Library Progress International *Print version ISSN 0970 1052*
Vol.44, No.3, Jul-Dec 2024: P.273-284 *Online version ISSN 2320 317X*

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

Strengthening Cybersecurity for Women in Nagaland: Governance, Legal Frameworks, Prevention Strategies, and Precautionary Measures

Sarovino Zumvu[1], Dr. Zahoor Ahmad Wani[2]

[1]PhD Scholar, Department of Political Science, School of Liberal and Creative Arts (Social Sciences and Languages), Lovely Professional University, Punjab.

[2]Assistant Professor at the Department of Political Science, School of Liberal and Creative Arts (Social Sciences and Languages), Lovely Professional University, Punjab.

How to cite this article: Sarovino Zumvu, Zahoor Ahmad Wani (2024). Strengthening Cybersecurity for Women in Nagaland: Governance, Legal Frameworks, Prevention Strategies, and Precautionary Measures, 44(3), 273-284.

Abstract

The use of technology in the advanced age creates unlimited possibilities in communication, education, and the development of economic systems. At the same time, it has contributed to creating new types of criminal activities that take advantage of the open nature of the internet. One of the key common and rising trends of threats is cybercriminal activities against women, which are now looming and endangering the safety, privacy, and dignity of women in virtual space. This article focuses specifically on the nature of governance structures, legal frameworks, preventive measures, and precautionary actions concerning cybercrime against women in Nagaland, one of the states of India's Northeastern Region.

The strategies that will be employed to fight cybercrimes against women in Nagaland will also be discussed in this paper. In this case, we will review the available literature to determine this paper's area of focus – governance structures would illuminate the existing institutional frameworks to deal with this problem at the state and national levels. The legal systems shall be reviewed to evaluate the capacity of the laws and efficiency in handling cybercrimes against women.

Additionally, it will be possible to research the prevention measures existing at the moment and their effectiveness in fighting cyber criminality. The article will explore the measures that women ought to practice as preventive measures in the new arena. This research paper forms part of a larger study on cybercrimes against women in India of which a focus on Nagaland has been adopted here. The aforementioned chapters may have described the genre and scope of cybercrime in the region but this part will endeavor to appraise the systematic approaches to deal with these adversities. Due to this reason, by adopting Nagaland as our area of study, we can provide a more focused insight into both the cultural and social/technological factors that may characterize cybercrime and its prevention in the Northeastern region of India.

Looking at these elements as a whole, one will be able to see the merits and demerits of the existing militarized approach to fighting cyber criminality against women in Nagaland. This systems approach is critical when it comes to formulating appropriate strategies that point to counter threats and ride them as well as work against them. In this regard, the article will start with exploring the current state of laws protecting women from cybercrimes in Nagaland. The paper will discuss the measures being taken by the governments and various organizations to check cybercrime. This will entail the consideration of the central-level institutions as well as policies like the Ministry of Home Affairs and the National Cyber Security Policy.

At the state level, the study examines Nagaland's units in police departments, the cooperation of

departments under the Nagaland police, and any other specific body combating cybercrime against women. The article highlights the precautions undertaken to discourage acts of cybercrime against women in detail. It also includes applications of technology and hardware like information protection structures and cyber defense mechanisms including those for forensic gain. In addition, the possibilities will be considered for furthering education, such as concerning programs in schools and colleges, as well as constructive campaigns required to enhance the cognizance of the public on cyber safety.

Safety measures to be practiced by female social media users will be highlighted. In this section, several initiatives that help to promote the digital literacy of users, recommendations concerning safe work on the Internet, and information about threat identification and their reporting will be mentioned. Finally, this paper will discuss the social services that women, who have been victims of cybercrime incidences in Nagaland, can access.

The need for an updated and comprehensive cybersecurity policy

Professional criminals are becoming a more sophisticated menace to society through cyberspace. The goals of state-sponsored computer hackers are to prepare for digital disruption and to engage in political and economic espionage. They have been perceived as a threat by the government due to their growing digital attack capabilities. There exist diverse forms of attacks that are executed and progressively expanding into multiple domains. Along with a variety of other activities, the daily assaults by non-state actors against the digital infrastructure of nations (Cyber Security in India). These advances necessitate a larger commitment from both public and commercial agencies to maintain the cyber-security infrastructure. Cybercriminals are highly driven, financially secure and proficient in technology. Their attacks put national efforts like e-governance, digital public identity management, and smart cities at risk. Private companies and military organizations process large amounts of sensitive data and information. In addition to financial losses, the possible harm could jeopardize national security if vital information infrastructure is attacked.

Globally, India is regarded as a favourable location for outsourcing, and many corporations have established global delivery centres there that share services and support, including Apple, Sapient, Citi Bank, Bank of America, HSBC, DSM, and others. Simultaneously, India has been implementing the largest information and communication technology program in the world, called "Digital India." This program aims to improve access, and governance across all domains, including health and education, and move India toward digital currency in the next year. The Indian digital countryside has evolved significantly in a relatively short period and has undergone an amazing amount of change (Chitrey et al., 2012).

India is currently engaged in massive governmental and private cyberspace initiatives that will open up a plethora of options for the country's digital transformation. This suggests that India can be most confident in its ability to safeguard national interests in the digital sphere while taking advantage of the economic and social opportunities that come with digitalization (Cyber Security in India). To strengthen all-encompassing implementation: India's approach to cyber security can be based on the fundamental principles outlined in the NCE Policy 2013, which is a positive start. However, India needs an updated strategy that goes beyond a simple declaration of principles and describes how to operationalize cyber security, including how to train cyber security professionals, create public-private partnerships, and encourage cooperation between the military and the civilian sector.

In general, the National Cyber Security Policy stressed the goal of building capacity, developing skills, and providing training to create a workforce of 500,000 workers proficient in the field of cybersecurity by 2013. According to Thakker (2017), an updated Cyber Security Policy blueprint should include precise instructions for the hiring and training of these cyber specialists in a timely way. The public and private partnership sectors are important components of India's cyber policy. There are active efforts to build public-private partnerships and cooperative engagements in cyber security that are effective. As a result, it concentrated on both technical and operational relationships. To address the private sector and cyber security, several industry partners, including the Data Security Council of India (DSCI), the Information Systems Audit and Control Association (ISACA), and the National Association of Software and Services Companies (NASSCOM), have joined forces.

Promoting increased civil-military cooperation in cyber security must be a top objective for any new cyber security strategy. a group of eighty top defense, intelligence, and strategic officials for national cyber

security standards. There is a need for the military and civilian segments of the public sector to engage more frequently and formally. India has to modernize its cyber security policies, create a more comprehensive framework, and keep up with the rapid development of the cyber landscape (Thakker, 2017).

Establishing a Cyber secure Ecosystem

i. To make it possible for a national nodal agency to arrange, with distinct roles and duties, all issues about cyber security in India.

ii. To assist both public and commercial entities that are in charge of cyber security initiatives and businesses.

iii. Encouraging all firms to create information security policies that are in line with their business plans and execute them according to global best practices.

iv. To ensure that every agency sets aside a certain amount of money to carry out cyber security projects about emergencies and cyber events.

v. To provide financial plans and incentives to support organizations, fortify, and improve information infrastructure about cyber security.

vi. To stop cyber events from happening and from happening again by promoting technological advancement, taking preventative measures, and adhering to cyber security regulations.

vii. To set up a system for data exchange, incident identification and response in the event of a cyber-security incident, and collaboration on restoration projects.

viii. To motivate organizations to implement policies that guarantee the acquisition of reliable cyber security and facilitate the acquisition of locally produced cyber security with security implications (Ministry of Communication and Information Technology, 2012).

Securing E-Governance services:

i. Managing the deployment of business continuity planning, cyber crisis organization plans, and global security best practices for all e-governance projects is the first step in securing e-government services.

ii. To strengthen security posture and lower the chance of distraction.

iii. To promote the nation's increased use of public key infrastructure for communications and trustworthy communication.

iv. To enlist the help of organizations and information security specialists to support e-government projects and guarantee adherence to security best practices (Ministry of Communication and Information Technology, 2012).

The primary goals are to protect financial and banking information, personal information, sovereign data, and other types of data or information. The establishment of NCSP (National Cyber Security Policy) in 2013 was a positive move in the right direction since it allows for the integration of new initiatives and programs under a framework that has a clear vision and a set of coordinated strategies that are sustained. India can develop a whole ecosystem with a secure computing environment. It takes into account the numerous contemporary advancements in the field of cyber security that are occurring on a global scale. Governments, corporations, and private citizens are among the entities that operate in cyberspace and disclose information to collect data.

Coordination of energy in the system is one of the dangers and problems. Information sharing between public and private agencies, availability of cyber security experts, cybercrime investigations, protection of vital information infrastructure, supply chain risks associated with ICT, strict auditing standards, cyber threat intelligence gathering, crisis management, incident response, broadcasting, and so forth. The NCSP is in charge of conducting a thorough evaluation of all these risks and problems, as well as a comprehensive policy. The implementation of the policy for setting the objectives is therefore the challenge. The analysis of the National Cyber Security Policy from 2013 shows that the policy offers plans of action at different levels together with

comprehensive instructions that are necessary for operationalization. The most crucial difference between the market-driven and regulated approaches is that NCSP makes them.

This strategy in India should be able to reduce security risks associated with acquiring ICT products, particularly from foreign wholesalers, while still fully utilizing the advantages of the global supply chain, which include having access to top-notch goods, services, and knowledge at reasonable costs. This was stressed in the Securing Our Cyber Frontiers report. (National Cyber Security Policy-2013 Analysis) The policy, for instance, encourages organizations to designate or work with civil society, create information security policies, adopt guidelines for obtaining reliable technology, and offer financial schemes and incentives to organizations that support cyber security and information infrastructure. The creation of cyber security products domestically through innovative R&D is another focus of the NCSP. The noteworthy policy approach is to collaborate with the industry through cooperative R&D projects and the establishment of Centers of Excellence. This goal is consistent with the government's Triad Policies for IT, telecommunications, and electronics.

- **The following qualities are included in the conspicuous aspects of NCSP**:

i. To provide residents and companies with a safe and reliable online environment.

ii. Empowering concentrated on lowering reaction and recovery times as well as conducting efficient cybercrime investigations to lessen the nation's susceptibility to cyberattacks and cybercrimes.

iii. To aim for capacity building, national alerts, cybersecurity-related technology, public and private partnership requirements, the security of vital information infrastructure, and the promotion of collaboration and information sharing.

iv. Concentrated on coordinating, collaborating, and integrating with Indian stakeholder entities

v. To encourage and support the tactics that align with the goals of the NCS policy.

- **Challenges**

i. Mandatory measures may increase costs, create barriers for enterprises, and disrupt innovation without increasing security. Mandatory measures may hurt industries with limited security implementation experience.

ii. The Internet Information Supply Chain risks portraying original items as more secure. 3.

iii. The implications of demanding the acquisition of verified cyber security solutions in the absence of suitable testing facilities, including procurement delays.

iv. India needs a comprehensive policy to combat threats and compete in the international arena (DSCI Analysis of the National Cyber Security Policy, 2013).

v. Lack of awareness

vi. Lack of national-level cybersecurity architecture

vii. Lack of trained labor

viii. Lack of cooperation and coordination.

ix. Inconsistency in internet-connected gadgets

- **Opportunities for improving cyber security**

i. Increased coordination among government institutions.

ii. Change in ICT attainment processes of organizations, particularly important sectors and e-government initiatives, to focus on product security; drive suppliers to develop product security; and raise acceptability of tested goods.

iii. Improved cooperation between government agencies and industry on cyber security issues.

iv. Increased collaboration and information exchange on cyber security issues.

v. There is a need to improve the maturity of security procedures as well as promote the security function within businesses, particularly in vital industries and e-government activities.

vi. Increased demand for security experts, including managers, implementers, auditors, and trainers.

vii. Increased investments in security, boosting the cyber security goods and services market in India

viii. Creating significant prospects for security product and service companies, as well as auditing firms.

ix. Boost the domestic security industry, particularly startups that provide specialist and creative security products.

x. Improved Research and Development through partnerships among government, business, and academia.

xi. Raising citizen, consumer, and employee awareness of cyber security issues, as well as basic and best practices.

xii. Supply of goods and services

xiii. Cyber forensics

xiv. Policy & Regulation

xv. Creating new goods through R&D collaborations

xvi. Capacity building in government and industry.

Need for a Cyber Security Policy

Most countries throughout the world, including India, are experiencing qualified turmoil and a sense of fear because of numerous reports of cyber espionage, cyber terrorism, cyber warfare, and cybercrime. Similarly, the problem has led to virtual paralysis and Artificial Intelligence. Legal prosecution tools have not evolved quickly enough to deal with increasing cybercrime. The recent cyberattack in India reveals that a wide range of offensive techniques is being studied by several agencies. The lack of a coherent cybersecurity policy will significantly impede India's national security and economic growth. More attention must be paid at the highest levels to ensure that cyber-related vulnerabilities that can have an impact on cyber security are identified and removed to combat cybercrime.

As a result, a coherent and widespread cyber security policy will include several major components, including accurate conceptualization of cyberspace threats, the construction of a robust cyberspace through strong measures such as technical, legal, PPP strengthening, international cooperation, and diplomatic, and the development of tolerable organizational structures. India's approach to cyber security has previously been ad hoc and fragmented due to a lack of national-level strategy. Several organizations have been formed, but their specific tasks have not been specified, nor has there been any synergy among them. It exceeds a large realm; this is within the scope of the NSCS charter.

However, there appears to be no institutional framework for policy implementation (Tomar, 2013). There hasn't been enough thought about the implications of cyber security and cyber warfare. For the present being, several governments are actively addressing cybersecurity doctrine and strategy challenges. There are several countries represented here, including the United States, France, China, Sweden, the European Union, South Korea, and Singapore. They are more actively working to ensure a safe and secure cyber environment for their population (Desai, 2012).

International Status of Cyber Security: Cyber security is attracting attention as an important aspect of information security on a global scale. The fast development of computer systems and information and communication technology has greatly benefited human welfare, but it has also produced hazards in cyberspace that have the potential to undermine international and national security. Critical infrastructure is especially vulnerable to cyber-based threats (Bamrara, 2013). Furthermore, the emergence of social media platforms such as Twitter and Facebook has produced a new sort of medium for strategic and policy communication that transcends national boundaries and national authorities.

The worldwide data transmission system is also heavily reliant on the northwest of undersea cables,

which are potentially susceptible to accidents and deliberate disruptions (Desai 2012). Given the positive and bad potential of cyber security, there has been talk of developing an international treaty on cyber security to ensure that states behave responsibly in cyberspace. There are already various international conventions in place, including the Biological Toxins Convention, the Chemical Weapons Convention, the Non-proliferation Treaty, and the Weapons Convention. Similarly, time is required to counter cyber-attacks. Cyber warfare falls into three categories: 1. Espionage. 2. Vandalism. 3. Sabotage (Desai 2012).

Cybercrime Prevention Efforts in Nagaland: Focus on Protecting Women

Nagaland has been endeavoring in the fight against cybercrime especially crimes against women. Criminal police departments of the state have formed specialized cybercrime sections and improved cooperation between departments to tackle the increasing dangers of cybercrimes. The CCPWC forensics and training facilities opened at the Police Complex in Chümoukedima are a product of these efforts. This facility is meant to provide specialized training for police personnel on cases especially as may affect the vulnerable in society such as women and children in case of cybercrimes.

The Nagaland Police have organized consultative meetings/panel discussions with the masses to create awareness concerning cyber threats. They are programs like the annual program held at PHQ Conference Hall in Kohima involving stakeholders like NES representatives from the Department of School Education, Collegiate Education, principals of private schools, students, social media personalities, and journalists. In these meetings, specialists draw attention to such a number as 1930 to help the population avoid scepters and contingents as well as possible financial losses and hacking, among others.

Moreover, the Nagaland government has been planning to form the Cyber Dome to enhance its capacity to tackle the issues of cybercrime. This initiative includes the leadership's determination to develop public trust in the online environment and to exclude any forms of cybercriminal activity. By implementing such extensive strategies, Nagaland attempts to improve the cybersecurity situation and the state's preparedness to manage the current and future threats**.**

Schemes/Services under the Ministry of Women & Child Development for Women and Children affected by violence

- 181-Women Helpline Nagaland provides 24-hour toll-free telecom service to women affected by violence and seeks support and information on women-related schemes and programs. WHL facilitates crisis and non-crisis intervention through referral to the appropriate agencies.
- Sakhi-One Stop Centre (OSCs) provides integrated support and assistance for women affected by violence under one roof with services like medical assistance, police assistance, psychosocial support, legal aid, shelter, and video conferencing. It is integrated with 181-WHL.
- CHILDLINE-1098 works for the protection of the rights of all children. It is an initiative for rescuing and assisting children in distress. CHILDLINE-098 is a toll-free number and it is available all over India.
- The Ujjawala Scheme is a comprehensive scheme for the prevention of trafficking and rescue, rehabilitation, and reintegration of women and child victims of trafficking.
- Swadhar Greh Scheme also seeks to address the needs of females in difficult circumstances, including victims of sex trafficking.

The Nagaland State Commission for Women (NSCW), Department of Social Welfare, Nagaland State Social Welfare Board (NSSWB), Mahila Shakti Kendra (MSK), 181-Women Helpline Nagaland, Sakhi-One Stop Centre (OSC), CHILDLINE 1098, Nagaland Adventure Club (NAC), Kohima Chamber of Commerce and Industry (KCCI), and Association of Kohima Municipal Wards Panchayat (AKMWP), the SRCW, will organize a 'Car Campaign' to commemorate the International Day for the Elimination of Violence. The major goal of this automobile campaign is to raise awareness and sensitize the public to the issue of violence against women.

Another notable project is the Purple Ribbon Campaign, which has been embraced as a symbol of solidarity with women who have been victims of violence, as well as to raise public awareness and positively influence society's attitudes and actions against violence against women. Purple ribbon badges will be worn by people to honor this day, according to the announcement. To prevent all forms of violence against women, district administrations, in collaboration with team members from Sakhi-OSCs, MSK-District Level Centres for Women

(DLCW), and Beti Bachao Beti Padhao, are actively campaigning to raise awareness about issues/problems and services available to women affected by violence, according to the SRCW.

"Gender-based violence includes sexual violence, physical violence, emotional and psychological violence, online and digital violence, harmful traditional practices, and socio-economic violence," it emphasized, adding that violence against women exists regardless of their status, class, caste, or religion. "It is a typical problem that we encounter everywhere, whether at home, school, job, or on the streets. “Some women and girls are subjected to this violence their entire lives”, the statement added. According to UN estimates, fewer than 40% of women who have experienced violence seek treatment. In the context of Nagaland State, many such cases are hushed and unreported. Particularly cases of domestic violence, the SRCW stated, while emphasizing that victims hesitate to report due to complex harsh realities including fear of society's stigmatization, pressure from relatives/ families to avoid reporting, ignorance about their constitutional rights, concerns about the uncertainty of the children's future and custody issues, insecurity about not having support. It stated that gender-based violence be domestic or cyber, is a global pandemic and that any move toward eliminating violence against women should be viewed as both an effort to question the deeply embedded patriarchal system and a step toward empowering women.

Cyber security law in India

Information technology has helped us close the global divide. People may now easily communicate with friends and relatives on any continent, place orders, and work abroad, but this has escalated cyber violence, particularly against women, because many users create cloned personas and can conduct crimes from anywhere in the world.

The laws that include legal provisions to combat cyber violence against women are listed below:

The Bharatiya Nyaya Sanhita (BNS), 2023 then Indian Penal Code (1860)

The BNS deals with all criminal acts in India and even specifies punishment for them. In 2013, the Indian Penal Code,now Bharatiya Nyaya Sanhita was amended to handle internet offenses against women and others. The followingparts were added (Women and Cyber Laws in India,).

- **Section 354A**

This section addresses sexual harassment. In any situation, if a person demands sexual favors, forcefully displays pornography, or makes filthy remarks, he may face jail for up to three years, a fine, or both.

- **Section 354C**

This section defines Voyeurism. It is a criminal violation when a woman is unaware that she is being recorded while performing a private act. Anyone who commits this offense faces a fine and imprisonment for up to three years on the first conviction and up to seven years on successive offenses.

- **Section 354D**

This section addresses cyberstalking. It entails following a woman online by sending direct messages, commenting on photos, and posting offensive photographs or videos even when the woman seems uninterested. A man can face a fine and imprisonment for up to three years for his first infraction and up to five years with a fine for successive violations.

- **Section 499**

When a woman is defamed for any purpose to harm her reputation, such as by disseminating obscene photographs or videos online, the person who commits this crime faces imprisonment for two years or more, as well as a fine.

- **Section 503**

This section covers Cyber Blackmailing, which occurs when a person is blackmailed into changing their decision in favor of the blackmailer, and if the victim does not comply, threats are made to ruin the victim's reputation or injure the victim. Any person detected blackmailing in cyberspace may be held liable under this clause.

- **Section 509**

states that if a person is caught using vulgar comments, gestures, or words to harm a woman's modesty online, they will face a fine and up to three years in prison.

The Information Technology Act of 2000 (Amended in 2008)

This act addresses cyber violence, cybercrime, and electronic trade rules. Anyone who commits a crime related to it issubject to the provisions of this act and will be penalized appropriately.

The following sections help to counteract cyber violence against women (Women and Cyber Laws inIndia, n.d.).

- **Section 66C**

This section contains cases of cyber hacking. It refers to when personal information such as photographs, videos, electronic signatures, and passwords are fraudulently extracted and then utilized to bring emotional anguish to thevictim. Individuals who violate this section may face imprisonment for up to three years, a fine of up to ₹1,00,000,or both.

- **Section 66E**

If discovered collecting, publishing, or posting a person's private parts on cyberspace without their knowledge, they may face up to 3 years in prison, a fine of up to ₹ 2,00,000, or both.

- **Section 67**

Sharing, circulating, or posting obscene content online may result in imprisonment for up to 3 years for first conviction and up to 5 years for successive convictions, or a fine of up to ₹ 1,00,000 or both.

- **Section 67A**

This covers the publication of sexually explicit content online. It includes posting content containing sexual actions online. If convicted, individuals may face imprisonment for up to 5 years for the first offense and up to 7 years for subsequent offenses, as well as a fine of up to ₹ 1,00,000 or both.

Indecent Representation of Women (Prohibited) Bill, 2012

This statute punishes individuals who attempt to depict an obscene image of women in the form of images or films.

This Bill has widened its reach to embrace online content as well. (Women: Cyber Laws in India, n.d.)

- **Section 5**

This section empowers the officer to enter and search any premises in the region at any reasonable time, as well as examine and seize any obscene content possessed by the person suspected of committing the offense.

- **Section 6**

Penalties include imprisonment for 6 months to 5 years and fines ranging from ₹10,000 to ₹50,000.

Suggestions to Combat Cyber Violence against Women

Dealing with cybercrime requires knowledge, clarity, and guts. The following are some of the approaches to combatcyber abuse against women:

- **Knowledge of cyber laws**

The most important thing is to understand cyber laws. The victim must report the crime and should not be afraid to disclose it, as doing so can exacerbate the issue. There are dedicated hotlines for reporting cybercrimes against women (1091/1090) that provide free legal assistance to victims. Awareness and expertise of cyber rules are becoming increasingly important.

- **Training for officials:**

Police officers, cyber law experts, and members of the judiciary must be trained to combat the growth in cybercrime. They must be made aware of how they manage various forms of cybercrime. Different cybercrime branches now address a variety of cyber concerns, including hacking, stalking, blackmailing, phishing, morphing, and others.

- **Privacy Policies & Guidelines**

Women must read all of the terms and conditions before accepting, as some sites are fraudulent and vulnerable to hacking. The women must review their privacy settings to ensure that their social media accounts are safe from hackers. When a person establishes an account on a website, they must follow the criteria since it will help them battle cybercrime in the future. It is a leisurely activity, and appropriate research should be conducted before randomly accepting any popup boxes.

- **Discourage Information Sharing**

Women should avoid sharing their passwords, electronic signatures, bank account information, and other personal information with others to prevent it from being leaked or exploited against them.

- **Change Passwords at Short Intervals**

To avoid hacking, one should change their passwords regularly. Passwords should be kept private and not shared with closed groups.

- **Knowledge of Cybercrime**

It is critical to raise knowledge about cybercrime. Young females, like most teenagers, are susceptible to such things, while young boys, out of ignorance, begin to commit these crimes. Campaigns, seminars, and workshops should be organized in schools. To raise awareness of cybercrime, a message can be distributed to a large audience using television and social media advertisements.

- **Preserving the Evidence:**

If a woman is subjected to cyber abuse, she must understand the need to preserve all evidence related to the offense, such as filthy remarks, pornographic recordings, and threatening communications addressed to her. One can keep track of the numbers from which they receive threatening calls. It can assist cyber law professionals in finding clues.

- **Install Anti-Virus Software**

One must install the most recent versions of anti-virus software on their laptops and personal computers so that a hacker's attempt to steal information is prevented. The firewall must be turned on. It protects your privacy from Trojans and other e-mail infections.

- **Avoid responding to spam calls and unknown friend requests**

When it comes to cyber security, one must be attentive. It is always best to avoid answering spam calls and accepting friend requests from people one does not know. It is simply a precautionary measure to prevent cybercrimes.

- **Legal Provisions for Various Cybercrimes**

Cyber laws must have different measures for all types of cybercrimes. Some cybercrimes are currently addressed under a single umbrella section, while others are not mentioned at all. All of the proposals serve as building blocks for fighting cyber violence against women. Women must be taught and made aware of all cybercrimes, and if they are victims, they must receive emotional and mental help. They must be encouraged to report and speak out to set an example for society as a whole.

4.1. Conclusion

Cyber hazards, particularly those affecting women in Nagaland, are a continuation of the myriad challenges plaguing many places in India and around the world. However, as the influence of digital technologies in society grows, so does the threat of cybercrime. Nagaland's law enforcement actions, supported by national and state frameworks, serve as frontline protection. However, due to the ever-changing nature of threats in cyberspace, such solutions must be regularly updated. One of Nagaland's significant competitive advantages has been the development of specialized cybercrime agencies within the police force. These units, which are tasked with dealing with cybercrime, particularly those targeting women, are beneficial in the sense that they assist in responding to such situations by investigating and prosecuting.

The Cyber Crime Prevention against Women and Children (CCPWC) lab and training centre in Chümoukedima exemplifies the state's commitment to training. However, decision-makers have long recognized that the future success of such divisions is entirely dependent on the company's ability to pay for technical advancement. Employee protection necessitates ongoing training and competency development, as cyber criminals develop increasingly advanced techniques.

Other reform areas identified for development include inter-departmental coordination. Such procedures necessitate the establishment of appropriate information-sharing mechanisms across departments such as the police, judiciary, and social welfare. These coordinates help to ensure that each case of cybercrime, particularly among women, is presented to the appropriate authorities with the necessary attention and seriousness. Nonetheless, inter-departmental coordination should be encouraged and made less person-dependent, as it proved to be quite beneficial during the research. The employment of information technology in these processes, such as databases or automated reporting systems, can significantly improve the efficacy of these mechanisms.

However, the importance of technology in strengthening governance and legal systems cannot be overstated here. Improving computers, telecommunications devices, and automated analytical tools for surveillance and crime mapping would considerably boost Nagaland's cybercrime units. In addition, one can form a collaboration with digital businesses, academic institutions, and civil society organizations to bring the necessary know-how and creativity to solve cybercrime issues more effectively.

Although legislative instruments exist, their execution is not without obstacles, particularly in a state with such a distinct social and cultural background as Nagaland. The provisions of the Information Technology Act are quite wide, thus, local legislation should complement it to address Nagaland's specific concerns and requirements. For example, one of the major challenges that require expanded legislative measures is the protection of victims' identities and the guarantee of prompt access to justice.

General preventive measures include raising awareness and sensitizing the public with public billboard advertisements, internet campaigns, and the establishment of online classes about the potential risks that one could expose oneself to by engaging in cyber activities. However, the effectiveness of these strategies is limited by the scope and intensity of the activities. As a result, any attempts to boost literacy rates among Nagaland residents who use digital devices must consider the entire population. Such activities should be culturally acceptable, ensuring that none of the targeted communities, including the most disadvantaged, is excluded.

As a result, while Nagaland has made significant progress in combatting cybercrime against women, much more work remains to be done. It indicates that the state's activities must be adjusted in response to the continually changing danger environment. This will entail consistent support for law enforcement, improvements to the legal system, public sensitization, and mental growth. Nagaland can ensure the security of women in the online arena, and thus its residents, by implementing a number of the aspects listed above as interconnected workspaces. Such a commitment to cybercrime prevention will not only safeguard individuals but will also rebuild the fabric of social ties and increase public faith in the digital economy, thereby contributing to the state's development.

References

Badve, O., Gupta, B.B. and Gupta, S. (2016). Reviewing the security features in contemporary security policies and models for multiple platforms. In Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security (pp. 479-504). IGI Global.

Bamrara, D., Singh, G. and Bhatt, M. (2013). Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector.

Ben-David, Y., Hasan, S., Pal, J., Vallentin, M., Panjwani, S., Gutheim, P., ... and Brewer, E. A. (2011, June). Computing security in the developing world: A case for multidisciplinary research. In Proceedings of the 5th ACM workshop on Networked systems for developing regions (pp. 39-44). ACM.

Chaturvedi, M.M., Gupta, M.P. and Bhattacharya, J. (2008). Cyber Security Infrastructure in India: A Study. Emerging Technologies in E-Government ', CSI Publication.

Chitrey, A., Singh, D. and Singh, V. (2012). A comprehensive study of social engineering-based attacks in India to develop a conceptual model. Internat. J. Information & Network Security, 1(2): 45. Data Security Council of India. 'Analysis of National Cyber Security Policy (NCSP – 2013)

Cyber Crimes Against Women- 2020. (2021, September 20). National Crime Records Bureau. https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/TABLE%209A. 10. pdf

Cyber Security in India: Opportunities for Dutch companies, available athttps://www.thehaguesecuritydelta.com/media/ com_hsd/report/218/document/Cyber-Security-in India.pdf Accessed on 26 March 2019)

Desai, Nitin (2012). 'India's Cyber Security Challenge' Institute for Defence Studies and Analyses. Task Force Report. Halder, T. (2014). A cyber security for a smart grid. In 2014 6th IEEE Power India International Conference (PIICON) (pp. 1-6). IEEE.

Gajendra and Bhatt, Mamta, Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector. Bamrara, D., Singh, G. and Bhatt, M. (2013). Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector.

Gajendra and Bhatt, Mamta, Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector (January 1, 2013).

Halder, D., & Jaishankar, K. (2009). Cyber socializing and victimization of women. Temida, 12(3), 5–26. https://doi.org/10.2298/tem0903005h Kumar, S. (2019). Cyber Crime Against Women: Right to Privacy and Other Issues The Origins & History of Symbol of Law (Hardbound) Book View project. www.jlsr.thelawbrigade.com

Kedar, M.S. (2015). Digital India: New Way of Innovating India Digitally. Internat. Res. J. Multidisciplinary Studies, 1(4): 34-49.

Kumar, S., & Baroda, S. (2018). Why Should Women on Corporate Boards: One Question Many Aspects. Pramana Research Journal, Vol. 8, Issue. 9, pp. 137-146. Majumdar, S. (2003, August 10). Sexual Control and Violence. The Tribune- Spectrum. https://www.tribuneindia.com/2003/20030810/spectrum/main1.htm#top

Kumar, V. A., Pandey, K.K. and Punia, D.K. (2014). Cyber security threats in the power sector: Need for a domain-specific regulatory framework in India. Energy Policy, 65: 126- 133.

National Cyber Security Policy, 2013 by Ministry Of Communication And Information Technology available at: https://nciipc.gov.in/documents/National_Cyber_ Security_Policy-2013.pdf

Santanam, R., Sethumadhavan, M. and Virendra, M. (2011). Cyber security, cybercrime, and cyber forensics: Applications and perspectives. Information Science Reference. Saraswat, V. K. Cyber Security Presentation [PowerPoint slides] (2018).

Shah, M. (2007). E-governance in India: Dream or reality. Internat. J. Education & Development Using ICT, 3(2). Ten, C.W., Liu, C.C. and Manimaran, G. (2008).

Singh, J. (2015). VIOLENCE AGAINST WOMEN IN CYBER WORLD: A SPECIAL REFERENCE TO INDIA. International Journal of Advanced Research in Impact Factor: 4, 400(1). http://www.hindustantimes.com/Punjab/chandigarh/Facebook-abuse-tops-cyber-crime-chart-in

Thakker, Aman, 2017. 'It's Time For India to Update Its Cybersecurity Policy' available at https://thediplomat.com/2017/10/ its-time-for-India-to-update-its-cybersecurity-policy/ Accessed on 22

March 2019)

Tomar, Sanjiv. (2013). 'National Cyber Security Policy 2013: An Assessment' Institute for Defence Studies and Analyses. pp.1-7. Ugale, B. A., Soni, P., Pema, T. and Patil, A. (2011, December). Role of cloud computing for the smart grid of India and its cyber security. In 2011 Nirma University International Conference on Engineering (pp. 1-5). IEEE.

Utreja, Savita. 'Cyber Security' Need for Proactive & Preventive Actions' Ministry of Communications and Information Technology, Government of India

Verma Vanya. (2021, July 1). The virtual reality of cyberstalking in India. IPleaders. https://blog.ipleaders.in/virtual-reality-cyberstalking-india/ Violence Against Women. (2021). World Health Organisation. https://www.who.int/health-topics/violenceagainst-women#tab=tab_1

Vulnerability assessment of cybersecurity for SCADA systems. IEEE Transactions on Power Systems, 23(4): 1836-1846. Thakker, Aman (2017). 'It's Time For India to Update Its Cybersecurity Policy' available at https:// thediplomat.com/2017/10/its-time-for-India-to-update-itscybersecurity-policy/

Women - Cyber Laws in India. (n.d.). Information Security Awareness. All Rights Reserved Ministry of Electronics and Information Technology (MeitY), Govt of India. Retrieved June 15, 2022, from https://www.infosecawareness.in/concept/cyber-laws-inindia/women#:~:text=Section%2066E%20of%20the%20IT,years%2C%20and%2For%20fine.