Electronic Journal of Social and Strategic Studies Volume 2/Issue 2
Date of publication: 20 September 2021 Aug-Sep 2021
https://doi.org/10.47362/EJSSS.2021.2210

India's domestic Cyber Security and CyberCrime: A Case Study of Social Media and Darknet Management by Manipur Police

Oinam Ghanashyam Khumancha and T.K.Singh[1]

Abstract:

It has been observed in the past few years that many states in India had shut down internet services from time to time citing one reason or another related to crimes or to maintain law and order. The observed phenomenon is more prevalent in the Indian State of Manipur. Manipur at present is in the category of "Disturb Area" under the Indian Constitution, and controversial security Act such as "Armed Forces Special Power Act-1956" has been imposed since 1980. Many individuals have been arrested in Manipur by police for violating the cyber law as per reports. This simply indicates that despite its normal duties associated with regular crimes, their understanding in the domain of cyberspace needs to be expanded along with the legal aspects (law). However, the daunting question is how the Manipur Police has improved to challenging crimes in social media and the forum of the darknet. This lead to the question of Manipur Police to explore more on legal aspects of cyberspace to efficiently handle crimes on social media and counter vulnerabilities in the Darknet. India as a country is still a confused on what cybersecurity and cybercrime in practical life.

Keywords: Cybercrime, Cyber Security, cyber law, Social media, darknet, Police, IT Act.

[1] Oinam Ghanashyam Khumancha is a Ph.D. candidate and T.K. Singh is an Associate Professor at the Centre for Security Studies, School of International Studies, Central University of Gujarat.

Introduction

India starts its internet service with the launch of the Educational Research Network (ERNET) in 1986 exclusively for eight premier institutes of that time plus the Department of Electronics (GoI). This service is fully funded by the Government of India (GoI) and the United Nations Developmental Program (UNDP). India got its first internet public service in 1995. VSNL provides this first internet service. After two and half decades by 2018, India becomes the second-largest internet user after China. With the internet, mass is access to mass information and information technology with its benefit and ill effects. And already overburden Police departments got many new forms of crimes cases to solve which they are not fully ready prepared to solve.

Eoghan Casey defined Cybercrime as any crime that involves a computer and a network in which the computer may or may not be the victim (Moore, 2011, p. 4). As per the Council of Europe's 'Convention on Cybercrime (2001),' identified cybercrime range from "offenses against confidentiality, integrity, and availability of computer data and systems" to "computer-related offenses to content-related offenses" to "infringements of copyright and related rights" (Convention on Cybercrime, 2001).

There is no clear-cut definition of cybercrime in India. India's first attempt for protection from something like cybercrime comes through Information Technology Act, 2000 (IT Act 2000) under which some activities are identified as offenses and are punishable. This offense includes tampering with the computer source document, computer-related offences, cyber terrorism, transmitting or publication child pornography, failure to preserve records, refusal to comply with orders, failure/refusal to decrypt data, trying to access protect the system, misrepresentation, breach of confidentiality and privacy, publication of false certificate, fraud, and offence or contravention committed (GoI, THE INFORMATION TECHNOLOGY ACT, 2000).

The Information Technology Act, 2008 (IT Act 2008), update the previous IT Act. Here, it defines "Cyber Security as protecting information, equipment, devices, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction" (GoI, The Information Technology ACT, 2008). It also added new offenses like 'sending offensive messages, receiving stolen computer resources/ communication device, identity thief, cheating by personation using computer resource, violation

of privacy, upload of any pornographic material, and disclosure of information in breach of lawful contract' to the original list.

In 2018, McAfee and the Center for Strategic and International Studies (CSIS) estimate that around one percent of global GDP (i.e., 600 billion US$) is lost due to Cybercrime yearly (Lewis, 2018, p. 6). According to that report, India is rising as a hub for cybercrime along with Brazil, North Korea, and Vietnam (Lewis, 2018, p. 4). If 600 billion US$ is lost per year to the global economy, then the actual size of the economy in the Cyber-world must be huge. So, India as one of the leading countries must and is taking interest in tackling problems in cyberspace and improving cyber-security.

Table of daily cybercrime active in the world:

Cybercrime	Estimated Daily Activity
Malicious scans	80 billion
New malware	300,000
Phishing	33,000
Ransomware	4,000
Records lost to hacking	780,000

Source: Lewis, James. *Economic Impact of Cybercrime- No Slowing Down.* Santa Clara: CSIS; McAfee; 2018. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

Techopedia defined "darknet/dark web" as those networks that are not indexed by normal search engines, which can be accessible to only a selected group of people through authorization, specific software, and configuration (Darknet). The use of the darknet/dark web is not a crime in itself but tends to facilitate cybercrime as a platform as it is anomalous to normal daily cyber-world.

Anglophile countries under UK-USA Security Agreement (Five Eyes Countries) with the Echelon program that involved worldwide hacking and industrial espionage (Schmid, 11 July 2001), and its allies are banning Chinese hardware from manufacture like ZTE and Huawei, etc. on National Security reasons in May 2019. Till 2nd November 2020, United States Secret Services claim that they can prove Huawei has backdoor access to mobile phone networks but fail to provide the prove (Brodkin, 2020). According to Charlie Mitchell, "a ban on government purchases of Huawei and

ZTE products was the simplest, most visible step lawmakers could take to show they were fighting Chinese" and "technology was a key part of the US-China trade wae that erupted in 2018" (Mitchell, 2020, p. 152).

To prevent hacking and observation on the internet web or spying by NATO, Five Eyes countries and its allies; Russia and China are developing alternate world wide web other than American developed and owned one (Uchill, 2019).

Cyber-Crime in India:

In 2016, the National Crime Records Bureau (NCRB) recorded 12,317 cybercrime cases. Pavan Duggal, a cyber law expert feels that the figure above represents only 1 percent of actual cybercrime incidents that occurred in India (Cybercrime cases in India are under-reported, say experts, 2017). A news website reported that Indian foreign policy thinks tank Gateway House: Indian Council on Global Relations calculated India lost 18.5 Billion US $ in its March 2019 report. In the same new site, it also reported that according to the United Nations Office of Drugs and Crime (UNODC) India is becoming a huge hub of illegal drug trade using darknet and cryptocurrencies (Staff, 2019).

According to the report of the National Crime Records Bureau (NCRB) 2016, out of the 12,317 cybercrime cases, 8613 are under IT Act, 3518 are under IPC (Indian Penal Code) and186 are under SLL (Special and Local Laws) (NCRB, 2018, p. 421). On the same report, it states that 957 cases are related to uploading/transmitting sexual content, 37 breaches of confidentiality, 2373 cases are of cheating, 12 cases of cyber terrorism, and 183 trademarks and copyright violation cases (NCRB, 2018, p. 424). Uttar Pradesh has reported 2639 cases, Maharashtra has reported 2380 cases, Karnataka has reported 1101 cases, and follows by Rajasthan with 941 reported cases. According to the same report of NCRB, Assam is the no. 1 in cybercrime rate, Maharashtra is the no. 2, Karnataka is the no. 3, Telangana is no. 4 and Goa is at number 5 (NCRB, 2018, p. 417). According to the same report with previous year pending cases and current year (2016) cases, the total cases stood tall with 24187, and only 9213 of it solved leaving 14973 remain to solved; this means that police across the country only able to solved 40.3 percent and around 60 percent unsolved (NCRB, 2018, p. 425). According to Statista Research Department, from 2014-2016 there were 16468 banking report cases in India (Department, 2019).

India as a country already has been burden with communalism, racism, mob justice, moral police, corruption, white colour crime, etc. The new information technologies seem to magnify the already hideous problems. The rise of "gau-raksak" and its manner of killing people and uploading videos, create terror to normal people. Rise of communal clashes as a result of viral false news and false facts through social media. Some commentators already joke about Indian masses getting schooled in 'WhatsApp' University as this has become a common medium to spread false information, false news, propaganda to the masses. The incident of SMSs and MMSs that triggered a mass exodus of North-East Indians in 2012 is still fresh in people's memory and unsolved. The event of that incident of the Mass exodus of 2012 forced the Indian Government to put a restriction on the numbers of SMSs allowed to send at a time or day by a number, and a special train was dedicatedly arranged to carry North Easters from Bangalore to their homeland.

Many mass anti-government protests are also encouraged by various social media. Even the Euro-median and Arab spring were fuel by social media. To prevent such kinds of things happens in India, many state governments had used the option of kill-switch of the internet. Four Indian states have used this kill-switch of internet till August 2019; those are else State of Jammu & Kashmir (4 times; 2014, 2016, 2017, 2019), Gujarat (2 times; 2014, 2015), Nagaland (twice; 2015, 2017), and Manipur (4 times; 2015, 2016, 2018, 2019).

As per the report, there have been only two instances of darknet activity in India in which the first was recorded in July 2017 when 21 people were arrested in Telangana for selling LSD bolts and MDMA, and the other in October 2017 when two drug peddlers were arrested in New Delhi for selling drugs to rave parties. A News in the Hindubusiness states that the International Narcotics Control Board (INCB) of UNODC states reports of 1000 plus illegal online platforms operating from India through the crypto market (India, a key hub for illicit drug trade; use of darknet, cryptos rampant: UN body, 2019).

Ministry of Home Affairs (MHA) released Rs 93.12 crores to states and union territory to prevent cybercrime against women and children under the program CyberCrime Prevention Against Women and Children Scheme (CCPWC). Out of it, Rs 87.12 crores were mean to develop and set up Cyber Forensic laps and hiring operators of these laps. The remaining Rs 6 crores to train 40500 police, prosecutors, and judicial Officers by 31-3-2020 according to MHA official website (MHA, 2021). With the Covid-19 pandemic, this paper presumes that the training of this police,

prosecutors, and judicial official is not accomplished in time. According to the same MHA official website, it indicated the presence of a network of centers to face cybercrime or threats in and on India. The units of this network are the National Cybercrime Threat Analytics Unit, Cybercrime Ecosysystem Management Unit, National Cybercrime Reporting Portal, Platform for Joint Cybercrime Investigation team, National Cybercrime Forensic Laboratory Ecosystem, National Cybercrime Training Centre. National Cyber Crime Research and Innovation Centre.

In mid of the Indo-Sino border tension of 2020, the Indian government bans many mobile apps of Chinese origin citing national security reasons but there is no evidence of those mobile apps are threatening India's Security posture or Indian citizens. That action of the Indian Government arises due to enmity or genuine threats or to score some political mileage both domestically and internationally is still a question. By March 2021 many those mobile apps that the Indian Government Ban in 2020 is back in 'play store' or similar app store.

India like any other anglophile country, India bars China's Huawei and ZTE from any new network development and in the process to phase out indirectly. India maintains that India will not have any hardware or investment from any countries that share a land border with India. This in a way directly targeting China as India's other neighbours that sharedland boundary are not capable for any investment or providing hardware. To date, there is no hard evidence of backdoor function on Chinese hardware and software that India is using.

India does not ban Israeli software or apps, even after been reported that Israeli software like 'Pegasus' snooped Indian Journalists, activists, and others (TimesofIndia, 2019). India is still and planning to continue using American and European hardware and software; even after with hard evidence of them having backdoor and spying on India for ages. Crypto AG a Switzerland-based American (CIA) owned hardware company sold many products to India for ages which has a backdoor and spying India through it for ages (Report: US, Germany spied on countries for decades via Swiss encryption firm, 2020). According to a report of Hindustan times of 2014, US National Security Agency installed spy software 'quantum' to Indian computers since 2008 even to the computer system that has no internet connection also (Reuters, 2014). This installation of a program without internet access may be mainly possible only with help of Operating Softwares (Microsoft), Processors (Intel and AMD), Motherboard (ASRock, Asus, Biostar, EVGA

Corporation, Gigabyte Technology, MSI, Intel, Foxconn, Acer), etc. which are American and Taiwan based companies.

According to reports of The Washington Post and The Guardian of 6th June 2013, under the Protect America Act, Foreign Intelligence Surveillance Court (FISC) and Foreign Intelligence Surveillance Act (FISA of 2008) program 'SIGAD US-984XN' or code name 'Prism' using Microsoft, Skype, Hotmail, Facebook, Google, Youtube, Yahoo, PalTalk, AOL, Vodafone groups, Global Crossing (Hutchison Asia Telecom Group is one of the major owners), Apple, Interoute communication Ltd, Alcatel, CenturyLink, Lumen Technologies, etc (Gellman & Poitras, 2013; Greenwald, MacAskill, Ball, & Rushe, 2013; Ball, Harding, & Garside, 2013). As per these reports the United States is using hardware, software, apps, cables, wi-fi, phones, mobiles, etc. companies that are based in United States, Europe, Taiwan, Hong Kong, etc. to spy on other countries. Still, India is accepting investment, hardware, software from all these vendors after such concrete shreds of evidence. This shows India's CyberSecurity understanding is very vague, immature, and murky; what India needs in form of CyberSecurity is again seem marionette by some external players keeping in an account of India's action for CyberSecurity in the past 10 years.

Cyber-Crime and Manipur police:

In Manipur, around forty ethnic communities are living at present in various parts. Many of these communities form ethnic conglomerates or umbrella groups like Kuki and Naga. These conglomerates are at times violently interacting with each other. The Hindu-Muslim clash of 1993 and the Kuki-Naga clash from 1992-97 are the biggest ethnic clash in Manipur till date. The possibilities of future ethnic clashes are always looming there as many ethnic groups are living in congested land. And India as a whole is increasingly communalized in the recent few years. Many ethnic groups are separately waging wars of Independence from the Republic of India.

North-East India is surrounded by countries like Bangladesh, Bhutan, China, and Myanmar. Manipur is a part of that North-East India. According to South Asia Terrorism Portal, a security think tank based in New Delhi, Manipur has more than forty armed groups actively or inactively operating in the state. Some of these groups are based on ethnic lines and demand for separate state or union territory inside India. Few are trying to unify to other newly created identities in another state to get a larger Independent country from India. Others are claiming to fight for independence

of else "Kingdom of Manipur". Most of these armed groups used to make based outside the Indian Territory, in countries such as Bangladesh, Bhutan, and Myanmar. However, in the last decade, the government of Bangladesh and Bhutan (with the help of India) managed to flush out these shelters (camps) from their territory. At present, India's State mechanism is in cooperation with Myanmar Government to repeat the success story of Bangladesh and Bhutan in Myanmar. As these armed groups are operated from outside India, they must be using some form of medium to communicate and execute their agenda. The medium may be telephone, radio, or internets which are optimal in usages.

It is again well documented that Manipur becoming a trade route of drugs like heroin or No.4, Marijuana or Ganja and Methamphetamine like "World is Yours (WY)" from Laos, Myanmar to India. At the same time drugs as Pseudoephedrine Hydrochloride to Myanmar and China from India. This drug trafficking in itself is a huge task for the police to stop it. Catching of contraband substances is possible due to frequent police checking and operations. Still, this does not ensure the end of the movement of illegal substances as the owner, buyer and seller did not directly involve in dealing with the smuggled goods. They normally do not use the physical mode of communication for money transfers or transactions. Simply, it is not possible to do on cash of that large amount or exchanges of goods in the same place. Understanding these vulnerabilities, using Darknet by the criminals to sell drugs or other illegal consignments cannot be ruled out. So far there has been no case as such; however, the absence of evidence does not mean the activity is not taking place. Maybe there is the likelihood that the police are incapable of tracing the modus operandi of criminals.

Delhi Police arrest one self-styled commander-in-chief of banned Manipur's outfit KCP (MC). The accused reveals the use of e-mails, SMS, and mobile phones in their illegal activities of drug trafficking, extortion, killing people, etc. (What was banned Manipuri outfit's chief doing in Bengaluru?, 2011). Again, another leader of the banned group KCP (PWG) was arrested by the Delhi Police in December 2018 on a charge of threat calls to the CM of Manipur (KCP war group chairman brought to Imphal, 2018).

https://doi.org/10.47362/EJSSS.2021.2210

Table of Cases register to Cybercrime Police Station Manipur from 24th June to February 2019:

Complaint Type	No. of Complaints Regd.	No. of Complaints Closed
Hacking	15	9
Economic Offence	238	148
Threat	77	52
Social Media Related Crime	208	140
Total	538	349

Source: Manipur Cyber Crime Police Station (as given at Author's request)

According to the report of the National Crime Records Bureau (NCRB) 2016, 11 cybercrime cases were reported in Manipur (NCRB, 2018, p. 417). The NCRB somehow is not releasing the new yearly report. Still, with a report from the Cybercrime Police Station Manipur which is displayed in the above table. It is easily translated as the number of cases reported is increases with the establishment of the cybercrime police station. Cyber Crime Police Station, Manipur was established on 24th June 2017. But before that two cybercrime police units were established in Imphal West and East in July 2013 (Laithanbam, 2013). From the report, it is magnificent that Manipur Cyber Crime Police Station able to be solved nearly 65 percent of the reported case. The Officer-in-Charge also informs that 23 were arrested for cybercrime under IT Act and IPC. Fourteen were arrested for sexual harassment; three were arrested for threatening on call and SMS (Short Message Service); five for impersonation and one for Nigerian Fraud. This shows the Manipur Cyber Crime Police Station its worthiness.

Manipur police's Cybercrime units were fast in arresting a Babua Thakur for sending and making threats viral video in Bihar (Remand for hate video kingpin, 2018). There are cases of arrests of a pervert by Manipur Police to date under the "cyber-law" and cybercrime for uploading pictures of a girl without dresses, in compromising position without the permission of the girl in social media. Such steps are good and worthy action of Manipur Police Cybercrime branches. But Still, cybercrime police cell is unable to solve Muslim clergy hate speech and depredatory words to other communities (Bewildered Manipur police cyber cell, 2016).

Legal and Constitutional Framework to face Cyber-Crime:

Manipur Police have stated that they used the IT Act 2000, IT Act 2008, IT Rules 2011, and IPC Sections. IPC Sections the Cybercrime Police used are 34, 124A, 383, 419, 420, 463, 499, 500, 503, 506, and 509. IPC Section 34 on cybercrimes cases were acting are done by a group of people in furtherance of common interest or intention. IPC Section 124 A is used on Sedition cases. IPC Section 383 is applied to web-jacking cases. IPC Section 419 is applied to cheating by personation cybercrime cases. IPC Section 420 is applied to bogus websites and cyber fraud cases. IPC Section 463 is applied to the forgery of electronic records. IPC Section 499 is applied to sending defamatory messages. IPC Section 500 is applied to e-mail abuse cases. IPC Section 503 is applied to sending threatening messages cases. IPC Sections 506 is applied to cases of criminal intimidation. IPC Section 509 is applied to cases of any act that insult the modesty of a woman.

India IT ACTS are used on these offenses like 'tampering with the computer source document, computer-related offences, cyber terrorism, transmitting or publication child pornography, failure to preserve records, refusal to comply with orders, failure/refusal to decrypt data, trying to access protect the system, misrepresentation, breach of confidentiality and privacy, publication of false certificate, fraud, and offence or contravention committed, offensive messages, receiving stolen computer resources/ communication device, identity thief, cheating by personation using computer resource, violation of privacy, upload of any pornographic material, and disclosure of information in breach of lawful contract'.

IT Rules 2011 are used to compile cooperation from the Banks, CERT-In, Cyber-café, Internet Providers, Mobile Service Providers, and Mobile Wallet Companies. With all these IT Acts, IT Rules and IPC Section help Cybercrime Police Station Manipur to solve cases reported to it.

Effect of Social media and its management by Manipur Police:

Currently on the ongoing Covid crisis many Bharatiya Janata Party's leaders at both national and state-level express, advice, and projected cow-dung and cow-urine as a cure to Covid-19 through various mediums. One unelected political Leader 'Leichombam Erendro' of Praja Party and one 'Wangkham Kishorechand' a journalist were arrested and put in lockup for citing that "Cow-dung and Cow-urine are not a cure to Covid-19, but Science and Common sense are a cure to Covid-19" in their respective Facebook post (Two held, remanded to police custody for FB post, 2021). These two individuals were arrested under the National Security Acts, section 153-A, 505(b)(2),

295-A, 503, 504, and 34 of IPC. One can assume how the IT-Acts, IPCs, IT rules, Telegraph Act, National Security Acts are used by Manipur Police for crime prevention, control on fake news and rumours, and social control.

In 2008, it has been observed that many social agitations in Manipur against the state government are being aggravated by social media. For example, the case of recent student-supported-by public agitation against the then Manipur University Vice-Chancellor crippled the state for many months (June-October 2018) and almost triggered communal clash based on the line of the unscheduled tribes and Scheduled Tribes. The issue which should stay inside the campus of the university comes out on all fronts. This is a classic example of how an issue of university owing to improper management of social media spread to the whole state like the butterfly effect. The government resolved to shut down the internet for days due.

In another interesting instance, a reporter was arrested in November 2018, for criticizing the present state government by using the slang "F-words". While he was arrested for misusing cyberspace (spreading hate speech through media), he was later booked under the National Security Act. Many human-right groups considered that as misused of Acts and Laws by the Government (India: Release Manipur journalist Kishorechandra Wangkhem and stop repeated crackdown on dissent and democratic space, 2018).

The fourth case out of missused of IT- Acts, IT Rules, Telegraph Acts, etc. is the arrest of six teachers and twenty-one students for throwing eggs at the posters of politicians and upload in Facebook (PRJA man arrested on frivolous charge of throwing eggs on portraits of politicians still interned, 2018). Another of such is the arrest of a leader of Manipur Student's Association Delhi (MSAD) by Delhi Police and Manipur Police under IPC Section 124 A for a Facebook post against the Citizen (Amendment) Bill 2019 (Student Leader From Manipur Arrested Under Sedition for a FB Post, Whereabouts Unknown, 2019).

The common denominator of the above cases is the upload of a video or comments on social media. Maybe due to which all are arrested under cybercrime and IT Acts. Still, individuals are arrested under which IT Acts is yet to be established. Right to express and IPC Sections are seen clash many times in the Cyberworld. And many Police official seem unaware of Indian Laws and Acts or constitutions.

https://doi.org/10.47362/EJSSS.2021.2210

On 25th February 2021, the Government of India announces new social media rules and regulations as a means to curb its misuse like a hate crime, sexual offence, etc. in the form of "Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021" which many terms as draconic ana a threat to democracy with big brother attitude. Citing that rules, as based a district magistrate, serves notice to two senior journalists for their online discussion titled "Media Under Siege: Are Journalists walking A Tight Rope" on 28th February 2021 (Leaflet, 2021). Later Amit Khare, Union Information and Broadcasting Secretary inform Manipur Government that only the Ministry of Information and Broadcasting can issue a notice under these rules.

It is most probably Manipur police seem working very hard to employ the use of new technology to counter the cyberspace disturbance to society for smooth functioning but looking and studying many news reports the use of new IT rules, IT Acts and old IPCs seem inappropriate at times. These lead to the question of Manipur Police to explore more on legal and constitutional aspects of cyberspace, IT Acts, and IPC Sections to efficiently handle crimes on cyberspace and in some cases in connection with other crimes; and countering vulnerabilities in Darknet which is lurking behind in the Cyber Space. In Manipur which is already under Disturbed Area Acts and Armed Forces Special Powers Acts (AFSPA), and twisted use of IT rules, IT Acts, Telegraph Acts, and IPCs by Manipur Police and other authorities make Manipur a perfect example of Police-State within a Democratic Republic structure of Government.

Observed hardware, the office of Cybercrime branch in Manipur head office:

The Officer-in-Charge informed that a state of art Cyber Forensic Lab is going to establish soon at FSL, Pangei and that will remove some hurdles faced by the department in handling cybercrimes. On 28th September 2017, the Ministry of Home Affairs sanctions Rs. 1,48,00,000/ for construction of Cyber Forensic Lab cum Training Centre under the project of Cyber Crime Prevention Against Women and Children (CCPWC) (Affairs, DETAILS ABOUT CCPWC (CYBERCRIME PREVENTION AGAINST WOMEN AND CHILDREN) SCHEME, 2021) and another 2,75,000/ for capacity building on 12th March 2018 under the same program (Affairs, DETAILS ABOUT CCPWC (CYBERCRIME PREVENTION AGAINST WOMEN AND CHILDREN) SCHEME, 2021) There was no visible complex hardware in the premise of the Cyber Crime Police Station of Manipur when the authors visit premise on 2019. It was working

like a normal office. There were only two desks top, few laptops (maybe personal), one monochrome laser printer and an inkjet colour printer. The officers were mostly sitting together in a circular arrangement. This shows how hard the Cyber Crime police unit must be working upon on their cases with such a situation where lack of facilities was seen. Or they are just forced to outsource most of the cybercrime cases to other state police and depend on other actors to corporate for investigation.

Conclusion

India has its official program to surveillance to monitor its citizen and people in form of the 'Central Monitoring System' (CMS) under Rule 419A which is based on Section 7 of the Indian Telegraph Act, 1885. Under which all mobile operators or telephone companies or internet providers to install an interception provisioning system installed by the Centre for Development of Telematics (C-DOT) and operated by Telecom Enforcement Resource and Monitoring Cells (TERM) (Telecommunications, 2012-2013; Addison, 2015). According to a report by the 'Reporters Without Borders' which was published by Indiatoday cited "India top three worst online spy on citizen and journalist" (Forget NSA, India's Centre for Development of Telematics is one of top 3 worst online spies, 2014).

By definition itself, Cybercrime is very vast and vague, plus it is relatively new but still able to hit the Cyberworld and physical world, hard in all sense. Like India, most of the countries in the world; must be struggling to provide a balance between cybersecurity, privacy, and copyrights. Even if India is still a developing country it manages to solve 40 percent of cases registered which is high given the circumstance of India as a country. With 60 percent unsolved cases, many reports are showing India as a hub of Cybercrime activities and home to thousands of drug seller platforms in the Darknet.

India is one of the 33 countries that have a "3rd Party" agreement or "Rampart-A" under which the United States National Security Adgency (NSA) is allowed to spy on Indian citizens (Purkayastha, 2014). With Basic Exchange and Cooperation Agreement (BECA) and the Communications Compatibility and Security Agreement (COMCASA), India is giving free hand United States to Spy in and around India (Khumancha, 2020, p. 188). India in its effort to install a hi-tech border surveillance system and high-speed communication system across India required to share its data

with United States (Sharma, 2019). With all these and still, India does not consider this condition as a violation of its sovereignty. On the other hand, there is no established evidence of spying through Chinese software like TikTok, Alibaba, mobile legends, pubg, etc. but were considered as a threat to India's National Security and ban in 2020. Even the United States fail to prove any backdoor system of Chinese hardware, under United States' advice India deems Chinese hardware as a threat to India's National Security. This may be out of context but did India lost its independent foreign diplomacy, This is a huge Question.

India has been considered as Mecca or Vatican City of online scammer and fake call centers and other cyber offences. Yet at the same time, India is one of the most regulated cyber systems in the world. On monitoring or surveillance to its on citizen, India is always a top three from various sources in one report it curbs with the United States and the United Kingdom; and in others it is curb will China and Russia as most surveillance country in the world. Here, future researchers should try to find the reason why such contradictions exist in India.

India as a country still unable to understand, "what is security and for whose cybersecurity is, what is cybercrime" in practical life. India perhaps got the most well-defined definition of Cyber Security, but when it makes laws for such it at times crosses the human rights like expressions, speech, religion, culture, etc. As India is also the country with the most abusive use of internet kill switch and unclear rules make more trouble for India. The recent sudden call of banning Chinese Apps makes look India a more authoritarian state. With the addition of new rules in 2021, many are pointing fingers.

Even though Manipur is plagued with separatists' movements, civil unrest, drug trafficking, ethnic conflicts, communalism; Manipur police Cyber Crime units have been able to solve more than sixty-five percent of registered cyber cases using IT Acts and IPC Sections. There are instances where the Manipur Police Cyber Crime unit unable to solved or registered cases of communal nature, which may be due to political pressure and which they will deny.

At times Human Rights groups question the activities of Manipur Police Cyber Crime units like the instance of arrest of a reporter, egg thrower to posters, critic to Citizen (Amendment) Bill, etc. for posting videos of expression in Social Media. So many Human Rights groups feel that the Manipur Police Cyber Crime units are used and manipulated by Political hegemony to get their

desired result and working conditions, for which many police cases and newspaper reports are self-evident.

At end of this paper, this paper wishes to suggest that "India's Central Government as well as States Government to give basic knowledge of Indian Constitution, IT Acts, IPCs and IT rules to its law regulatory bodies employees and other concern departments employees. To uphold the democratic principle of the Republic of India". Without the basic understanding of the Indian Constitution, IT Acts, and IPCs resulting abuse of powers in many cases as mention in the paper and in some case denial of justices which fail to reports as police's cases. In the words of Addison Litton "India, the world's largest democracy could devolve into an Orwellian State".

References

Addison, L. (2015). The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression. *Washington University Global Studies Law Review, Volume 14, Issue 4 Global Perspectives on Colorism (Symposium Edition)*, 799-822.

Affairs, M. o. (2021, May 21). *DETAILS ABOUT CCPWC (CYBERCRIME PREVENTION AGAINST WOMEN AND CHILDREN) SCHEME.* Retrieved from Ministry of Home Affairs: https://mha.gov.in/sites/default/files/AndharaPradesh_11052018(3).pdf

Affairs, M. o. (2021, May 18). *DETAILS ABOUT CCPWC (CYBERCRIME PREVENTION AGAINST WOMEN AND CHILDREN) SCHEME.* Retrieved from Ministry of Home Affairs: https://www.mha.gov.in/sites/default/files/AndhraPradesh_11052018(2).pdf

Ball, J., Harding, L., & Garside, J. (2013, August 02). *BT and Vodafone among telecoms companies passing details to GCHQ.* Retrieved from The Guardian: https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq

Bewildered Manipur police cyber cell. (2016, July 23). Retrieved January 26, 2019, from E-Pao: http://e-pao.net/epSubPageExtractor.asp?src=news_section.editorial.editorial_2016.Bewildered_Manipur_police_cyber_cell_IT_20160723

Brodkin, J. (2020, 11 02). The *US says it can prove Huawei has backdoor access to mobile phone networks.* Retrieved 04 05, 2021, from ArsTechnica: https://arstechnica.com/tech-policy/2020/02/us-gave-allies-evidence-that-huawei-can-snoop-on-phone-networks-wsj-says/#:~:text=US%20officials%20say%20they%20have,Street%20Journal%20article%20published%20today.&text=US%20officials%20said%20they%20have,equip

Convention on Cybercrime. (2001, November 23). Retrieved August 23, 2019, from https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Cybercrime cases in India are under-reported, say experts. (2017, December 13). Retrieved August 20, 2019, from live mint: https://www.livemint.com/Politics/kmE7EC9twVDn3DSIZlH8QM/Cybercrime-cases-in-India-are-underreported-say-experts.html

Darknet. (n.d.). Retrieved August 24, 2019, from Techopedia: https://www.techopedia.com/definition/2395/darknet

Department, S. R. (2019, January 18). *Cybercrime in India - Statistics & Facts.* Retrieved August 24, 2019, from Statista: https://www.statista.com/topics/5054/cyber-crime-in-india/

Forget NSA, India's Centre for Development of Telematics is one of the top 3 worst online spies. (2014, March 12). Retrieved from India Today: https://www.indiatoday.in/india/story/indias-centre-for-development-of-telematics-worst-online-spies-reporters-without-borders-184570-2014-03-12

Gellman, B., & Poitras, L. (2013, June 07). *U.S., British intelligence mining data from nine U.S. Internet companies in the broad secret program.* Retrieved from The Washington Post: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

GoI. (2000). *THE INFORMATION TECHNOLOGY ACT.* Retrieved August 23, 2019, from https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf

GoI. (2008). *The Information Technology ACT.* Retrieved August 23, 2019, from http://nagapol.gov.in/PDF/IT%20Act%20(Amendments)2008.pdf

Greenwald, G., MacAskill, E., Ball, J., & Rushe, D. (2013, June 07). *NSA Prism program taps in to user data of Apple, Google, and others.* Retrieved from The Guardian: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

India, a key hub for illicit drug trade; use of darknet, cryptos rampant: UN body. (2019, March 05). Retrieved August 22, 2019, from Hindu Business Line: https://www.thehindubusinessline.com/news/india-a-key-hub-for-illicit-drug-trade-use-of-darknet-cryptos-rampant-un-body/article26440255.ece#

India: Release Manipur journalist Kishorechandra Wangkhem and stop repeated crackdown on dissent and democratic space. (2018, December 26). Retrieved January 18, 2019, from Forum Asia: https://www.forum-asia.org/?p=27923

KCP war group chairman brought to Imphal. (2018, December 23). Retrieved February 14, 2019, from Imphal Free Press: http://www.ifp.co.in/page/items/54824/kcp-war-group-chairman-brought-to-imphal

Khumancha, O. G. (2020). 'Dynamic Positioning' of India in Indian Ocean Region. In M. K. Shrestha, P. Jaiswal, & M. B. Poudel, *Nepal's Foreign Policy and Emerging Global Trends* (pp. 175-199). New Delhi: G.B. Books.

Laithanbam, I. (2013, July 29). *Manipur Police set up cybercrime units.* Retrieved January 13, 2019, from The Hindu: https://www.thehindu.com/news/national/other-states/manipur-police-set-up-cyber-crime-units/article4964088.ece

Leaflet. (2021, March 02). *Manipur Journalist First Target of New Digital Media Rules, News Outlet Issued Notice.* Retrieved April 5, 2021, from The Leaflet: https://www.theleaflet.in/28321-2/#

Lewis, J. (2018). *Economic Impact of Cybercrime- No Slowing Down.* Santa Clara: CSIS; McAfee.

MHA. (2021, May 12). *CYBER AND INFORMATION SECURITY (C&IS) DIVISION.* Retrieved from Ministry of Home Affairs: https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division

Mitchell, C. (2020). *Cyber in the Age of Trump: The unraveling of America's National Security Policy.* London, New York: Rowman & Littlefield.

Moore, R. (2011). *Cybercrime: Investigating High-Technology Computer Crime.* Oxford: Anderson Publishing.

NCRB. (2018). *Crime in India 2016.* New Delhi: Ministry of Home Affairs.

PRJA man arrested on a frivolous charge of throwing eggs on portraits of politicians still interned. (2018, October 16). Retrieved January 23, 2019, from Imphal Free Press: https://www.ifp.co.in/page/items/52911/prja-man-arrested-on-frivolous-charge-of-throwing-eggs-on-portraits-of-politicians-still-interned/

Purkayastha, P. (2014, July 10). *Indian Intelligence Agencies are Helping NSA to Spy on its Citizens.* Retrieved from Newsclick: https://www.newsclick.in/indian-intelligence-agencies-are-helping-nsa-spy-its-own-citizens

Remand for hate video kingpin. (2018, June 18). Retrieved January 26, 2019, from E-Pao: http://e-pao.net/GP.asp?src=12..190618.jun18

Report: US, Germany spied on countries for decades via Swiss encryption firm. (2020, February 11). Retrieved from Deutsche Welle: https://www.dw.com/en/report-us-germany-spied-on-countries-for-decades-via-swiss-encryption-firm/a-52344255#:~:text=News-,Report%3A%20US%2C%20Germany%20spied%20on%20countries%20for%20decades%20via%20Swiss,authorities%20are%20investigating%20the%20allegati

Reuters. (2014, January 15). *US spy software installed in comp network in India.* Retrieved from Hindustan Times: https://www.hindustantimes.com/world/us-spy-software-installed-in-comp-network-in-india/story-k1TEqolatuHJAhFvVGdEOO.html

Schmid, G. (11 July 2001). *Report on the existence of a global system for the interception of private and commercial communication (ECHELON interception system) (2001/2098(INI)).* Brussels: European Parliament.

Sharma, N. (2019, October 16). *India's among the world's top three surveillance states.* Retrieved from Quartz India: https://qz.com/india/1728927/indias-among-the-worlds-top-three-surveillance-states/

Staff, I. (2019, March 07). *India Loses $18.5 Bn Due To Illegal Business Done Over Darknet: Report.* Retrieved August 23, 2019, from Inc42: https://inc42.com/buzz/india-losses-18-5-bn-due-to-illegal-business-done-over-darknet-report/

Student Leader From Manipur Arrested Under Sedition for a FB Post, Whereabouts Unknown. (2019, February 17). Retrieved March 20, 2019, from The Citizen: https://www.thecitizen.in/index.php/en/NewsDetail/index/3/16303/Student-Leader-From-Manipur-Arrested-Under-Sedition-for-a-FB-Post-Whereabouts-Unknown

Telecommunications, D. o. (2012-2013). *Annual Report.* New Delhi: Ministry of Communication & Information Technology, Government of India.

TimesofIndia. (2019, October 31). *Israeli spyware on WhatsApp 'snooped' on Indian journalists, activists, and others.* Retrieved from Times of India: https://timesofindia.indiatimes.com/gadgets-news/whatsapp-spyware-pegasus-reportedly-snooped-on-indian-journalists-activists-and-others/articleshow/71833377.cms

Two held, remanded to police custody for FB post. (2021, May 15). Retrieved from The Sangai Express: https://www.thesangaiexpress.com/Encyc/2021/5/7/By-Our-Staff-ReporterIMPHAL-May-6-Duty-Magistrate-Imphal-West-remanded-two-persons-to-6-days-po.html

Uchill, J. (2019, November 21). *Russia and China get a big win on internet "sovereignty".* Retrieved March 15, 2021, from Axios: https://www.axios.com/russia-china-united-nations-internet-sovereignty-3b4c14d0-a875-43a2-85cf-21497723c2ab.html

What was the banned Manipuri outfit's chief doing in Bengaluru? (2011, May 10). Retrieved August 23, 2019, from Rediff.com: https://www.rediff.com/news/report/what-was-banned-manipuri-outfit-chief-doing-in-bengaluru/20110510.htm