Need for Cybersecurity Awareness in Rural Communities: A Socio-Legal Perspective

Reema Koshy

Christ University, Lavasa, Maharashtra, India

Abstract: *The cyberspace and its awareness have been expanding vastly since its entrance into the common world. There is now so much that can be done in the cyberspace and so many ways to use the Internet, wherein there have been rapidly increasing numbers of cyber-crimes and exploitations. Cyber-attacks are becoming more common and it is only the educated and urban communities who have information regarding how to prevent and/or face the attacks. There is an ever-growing need to push the concept of cyber-security to the rural regions in any country, there is a need to educate on the dangers of the cyber-world. As internet connectivity is reaching rural areas now, there is a higher risk of cyber-threats as well. The paper aims to enunciate the dangers of the cyber-space and the need for cyber-security in rural regions in India. It will layout the existing legal framework on cyber-security in India which the author will attempt to critically analyse. The paper will also contain recommendations on how to address the issue and aims to positively make a difference in the use of the cyber-space.*

Keywords: Cyberspace, cyber threats, rural, technology

I. INTRODUCTION

India is a country that has seen an exponential increase in the use of Internet and everything surrounding it, in the past few years. Digitalization has developed the country immensely and everything that was earlier done quite traditionally, is now being done online. Emails, social media, E-banking services, online government services etc have taken over the country by storm. But every good thing has its own disadvantages; the rising increase in internet and mobile use increases the risk of facing cyber-attacks. Cybercrimes are those crimes that are done through online/computer means, and the source is generally hard to detect. Cybersecurity acts as a major solution to this issue and it is slowly gaining much needed recognition.

The interesting point to note however is that the awareness about cyber security has been spreading everywhere, but we have not developed enough to make aware rural communities too. Neglecting rural areas in this regard can raise graver concerns in the future, such as threats to the national security of the country, because that is how penetrable the cyberspace is if not secured. People not aware about the concept of cybersecurity and cyber ethics can create vulnerabilities. The reason for lack of awareness may be the lack of exposure, lack of technical expertise, not being educated, limited financial means etc. However, the nation has to be all-inclusive when dealing with cybersecurity and thus the rural communities have to be specially prioritized in this regard.

The paper aims to highlight the rising use of the internet in rural areas in India and the cyber-threats coupled with it. The legal background of cybersecurity will also be discussed and recommendations for the same by the author will be laid out in the paper.

II. RESEARCH QUESTION

The research question that the author aims to answer is not one that has been dealt with commonly. It is one of utmost importance that has to be resolved in the near future due to the scaringly fast-pace growth in use of technology. The question formulated is thus: 'Whether there is an urgent need to spread cybersecurity awareness to rural communities?' The author has explored many aspects of the cyber-space and the rising threats to it, and the stand of rural areas with respect to cyber-use, in order to come to a conclusion regarding the question. The existing legal framework pertaining to cyber-security has also been scrutinized in order to bring about recognition for the implementation of more effective law. The research question carries significance as technology is advancing greatly and is being explored by those in the rural areas as well.

III. RESEARCH METHODOLOGY

The non-empirical research approach was employed in this essay. The research used secondary data analysis, a qualitative research technique, to examine information from published papers, journals, official government publications, news stories, and other secondary sources. The study is founded on a careful examination of several studies and publications produced over the past few years in the form of a literature review that emphasises and groups different facets of cyber security. The paper made use of quantitative research techniques and data gathered from ICUBE 2020 study and also other studies.

3.1 Cybersecurity and Rural Communities

A. Fast-pace growth in use of Cyberspace

India being a developing country is rapidly seeing a rise in the incorporation of technological advancements, both in the field of telecommunications and in online services. Various e-shopping sites, online gaming apps, e-banking apps, and other online services such as Wi-fi calling, video calling, food delivery etc have been coming up in the recent times and there is a high demand for the same as well. The cyber-space is so vast and valuable that everyone wants a taste of it, the autocrat and the commoner. According to cyber experts, India has experienced a peak in digital transformation but there has been a dearth of education and awareness of technology and online scams, among the public.[1]

This digital transformation is not only through use by the urban folks and big MNCs, it is also contributed by those living in rural areas and also small-time businesses. But the growth is too fast that people cannot keep up with the negative impacts of this development.

According to a report by IAMAI and KANTAR titled 'Internet in India' that is based on a study conducted in 2021, there are 692 million active internet users in India as of Dec 2021, out of which 351 million users come from rural India. This is a whopping 50% of the entire number of users. They have a 37% penetration rate as well. It also estimates that the numbers will reach 900million by 2025. The report also notes that there has been a 51% increase in digital transactions just two years, from 2019, due to the pandemic.[2] All these figures are factual proof of the existence of fast-pace growth and it also establishes the amount at which rural communities engage in internet usage. Even though rural communities hold such high numbers, it is not wrong to say that they are not educated enough on the complexities of the internet and vulnerable position they may be in. The same report also states that those from rural areas who do not actively use the internet are those who do not have the know-how. It can thus be assumed that those who do have the know-how may only have a basic idea, and it is hence necessary to spread awareness about the same.

B. Rising Cyberthreats to Rural Communities

The growing use of the Internet, as enunciated in the above section has led to serious concerns being raised about the cyberspace, including mainly the threat of cyber-attacks. It also creates concerns regarding national security.

The key issue surrounding the cyberspace is the idea of cybercrimes. Even though such crimes are non-physical and the perpetrator may not be known, cybercrime is the most dangerous form of crimes, because anything is possible on the Internet. The vastness of the cyberspace leaves it quite vulnerable. Data from the National Crime Records Bureau (NCRB) shows that India reported 52,974 cases of cybercrime in 2021, up more than 5% from the total of 50,035 incidents in 2020 and more than 15% over the previous year (44,735 cases).[3] This data displays an almost steady rise in the number of crimes committed. It is also understood that these numbers are just those of reported cases, and there could be thousands of more cases that could actually be occurring, where the victim is either unaware of how to fight such instances, or where they don't have the means to. Those in the rural areas may not possess the knowledge of how to report a cyber-crime, or even recognize when something is a scam online.

---

[1] Akriti Anand, *Explained| The Increasing Rate of Cybercrime in India*, (June 25 2022) https://www.cnbctv18.com/india/cyber-crime-are-on-a-rise-in-india-amit-shah-cyber-security-ncrb-data-13913912.htm.

[2] https://www.livemint.com/news/india-to-have-around-900-million-internet-users-by-2025-report-11659063114684.html(last accessed 19/11, 10 am)

[3] https://www.drishtiias.com/daily-updates/daily-news-editorials/indias-cyber-ecosystem

There are many cases now of cyber phishing which is a cybercrime where fraudulent messages are sent from what appears to be a trusted source. India has been prone to many such attacks especially in the region of Jamtara.[4] There are various other online scams as well, to which the young and the old may fall prey to. One of the most common scams these days are banking and payment frauds, where fraudulent SMS are sent regarding loan repayment, and winning of lottery etc. Those in rural areas may not be aware that such crimes exist, and are easily prone to the attacks. Youth also face various kinds of cyber-bullying online which they may not speak up about. They are also susceptible to being recruited by scammers.[5]

Local and small businesses are also highly prone to cyber-attacks such as ransomware attack, fake payment requests, hacks etc. However, they are less aware about cyber-security and how to go about it than large businesses in the cities.[6]It is also a possibility that they have less funds to set up a proper cyber-security system.

The rural community in the country is the most vulnerable when it comes to information technology and development as most of such regions are yet to develop. The ones who already have internet connectivity may not be educated on all aspects of it. This leaves the community prone to greater threats, which also acts as an aggregate threat to the country and national security, because cyber-terrorists can use any means to infiltrate the nation's resources. Thus, the lack of cyber-security in rural communities is not just harmful to them, but to the whole country. It is necessary to strengthen every individual and community in the cyber-world because it is a sensitive place where crimes can be committed in all ways, even unknown ones, unlike the physical world.

C. Legal Framework

The legal backing when it comes to any cyber-related issue in India is shaky. There is only one legislation in India that has incorporated how far the country has developed technologically and that is the IT Act of 2000. Governing many cyber-related aspects, the IT Act is the one legislation that recognizes cybercrimes and penalizes them. It also contains provisions for data privacy and protection. The important provisions of the act include section 43a -43h, which deal with cyber contraventions and sections 63-74, which are specifically cyber-offences. The act was enacted originally to regulate computer misuse and e-commerce activities but has now has extended to address cyber-security and data protection concerns, along with the IT rules.[7]

It is a growing concern that there exists no uniform and comprehensive law specific to cyber-security. In this era, when technological developments are at a peak, cyber-security is just as, maybe even more so important than normal law enforcement. Just as our homes are proofed so as to restrict entry to robbers, our computer and online systems too must be secure to face and prevent any attack.

The National Cyber Security Policy of 2013 is the one policy framework dedicated to enabling cybersecurity. The policy came about as a consequence of the NSA surveillance issue which occurred the same year. The policy, framed by the Department of Electronics and Information technology aims to create a safe cyberspace by protecting information and infrastructure. It aims to promote cybersecurity, establish systems to respond to and fight cyberthreats and also to reduce vulnerabilities. However, the policy is now outdated and its implementation has been poor as well. There have been many developments and drastically increased rates of cyber-attacks since the establishment of the policy, which it is not provisioned to handle. It also does not provide for the cybersecurity system for rural areas, which have to be viewed differently from urban infrastructure. The policy has to be reviewed in order to strengthen cyber infrastructure and also to make the system resilient to outside attacks.[8]

Modi announced a new policy to be released soon, a few years back and India has still not witnessed the emergence of this policy. This newly formulated policy is the need of the hour to resolve the gaps in the 2013 policy and to build a

---

[4]Nirmala Ganapathy and Debarshi Dasgupta, *India's scam central: Inside villages of cyber cheats*, The ST(Jul 24, 2022), https://www.straitstimes.com/asia/south-asia/indias-scam-central-rural-villages-see-surge-in-cybercrimes

[5] Id.

[6]https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/importance-of-cybersecurity-awareness/ (last accessed: 20/11, 5:40pm)

[7]https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india. (last accessed 20/11, 8 pm)

[8]https://timesofindia.indiatimes.com/india/india-needs-to-review-its-2013-cyber-security-policy/articleshow/76502600.cms (last accessed 20/11, 8:30pm)

stronger system to combat cybercrime and secure the cyberspace. This policy may take form drawing from the National Cyber Security Strategy envisioned by the Data Security Council of India in 2020. The strategy contains many well thought features including digitisation of public services, security for small/medium, businesses, state-level cybersecurity, cyber-insurance etc. The author believes that the upcoming, much awaited policy from the Ministry of Communication and Information Technology must incorporate the above strategy as it has conceptualized many necessary things. The policy should also be sensitized towards the rural communities and treat them with expert care. It should envision technical assistance for these areas and also funds to be dedicated for improving cybersecurity infrastructure in rural areas and also of small, local businesses. The policy must be tuned to provide a structured redressal mechanism which is easily accessible to rural communities as well.

Not attending to rural needs can create a gap which can be exploited by cyber-criminals, which can inturn affect national security[9]. India is yet to develop a robust policy framework that will attend to rural needs and prioritize their awareness, in order to strengthen overall national security.

IV. RECOMMENDATIONS

There is a clear need to educate rural communities and small businesses on the nuances of cyberspace and the impacts of attacks to it. It can impact daily life in a drastic way thus educating them will enable them to reduce the risks and prevent plausible damage. The author's recommendations to address the issue are thus laid out below:

1. It should be made a priority to initiate awareness programs in the most rural parts of the country to educate on the dos and don'ts of cybersecurity. People should also be taught preventive mechanisms and be made aware of where and how to complaint when they face cybercrimes. The funds to conduct such extensive programs could come from sources like the Government, MNCs (CSR) , politicians, NGOs, or any interested party.

2. The author strongly suggests that there be enacted strict procedural laws in order to efficiently enforce cybersecurity in all places. Such law will also enable those part of the rural community to know and enforce their rights, and the way to do it. The Legislature should urgently consider this aspect and act on it. Such law should inter alia contain complaint procedures and investigation provisions.

3. The media plays an important role in any major development. The major TV and radio channels, and also newspapers should take should use their voice to spread awareness about cybercrimes and prevention methods. The huge number of populations who are actively dependant on such sources will be educated through such means. Education is a crucial factor in solving the issue at hand.

4. The author also recommends that there should be improved coordination between centre and state for cybersecurity in order to create a safer space for rural communities. The State govt is more familiar with the rural regions and will should be given some discretion and authority to take actions favourable to the communities.

V. CONCLUSION

Awareness of the cyberspace has been spreading over the years and it has now reached even the most rural parts of developing countries such as India. Such rapid development carries with it major challenges as well and in this case, it's the concern of ever-increasing threats to the cyberspace, and individual life through it. Cybercrimes are increasing daily and many people, who do not have the awareness fall prey and are left with no recourse. Cybersecurity should be the top priority for any country during these times, when anything is possible on the internet. There are two sectors of the population consuming Internet, and it's the urban and rural communities. Where the former may be educated and experienced enough to handle online scams and offences, the latter may not, due to lack of awareness. The paper thus focused on bringing into light the need to educate rural communities on cyberspace. It also laid out the legal framework governing cybersecurity in India presently and the necessary changes to be made, to be sensitised to the rural areas. Cybersecurity it is the need of the hour and the government should take initiatives to promote it and establish strong and robust mechanism to enforce.

---

[9] Senthuran Nallainathan, *Study among Rural area citizen regard to Cyber Security awareness &Factors relating to it*, 9 IJEDR (2021), pg322

BIBLIOGRAPHY

[1]. https://www.livemint.com/news/india/rural-india-has-20-more-internet-users-than-urban-areas-nielsen-11651812524529.html

[2]. https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/importance-of-cybersecurity-awareness/

[3]. https://www.arcweb.com/blog/cybersecurity-rural-communities-often-neglected

[4]. https://www.financialexpress.com/brandwagon/rural-india-drives-indias-internet-adoption-report/2609379/

[5]. https://www.straitstimes.com/asia/south-asia/indias-scam-central-rural-villages-see-surge-in-cybercrimes

[6]. Syed Ubaid , Shakil, Mohammed Talha Alam, Shahab SaquibSohai, *Rising Cyber Crime in Rural India: A Review*, 6 IJARSCT 199 (2021)