Abstract
As far as India, the pandemic Covid –19 terrifically undermined the socio-economic life of the people, more than 4 million people lost jobs and pushed into acute poverty, the life of the people is dismal especially people who are working in small and medium scale sectors, industries, commercial and service sectors. Nationwide lockdown declared since March 24, 2020, and except few states in almost all the states, the pandemic is pervasive. The normal life of the people has been redefined and people are pushed to work from home through computer and other electronic gadgets. When more and more people log in to the internet then it is inevitable that there is a spike in the number of cybercrimes also.

Introduction
Covid –19 pandemic rendered global community, especially the migrant population, weaker section and marginalized communities in to extremely vulnerable. The Pandemic affected more than 200 countries around the world, millions of people infected, abysmally died, the casualty is extremely high in the USA, UK, France, Spain and Belgium. As far as India, the pandemic Covid –19 terrifically undermined the socio-economic life of the people, more than 4 million people lost jobs and pushed into acute poverty, the life of the people is dismal especially people who are working in small and medium scale sectors, industries, commercial and service sectors. Nationwide lockdown declared since March 24, 2020, and except few states in almost all the states, the pandemic is pervasive. The normal life of the people has been redefined and people are pushed to work from home through computer and other electronic gadgets. When more and more people log in to the internet then it is inevitable that there is a spike in the number of cybercrimes also. The issue of how to contain cybercrimes during the pandemic crisis is also one of the topics for debate and discussions at the global level.

Drop in Conventional Crimes
As the available data show that, there is a sharp decline in convention crimes such as robbery, drug trafficking, killing innocent people for hefty money, housebreaking etc. For instance, The Hindu newspaper reported\(^1\) in Chicago, one of America's most violent cities, drug arrests have plummeted 42 per cent in the weeks since the city shut down, compared with the same period last. Further, the

\(^{1}\) Professor and Deputy Controller of Examinations, Dept. Of Political Science and Public Administration, Annamalai University
overall crimes in Chicago declined 10 per cent after the pandemic struck. Even in other parts of the USA, fewer people are being killed and fewer robberies are taking place. Law enforcing authorities in the country are much worried about the spike in domestic violence across the country. The same situation is prevailing in Latin America; crime is down to levels unseen in decades. El Salvador reported an average of two killings a day in the month of April, down from a peak of 600 a day a few years ago. In South Africa, the police reported a stunning decline during their first week of lockdown measure. Rapes were down from 700 to 101 over the same period last year. Serious assault cases plummeted from 2,673 to 456, and murders fell from 326 to 94.

**Trends in India**

The Covid-19 pandemic has triggered a huge spike in domestic violence against women in China, Australia, France, UK, Spain, and Bangladesh, among others. In India, too, the National Commission for Women (NCW) has reported a large increase in distress calls from victims of domestic violence since the pandemic broke out. The NCW has launched a helpline number 0721-7735472 to enable those facing domestic violence to send a WhatsApp message to access help. Most of the women are much comfortable with sending messages through WhatsApp than sending an email. That is why the NCW decided to launch WhatsApp helpline number.

**Phishing Racket**

Phishing Racket is a fraudulent attempt by miscreants to steal the valuable data such as username, password, credit and debit card details, Aadhar Card details and other valuable data, what most of the people called as Big Data, from the customer by disguising oneself as a trustworthy entity in an electronic communication. During the pandemic period, the Bank has been sending out alerts to its customers that their staff will never ask for customers CVV, PIN or IPIN numbers. But the scamsters posed as a bank executive and calling the people to furnish certain confidential bank account details to waive EMI or skipping to pay the monthly payment due in the wake of the announcement by the state government, that the Bank should not compel its customers to repay the month EMI for three months. Cyber Crime officials have appealed to the public not to attend calls coming from casters and cyber criminals. Further, they have warned the people against installing screen sharing mobile apps such as Quick Support, Any desk and Team Viewer. Another dimension of cybercrimes during the pandemic crisis is, fake emails floating of bogus accounts seeking monetary contributions to the PM's of CM's relief fund. Chennai city police receive about 40 to 50 complaints online every day since the lockdown began.
Mha Warning

The Home Ministry warned that 'Zoom' – a popular mode for holding meeting via video conferencing – was not a safe platform, the ministry has put out a set of guidelines that users may follow to ensure their safety while using the application for private purpose. Zoom App was designed in the USA but the software being used in the App is developed by the Chinese company. It was alleged that certain calls, video, data or any other information shared in the platform will go to servers located in China or in other words the Chinese company or government can access the data shared or published in the Zoom app. The government advocated enabling of waiting room so that every user could enter only when the host conducting the meeting admits the person. It suggested disabling 'join before host' and allowing screen sharing by host only.

Hate Speeches in the online

Now a day the social media platforms such as WhatsApp, Facebook, Instagram, Linkindia, Quora etc. have become a perfect tool for spreading hate politics and creating social disharmony among various communities. Social media users, especially users in platforms like Wikipedia, Quora, Facebook, WhatsApp and Twitter, are waging war against communalism in the wake of covid-19 pandemic cluster across the country. Much of the outrage is being led by social media users in the Arab world. In some instance, netizens in the Gulf countries who published blatantly communal posts have lost their jobs and many even face police action for hate speech in the online platforms. A company in Sharjah has warned its employees that, anyone openly racist and discriminatory in the country will be fined and made to leave. The Wikipedia too has deleted a page posted by a writer about covid-19 epidemic. Jimmy Wales, the founder, said that, “the article was incredibly poor written and zero sources”. Similarly the Quora, another platform, removed several inflammatory questions on the site.

Children and Women are Vulnerable

Children and women are also victims of online crimes during the pandemic period. The Hindu dated April 14, 2020 stated that online child porn traffic rises by 95 per cent after the lockdown. With online data monitoring websites showing an increase in demand for searches like "child porn", "sexy child" and "teen sex videos". Online traffic from India was increased to 95 per cent between March 24 and 26, 2020, as compared to average traffic before the lockdown", the India Child Protection Fund (ICPF) said in a statement citing the data obtained from Pronoun, the world's largest pornography website. The women and child are vulnerable to cyber crimes like online
pornography as during the lockdown period the women and children are spending most of the time with mobile phone and other electronic gadgets connected with internet. International agencies such as UNO, Europol, ECPAT (End Child Prostitution and Trafficking) have reported a huge spike in porno traffic on the internet especially after the worldwide lockdown announced. The agencies and social activists have called the government at the worldwide to take an urgent note on this issue and take stiff actions to curb the menace of child and women pornography in the online. The defaulters know that, under section 156 of the POSCO Act, a person who stores child porn for the commercial purpose shall face imprisonment for up to 3 years or will have to pay a fine or face both punishments. But the lukewarm response from women and children, fear that their right to the internet will be curtailed by their parents if they report the cases police, undermines the spirit of the POSCO act and in most of the cases the defaulters were not punished. Significantly the Kerala police have cracked a cybercrime on fast-track by tracing a 19-year-old Instagram user who allegedly misused the profile photos of more than 15 girls from various parts of Kozhikode district and circulated them widely through his fake accounts with derogatory comments\textsuperscript{10}. The youth was charged under Information Act 2008\textsuperscript{11} for circulating photos without the concern of the girls with derogatory comments. The Indecent Representation of Women (Prohibition) Act 2013 also seeks to broaden the scope of the law to cover the audio-visual media and content in electronic form, prescribing stringent penalties which would act as a deterrent to violation of the law. As per the Act, the distribution of material will also include distribution on the internet. Under Section 354A of the Act, any demand for sexual favors/showing pornography against will is punishable. Further section 354C prohibits disseminating such information without the consent of the women or girl. Section 354D deals with cyber stalking, despite clear indication of disinterest, or monitoring cyber activity. Further, the bill enhances penalties for various offences. For representing women indecently, the penalty for the first offence was increased to imprisonment of three years from two years and a fine between Rs 50,000 and Rs 1 lakh from Rs 2,000. For a subsequent offence, the term of imprisonment shall be between two and seven years and a fine between Rs 1 lakh and 5 lakh\textsuperscript{12}. But despite strong Laws number of persons arrested and punished for cybercrimes, especially against women and children, is very meager. Women, children and other stakeholders in the society need to be sensitized about the existing legal mechanism and various Acts to protect them from any kinds of cybercrimes.
**Shrinking Cyber Space for Women and Children?**

Human Rights activists around the world compared cyberspace with the public sphere. Hence, any forms of online women's rights violations are equivalent to harass women in the street or public. The major focus here is how to expand safe space for women to express their views, opinion freely without any external aggression. Women themselves adopt numerous strategies to deal with abuse online. These include ignoring it, moderate comments on forums that allow this, blocking persistent or vicious abusers, reporting abusers, looking for and find support, naming and shaming, taking abusers head-on, and self-censorship. Women refuse victimhood in these situations, instead of turning to their resource or online communities of support.

**Hackers target Health Research Data**

In the wake of Covid – 19 numerous research is being conducted all around the world to develop vaccination to fight against the pandemic. The Hackers lure to setting up fraudulent internet domains, promised to supply masks and medical relief materials and types of equipment, and then deliver fraudulent loans, extortion etc. In addition to regular cybercrimes, the Federal Bureau of Research (FBI) reported that attempt was made to target the US national healthcare sector and the US' Covid-19 research capabilities. The hackers are largely from countries having the desire for covid-19 related research information, vaccination being developed by the countries in their laboratories and simply they wanted to know what is happening in the health care system in all around the world, especially the USA\(^\text{13}\). There are a considerable number of registered domains on the Internet that contain the terms: "corona virus", "corona-virus", "covid19" and "covid-19". While some are legitimate websites, cybercriminals are creating thousands of new sites every day to carry out spam campaigns, phishing or to spread malware.

**Malware**

Cybercriminals are taking advantage of the widespread global communications on the corona virus to mask their activities. Malware, spyware and Trojans have been found embedded in interactive corona virus maps and websites. Spam emails are also tricking users into clicking on links which download malware to their computers or mobile devices.

**Ransom ware**

Hospitals, medical centers and public institutions are being targeted by cybercriminals for ransom ware attacks – since they are overwhelmed with the health crisis and cannot afford to be locked out of their systems, the criminals believe they are likely to pay the ransom. The ransom ware can enter
their systems through emails containing infected links or attachments, compromised employee credentials, or by exploiting vulnerability in the system. With an increasing number of countries encouraging citizens to stay, learn or work from home, now is the moment to focus on cyber security, whether it's for yourself or your workplace.

i. Keep all the information very safe by developing back up files stored in the cloud or an external drive.

ii. Always be careful in log in to the website and make sure that it is a legitimate website before entering login details.

iii. Have a strong password and try to change the password frequently.

iv. Developing a vibrant firewall in the computer is also another way to combat cybercrimes.

v. Ensure that you have installed original not pirated anti-virus software in your computer and mobile devices. Periodically scanning of the entire system is also essential at this juncture.

vi. Secure email gateways to thwart threats via spam

vii. Download software or mobile applications from the only trusted site only.

viii. Regularly check updates and privacy setting in your computer and other electronic devices.

ix. Don't connect your mobile phones or computers/laptops with public wifi which will pave way for transferring all the data stores in your computers to the third party.

x. Sensitize various stakeholders, including your kids and spouse, about various forms of cybercrimes and how to combat it.

xi. Do not click on links or open attachments in emails which you were not expecting to receive, or come from an unknown sender.

It is worth to mention here that, the official website of Karnataka Government has advised all citizens, especially the women and children, to be conscious of any possible violations of their rights in the online world and suggested some of the safety tips to protect their rights also. The following are guidelines suggested by the government:

i. Remember that all other internet users are strangers.

ii. Be extremely careful about how you share personal information about yourself online.

iii. Be extremely cautious about meeting online friends in person.

iv. Save all communications for evidence.

v. Be aware of all e-mails and SMS from any stranger

vi. Be sure that your WIFI Network secured, use a strong password.
vii. Never share your passwords with anyone.
viii. Change the password frequently
ix. Never forget to sign out of your email or any other accounts.
x. Never reveal your personal information to any stranger in online chatting.
xi. Watch for 'https' in the address bar.

xii. Never post sensitive information in social networking and marriage sites.
xiii. Never be greedy for free downloads. They might infect your computers.
xv. Don't share your personal information, photos and other secret information on Face book, Whatsapp, Twitter, Link India.....with others.
xvi. Don't share your ID, password, PIN nos... to others.

Conclusion
As has been very clear from the foregone discussion that, Covid-19 pandemic crisis period witnessed a huge spike in the number of cybercrimes all over the world, including India. Conventional crimes such as robbery, killing of people for personal gain, housebreaking etc. declined considerably. The nationwide lockdown and subsequent government instructions to people to work from home certainly paved the way for surge in cybercrimes. When more people log in to website, especially the children and women, then the risk of cybercrimes is imminent. The cybercriminals, hackers, casters etc. target Covid-19 related research data and countries advancement in finding out vaccination also. Data related to Covid-19 affected patients and the kind of treatment being rendered to them are more vulnerable at this juncture. Social media users, especially users in platforms like Wikipedia, Quora, Facebook, WhatsApp and Twitter, are spreading the virus of communalism in the wake of the covid-19 pandemic cluster across the country. Political analyst believed that, more than spreading virus in the computer spreading virus of communalism through social media is a potential threat to the secular fabric of the society and certainly it will have a deep impact and cleavage in the society. Hence, it is imperative to curb such menace in the online platform immediately. The government needs to encourage ‘Ethical Hackers’ to combat cybercrimes. The guidelines issued by the UNO and other agencies are worth mention here. People and other stakeholders should be sensitized about safe surfing on the internet are essential and inevitable at this juncture. By creating awareness about evils of cybercrimes,
checking anti-virus status, checking privacy settings, frequent changes in the password alone can minimize the occurrence of cybercrimes.

References
2. Ibid.,
5. A person who commit mistakes and participate in dishonest business
8. On Wikipedia, Quora & Twitter, battle rages against Communalism, Times of India, April 22, 2020.
11. Under Information Technology Act 2008 Section 66C: any identity theft is liable for punishment. Under Section 66E: any attempt to violate the privacy of the girl or women will invite punishment and imprisonment. Section 67 of the act deals with publication and transmission of obscene content, Section 67A: publication and transmission of sexually explicit material, Section 67B: publication and transmission of child pornography and Section 72 deals with breach of privacy and publication of material without consent of the girl or women.
15. An ethical hacker is an individual hired to hack into a system to identify and repair potential vulnerabilities effectively preventing exploitation by malicious hackers .https://www.techopedia.com/definition/16089/ethical-hacker.