May 2018 (Shariff, S. 2015). Article 8 of the Charter of the European Union governs the transfer of personal data outside the European Union and the European Economic Area (Suler, J. 2004). GDPR is directly applicable with the force of law, but also provides flexibility to its member states to modify some provisions. By considering GDPR United Kingdom and California also adopted privacy Acts, having similarities with GDPR (UNESCO, 2019). The regulation applies if the data controller or data person is based in the EU and rarely to the organisations based outside the EU (Van der Wilk, S. 2021). GDPR also gives the right of compensation to the victim in Article 82. The Court of the European Union gave an interpretation of the right to compensation to those women who are affected and are more likely to exercise their rights granted by GDPR, as compared to men (UI v. Österreichische Post AG, CJEU, 2023).

United Nations Women, Asia and Pacific: The UN Women, founded in 2010, is the United Nations entity for gender equality and women's empowerment. It advocated the women's rights, violence against women, violence against LGBT people and women facing online violence (West, S. M. 2019). The organisation has an executive board which is represented by different regions. UN Women has to work according to the provisions of the UN Charter. Since 2021, UN Women has been implementing the project

of women, peace and cybersecurity in the digital world. In 2024, it launched a free e-learning platform for women to learn and enhance their knowledge and skills according to the modern era (World Economic Forum, 2021).

Framework India: Women in India are becoming more vulnerable to cybercrimes. In 2022, the National Commission for Women received 31,000 complaints by women (Grentzenberg, V., Pohle, J., Adelberg, P., & Blum, L., 2024). Revenge porn is a major crime committed in India. Section 10 of the Indian Penal Code 1860 defines a woman as "a female human being of any age". The laws of India which deal with cybercrimes are the Information Technology Act 2000, the Indian Penal Code 1860 and the POCSO Act 2012 (a special law for child sexual abuse). Section 72 of the IT Act 2000 says that any information of a woman obtained without her consent and disclosed or published is an offence, punishable with 3 years' imprisonment or a fine of up to 5 lac rupees or both. The law outlines the fundamental aspects of the situation, namely, that even if data is disclosed, such an act may attract imprisonment, as it involves safeguarding a woman's privacy. The right to privacy was recognised as a fundamental right by the Honourable Supreme Court of India in 2017, in the landmark judgment of *Justice K.S. (*Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1*)*, delivered by a nine-judge bench under Article 21 of the Constitution. Despite this historic recognition, India continues to struggle with a high incidence of cybercrimes across the states.

Framework Germany: Germany has been very strict with its privacy laws and implementations. The privacy rights enshrined in Germany's constitution also extend to foreigners and those living abroad and cover their online data. The German Federal Court of Justice, on 18 November 2024, made a judgment based on a personal data breach at Facebook (Lucarini, F. 2020). The plaintiff claimed that Facebook did not take appropriate measures to secure his personal data and was awarded EUR 250. In Germany, data protection has constitutional dimensions (Cole, O.2014). Privacy in the online dimension is governed by data protection provisions of the German Telemedia Act (TMA). Germany also transposed the European Union through TMA Germany has a long history of data protection, dating back to the late 1960s. In 2008, the FCC issued a

decision on online searches, and the court created a new constitutional right which guarantees the integrity of the Information Technology system (Lucarini, F. 2020).

Solutions and Strategies for Addressing Gendered Cybersecurity Risks

As digital spaces evolve, gendered cybersecurity risks continue to disproportionately affect women and marginalised genders. While these challenges pose serious threats to mental health, safety, and professional growth, a multifaceted approach involving legal frameworks, technological advancements, corporate responsibility, and digital literacy can mitigate these risks. This paper explores effective solutions and strategies to combat gendered cyber threats and foster a safer, more inclusive digital environment.

Legal Reforms and Law Enforcement Strategies

Federal, Provincial and Local governments should approve comprehensive and strict cybersecurity laws specifically addressing gender based digital violence, such as cyber stalking, online harassment, and image-based abuse or giving threats to do so. Existing laws should always be updated to reflect emergent digital threats. Law enforcement agencies, for example Police and the FIA, should receive specialised training on cybercrimes targeting women. Gender sympathy training can improve their ability to handle complaints efficiently and support victims seeking justice. Moreover, the special courts should be constituted so that the trained judges can decide the cases. Cyber threats always exceed national borders, necessitating international cooperation. Countries should collaborate on repatriation policies and joint investigations to hold perpetrators accountable, regardless of jurisdiction. A distinct legal framework for cyber jurisdiction should be established.

Corporate Responsibility and Platform Regulation

Social media handles must enhance the content restraint to quickly identify and remove harmful content automatically, including cyber harassment, hate speech, and revenge pornography. Artificial intelligence (AI) and machine learning can be leveraged to identify and prevent cyber threats before they escalate. In the

present era, laws do exist; however, they are primarily reactive, being applied after the commission of a crime, rather than pre-emptive in nature. Algorithms and calculations should be refined to recognise patterns of online abuse and take proactive action. Tech companies should implement clear, convenient, easy, and user-friendly reporting mechanisms that allow victims to report cyber abuse easily. Guaranteeing prompt responses and support services can progress victim support, and their identification can also be kept private, because some of the victims do not report to avoid the familial issues or being called a woman of low character.

Digital Literacy and Cyber Awareness Initiatives

Educational programs should also contribute to cybersecurity training from an early age, teaching women and girls how to protect their online presence, use privacy settings effectively, and recognise digital threats. Governments, NGOs, and the private sector should cooperate, considering it their duty to work on the public awareness campaigns highlighting digital safety, cyber etiquette, and ways to stop online abuse. Rural and underprivileged women often have limited access to cybersecurity resources. Communal-based training programs can bridge the digital literacy gap and empower these groups.

Psychosocial and Legal Support for Victims

Dedicated helplines for cybercrime victims can provide direct support, guidance, and capital to women facing online abuse. Counselling and mental health services should be made available to victims of cyber violence, helping them cope with trauma and regain confidence in digital spaces. Many victims face financial barriers to looking for legal recourse. Providing free or low-cost legal services can empower women to take action against cyber criminals.

Promoting Gender Inclusive Cyber Policies

Women should be enthusiastically involved in drafting cybersecurity policies to ensure gender sensitive tactics for digital safety. Data on gender based cyber threats should be methodically collected to inform policy choices and track the efficiency of interventions. Organisations must implement strict anti-harassment

policies, discourage such acts and provide cybersecurity training to employees, ensuring a safe digital work environment. Addressing cyber security risks for marginalised and affected genders, such as females and transgender individuals, calls for a multi-stakeholder approach, incorporating land enforcement of the legal reforms, corporate accountability of cyber-criminals, digital literacy, a reporting mechanism, and victim support devices that must be implemented. Strengthening the policies, fostering digital inclusivity, and pleasing to the eye technological interventions can create harmless online environments for women. By employing all-inclusive strategies, cultures can work toward a future where digital spaces are secure, empowering, safe, and reasonable for all.

Future Directions and Policy Recommendations

As cyber threats against women and marginalised genders continue to evolve, it is imperative to develop advanced thinking policies and frameworks that efficiently address such challenges of cybersecurity threats. Future generations must focus on legal reforms, technological advancements, public awareness, and multi-stakeholder associations to ensure a safer digital space for marginalised genders. This section outlines key futuristic outlook and policy recommendations in order to mitigate gendered cyber threats.

Strengthening Legal Frameworks

Current legal frameworks and law enforcement agencies often fail to sufficiently address gendered cyber threats such as online harassment, image-based abuse, and cyber-stalking, because of a lack of digital strength and support. Future policies should present gender-specific provisions in cyber laws, execute stricter penalties for perpetrators of gendered cyber-crimes and provide clear guidelines for law enforcement agencies. Given the borderless nature of cybercrime, international cooperation is crucial. All governments should work with global institutions like the United Nations and INTERPOL to create standardised regulations and specify the jurisdiction with respect to cybersecurity issues; develop extradition treaties for cyber criminals targeting individuals across borders, which is an important principle in international law to reduce criminal activity. It is imperative to foster cross-border

collaboration between cybersecurity agencies of all countries around the world.

Public-Private Partnerships for Cybersecurity for a Safer Online Environment

Tech companies play a vital role in creating safer and convenient online environments for the affected gender. Future policies should always encourage stronger content moderation policies on social media and digital platforms, increased transparency in how algorithms detect and remove harmful content automatically and User-friendly reporting mechanisms for cyber harassment and other gender specific cases. These mechanisms should include the non-disclosure of identification, solved while resolving the issue.

Public-private partnerships can enhance digital safety. Recommended strategies include: Joint development of AI-driven tools to detect and prevent cyber threats, sharing threat intelligence data between government agencies and private firms and establishing cybersecurity research initiatives focused on gender specific threats.

Digital Literacy and Awareness Programs

Digital literacy should be a core component of education to equip individuals with essential cybersecurity skills. Schools and universities should teach students about safe online practices and digital rights, educate young users on identifying and responding to cyber threats and promote ethical digital behaviour to reduce cyber-bullying and harassment.

Women, activists, and marginalised communities require specific training to combat online threats. Governments and NGOs should conduct workshops on online safety and privacy protection, provide resources on legal rights and mechanisms for reporting cybercrimes and develop culturally and linguistically appropriate awareness materials.

Ethical Development of AI and Cybersecurity Technologies

AI tools used to detect cyber threats often exhibit bias, failing to recognise gendered abuse. Future efforts should train AI

systems with diverse and inclusive datasets, ensure transparency and accountability in algorithmic decision-making and implement human oversight in content moderation processes. Advancements in privacy technologies can help users protect themselves online. Recommended measures include encouraging the development of encrypted communication tools, expanding access to VPNs and anonymity-preserving technologies and strengthening biometric authentication methods to prevent identity theft.

Establishing Support Networks for Victims

Governments and NGOs should establish dedicated helplines and online platforms where victims can report cybercrimes easily and seek help. Victims of cyber threats often suffer emotional trauma and legal uncertainty. Future policies should offer free legal aid for victims of cyber harassment, provide mental health support services for those affected by online abuse and develop recovery programs for individuals targeted by cyber mistreatment.

The future of cybersecurity must always be equipped with gender sensitive policies, technological advancements, and wide-ranging support systems, so that the marginalised gender may not be in harm. By strengthening legal frameworks, fostering public-private partnerships, improving digital literacy, and promoting ethical AI development, policymakers can create a safer and more all-encompassing digital environment. The operation of these recommendations will be critical as well as important in combating and safeguarding the gendered cyber threats and guaranteeing that all individuals can engage freely and securely in the digital space of this century.

Conclusion

This research paper has discovered the multilayered nature of gendered cybersecurity risks, explaining the predominance of online threats such as cyber harassment, cyber stalking, image-based abuse, and digital discernment. It has been established that women and marginalised genders face unequal exposures in digital spaces, exacerbated by socio-cultural biases, inadequate legal protections, and technological needs. This research work has also stressed the most important psychological, social, and economic effects of these cyber threats on victims. The role of digital literacy,

legal frameworks, corporate obligation, and technological advancements has been thoroughly scrutinised. This research has also recognised needs and flaws in existing policies and proposed approaches to come out of and alleviate gendered cyber threats through multi-stakeholder engagement, ethical AI development, and comprehensive victim support mechanisms.

The findings of the paper properly underline the urgent and important need for gender-sensitive cybersecurity policies that bridge the digital divide and discourse systemic inequalities. Governments, private sector entities, and civil society organisations must always be bound to cooperate to implement robust legal protections, technological solutions, and public consciousness. Strengthening the international cooperation between the states, implementing stricter laws and rules, and promoting inclusive digital education are critical steps towards ensuring a safer online environment for all, especially the marginalised genders. Additionally, tech companies must take pre-emptive measures in refining their content moderation policies, enhancing reporting mechanisms, and ensuring user privacy and security. Without a rigorous effort from policymakers, law enforcement agencies, and technology developers, gendered cybersecurity risks will continue to escalate, deterring digital inclusion and equity.

Given the hurriedly evolving landscape of cybersecurity threats, future research should discover emergent technologies, for example block block blockchain, AI-driven cybersecurity, and digital forensics in addressing gender-based online abuse. Cross-cultural studies can also deliver insights into how different legal systems and social structures influence the efficiency of cybersecurity policies. Further empirical research is needed to assess the long-term psychological and professional impressions of cyber threats on women and marginalised societies.

As the digital period continues to reshape human communications, ensuring cybersecurity is no longer just a technical challenge but a fundamental human rights issue. Gendered cyber threats demand urgent and wide-ranging responses that integrate legal, technological, and societal viewpoints. By nurturing a safer and more inclusive digital space, we can empower individuals to navigate the online world without fear, discrimination, or harm. The responsibility to create such an environment lies with all stakeholders, including governments, corporations, educators, and

the digital community at large. Only by taking collective action can we shape a future where cybersecurity upholds equality, dignity, and justice for all.

Acknowledgment

Our heartfelt thanks also go to our Respected teachers, Sir Azhar Ali Mallah and Sir Abrar Ali Mangi, whose invaluable insights and academic guidance have significantly contributed to the development of this research.

A special note of gratitude is owed to Advocate Zain ul Abdin Sahito for his critical feedback and expert advice, which have greatly enhanced the quality and depth of our study. His mentorship has been instrumental in refining our research approach.

References

Ahn, J. (2020). *Digital security and privacy in the age of cyber threats.* Springer.

Aiken, M. (2016). *The cyber effect: A pioneering cyberpsychologist explains how human behaviour changes online.* Spiegel & Grau.

Amnesty International. (2018). *Toxic Twitter: A toxic place for women.* https://www.amnesty.org

Bailey, J., & Steeves, V. (2015). *eGirls, eCitizens: Putting technology, theory, and policy into dialogue with girls' and young women's voices.* University of Ottawa Press.

Balkin, J. M., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (2019). *Cybersecurity: Law and policy.* Foundation Press.

Barlow, J. P. (1996, February 8). *A declaration of the independence of cyberspace.* Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Bartle, R. (2004). *Designing virtual worlds.* New Riders. https://www.pearson.com/en-us/subject-catalog/p/designing-virtual-worlds/P200000000149

Bhattacharya, S. (2021). *Gender, cyber violence, and digital rights.* Palgrave Macmillan. https://link.springer.com/book/10.1007/978-981-33-6044-0

Blum, A. (2012). *Tubes: A journey to the centre of the Internet.* Ecco. https://www.harpercollins.com/products/tubes-andrew-blum

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet age and how to protect your family.* Greenwood Publishing Group.

Boudreau, B., & Petley, J. (2022). *Hate speech in digital spaces.* Routledge.

boyd, d. (2014). *It's complicated: The social lives of networked teens.* Yale University Press.

Brown, C. S. (2018). *Cybercrime: Digital cops in a networked environment.* MIT Press.

Buchanan, R. (2017). *Online abuse: How social media is failing women. Feminist Media Studies, 17*(4), 654–671.

Burke, K. (2019). *Women in cybersecurity: Breaking barriers and bridging gaps. Cybersecurity Journal, 12*(3), 45–67.

Cyber Civil Rights Initiative. (2020). *Online harassment and gender-based violence.* https://www.cybercivilrights.org

Cole, O. (2014, December 15). Ten female tech pioneers history has forgotten. *The Daily Dot.* https://www.dailydot.com/via/womenwhochangedtechindustryforever

Court of Justice of the European Union. (2023, May 4). *UI v. Österreichische Post AG, Case C-300/21, ECLI:EU:C:2023:370.* https://www.sciencedirect.com/science/article/pii/S1877050921022262

Demos. (2017). *The rise of online misogyny: Trends and solutions.* Demos Policy Report.

Duggan, M. (2017). *Online harassment 2017: The prevalence and impact of online abuse.* Pew Research Center.

European Commission. (2021). *Cybersecurity threats against women: Policy responses and implications.* https://ec.europa.eu

Finkelhor, D. (2021). The internet and victimization of women and girls: Challenges and solutions. *Journal of Cybersecurity Studies, 8*(2), 122–140.

Franklin, K. (2019). Privacy, security, and gender-based violence online. *Journal of Digital Ethics, 6*(1), 55–73.

Gill, R. (2017). *Gender and the media: A critical introduction.* Polity.

Gottschalk, P. (2022). Preventing cyber harassment through law enforcement intervention. *Cyber Crime & Security Review, 5*(3), 88–109.

Grentzenberg, V., Pohle, J., Adelberg, P., & Blum, L. (2024, November 19). *[Title unavailable – citation incomplete].*

Halder, D., & Jaishankar, K. (2011). *Cyber crime and the victimization of women: Laws, rights, and regulations.* IGI Global.

Henry, N., & Powell, A. (2018). *Sexual violence in a digital age.* Palgrave Macmillan.

Internet Governance Forum. (2021). *Online gender-based violence: Challenges and global policy responses.* https://www.intgovforum.org

Jenkins, H. (2006). *Convergence culture: Where old and new media collide.* NYU Press.

Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

Kim, K. J. (2022). Digital gender violence and algorithmic biases. *Feminist Review, 8*(4), 203–225.

Klein, R. (2019). Gender, power, and digital technology: A feminist critique of online spaces. *Cyberfeminism Journal, 14*(1), 92–117.

Kshetri, N. (2019). *Cybersecurity and cybercrime in the global South.* Palgrave Macmillan.

Lam, A. (2018). Intersectionality and online harassment: A comparative study. *Feminist Cyber Studies, 11*(2), 45–78.

Lessig, L. (2006). *Code and other laws of cyberspace.* Basic Books.

Lievens, E. (2010). *Protecting children in the digital era: The use of alternative regulatory instruments.* Martinus Nijhoff Publishers.

Lucarini, F. (2020, July 12). The differences between the California Consumer Privacy Act and the GDPR. *Adviser.* Archived at Wayback Machine.

Manne, K. (2018). *Down girl: The logic of misogyny.* Oxford University Press.

Matias, J. N. (2020). The effectiveness of online moderation against online harassment. *Journal of Digital Communication, 13*(3), 89–104.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.

Phippen, A. (2017). *Children and internet safety: Risks, rights, and responsibilities.* Palgrave Macmillan.

Rainie, L., & Wellman, B. (2012). *Networked: The new social operating system.* MIT Press.

Reardon, M. (2020). Tackling cyber abuse: Policy frameworks and best practices. *Cyber Policy Journal, 9*(2), 34–59.

Salter, M. (2017). *Crime, justice and social media.* Routledge.

Shariff, S. (2015). *Confronting cyber-bullying: What schools need to know to control misconduct and avoid legal consequences.* Cambridge University Press.

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior, 7*(3), 321–326.

UNESCO. (2019). *Internet universality and gender equality in cyberspace.* https://en.unesco.org

Van der Wilk, S. (2021). Understanding online gender-based violence in the digital era. *Digital Rights Journal, 10*(1), 68–95.

West, S. M. (2019). Racial and gender bias in AI systems: Implications for cybersecurity. *AI & Society, 12*(4), 347–368.

Wilcox, J. (1998). *Sharing the burden: Women in cryptology in WWII.* Centre for Cryptologic History, National Security Agency. https://www.nsa.gov/about/cryptologicheritage/historicalfigurespublications/publications/wwii/assets/files/sharing_the_burden.pdf

World Economic Forum. (2021). *Cybersecurity and gender: A global perspective.* https://www.weforum.org