Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/13404
DOI URL: http://dx.doi.org/10.21474/IJAR01/13404

ISSN NO. 2320-5407

RESEARCH ARTICLE

IMPACT OF CYBER LAW IN MODERN ERA WITH ADVANCEMENT IN TECHNOLOGY AND PROTECTION FROM RISING THREATS OF CYBER CRIMES IN OUR SOCIO ECONOMIC SECTOR

Dr. Sumanta Bhattacharya[1], Bhavneet Kaur Sachdev[2] , Arpan Kundu[3]

1. Research Scholar At MAKAUT, Public-Foreign-Defence Policy Analyst , C.E, CH.E , M.Tech, LLB.
2. Political Science Hons (Calcutta University), Masters in Development Studies.
3. BA LLB (Hons) Calcutta University, Business Professional Programmer, Diploma in Computer Application.

Manuscript Info

Manuscript History
Received: 14 July 2021
Final Accepted: 18 August 2021
Published: September 2021

Key words:-
Cyber Space, Gaming Industry, Cyber Law, Phishing, Spamming, Cyber Warfare, Digital Economy, Economy

Abstract

Cyber space industry has made massive profit during this pandemic with everything going online along with the electronic industry in India , Today , Asia has the maximum population playing video gamers, the gaming industry is earning in billions , digital education , digital economy , work from home everything went online over night , which gave rise to cyber crime cases in India . India data is vulnerable and there is no cyber law which talks about privacy , more than 50% of the population lost their sensitive information online , there was cases of online job frauds and debit and credit fraud . The cyber law in India requires reform where phishing and cyber warfare are given legal protection in India , DATA protection , privacy and spamming requires legal attention . Banks are sensitive to cyber criminal because of the poor cyber security system and not so strong cyber laws which has affected the economy , people have lost many in lacs in these months , The cases of risen in 2020 to 2021 . India also needs to upgrade its cyber security policy and bring in professional in this field .

Introduction:-

With the evolution of Internet , technology, social media taking grounds from the early 2000s more and more people have joined Facebook and other social media platform over the years . People identify is becoming public and so are their information which is spreading across the globe . Technology has numerous benefit where you can get in touch with anyone in this world through Internet . It is the age of globalization , we are entering a world of Digitalization and technology where no country is left behind . Digital education and digital economy is ruling the Industry , Everything is happening one -platform which has also open doors for cyber crime . Today we are experiencing cybercrime at a rapid rate every minute a cyber crime happening in any part of the world .With the launch of video games over the past few years , around 5 billion people play video games where we interact with new people, share our personal information , there are cyber spy sitting across the world , operating from a different country and the head office is in a different country . So many bank fraud happens , ATM details reaches the criminal in no time . They want through hidden web , there are different sites about which very few are know , the 21st century is being ruled by the cyber space , and today we are facing cyber terror . India has been a victim of cyber attach more than 40,000 times from China . Mumbai is a victim of cyber warfare .However much can't be done when it comes to cyber warfare , until we have a proper infrastructure and a cyber security system . In India the cyber security is not safe , the data is vulnerable , job frauds , credit and debit card frauds case have made the life of

Corresponding Author:- Dr.Sumanta Bhattacharya
Address:- Research Scholar at MAKAUT, Public–Foreign-Defence Policy Analyst, C.E, CH.E, M.Tech, LLB.

people miserable , where as criminals are trying to hack banking websites .Over the years we are seeing that is the young generation who are vulnerable to cyber crimes . Through Facebook , YouTube pages , dating apps people are gathering information about people and then there is a seen cyber attack . Hacking is the most common way to get information and it's a criminal offence . We can simply define cyber crime as an criminal offence which is conducted using Internet through the tools like computer , laptop ,telephone . Digitalization has made our life simple and easier , we are 24*7 depend on Internet , the way we talk , majority of the people today Interact over WhatsApp than on phone calls , for every single study material we are depended on technology , YouTube has also been a platform for many people to earn , Cyber space is earning in billions with that cyber crime is also intensifying in India . From shopping to purchase grocery or for medicine to doctor appointment to booking of ticket both railways and airline everything happens on an online platform where aadhar card details , debit/ credit details , bank account details , PAN card everything is shared and it wont take time for criminals to get access to information in seconds through certain apps .

Objective of the Research Paper:-

1.A study on the rising cyber crime cases in India and cyber warfare.
2.Impact of cyber laws in combating cyber crimes and the loopholes in Cyber laws in India .
3.Why India needs to upgrade its Cyberlaw .

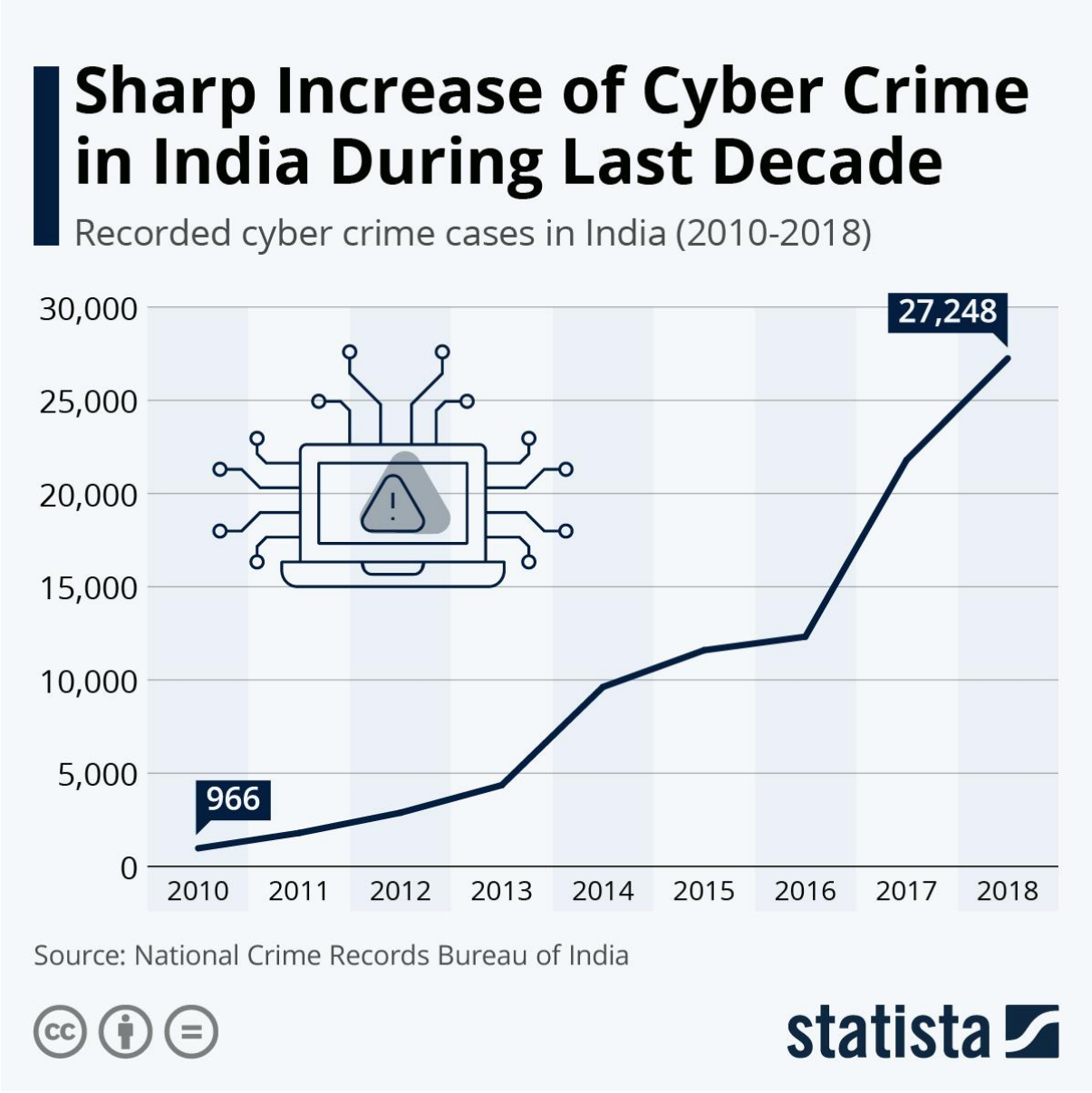
Analysis

When Internet was first brought into use , no one knew that it could emerge as a platform for criminal activities . Today we are dependent on cyber for everything out of which millions of people have become victim of these illegal cyber activities . To prevent cyber crime and right of the Internet users , the India government brought the Information Technology Act of 2000 .There are many sections in this act which protect and empower a user to protect him/her from cyber crime. Section 65 when a person try to alter or destroy any computer source ,the offence is imprisonment for 3 years and a fine of 2 Lakh has to be paid , Section 66- if a person uses password or digital signature or any Identification card fraudulently , he/she is punished for a period 3 years with a fine of 1 Lakh . Section 66E – if a person cheats using a computer resource or device on someone , the punishment granted is imprisonment and 3 years of fine , Section 66F deals with act of cyber terrorism – in which if a person is caught , he /she shall have to face lifetime imprisonment, intent to threaten the unity , integrity , security and sovereignty of India or strike order . Knowingly or unknowingly access information , data or data base where access is restricted for reasons of security of the state or foreign relation , injury to interest of sovereignty and integrity of India , security of the state , friendly relationship with foreign nations, public order , or decency or morality .Contempt of court or defamation or incitement to an offence or to the advantage of any foreign nation or group of individuals , example 9/11 attack of 2001 , hacking , defence , railways or any government sites. Section 67 -publishing of obscene material on e platform where the punishment is of 3 years and fine up to 5 Lakh , section 67A deals with uploading of material containing sexual explicit in e- form , for the first time the punishment is of 5 years and a fine of 10 Lacs followed jail of 7 years if the crime is committed for the second time and the fine remains same whereas Section 67B deals with crime where a person has uploaded material depicting children in sexual activities , in short child pornography where the punishment is same as for Section 67A . Where as section 67C , 68 , 69 , 69A , 69B and 70 deals with deals with cyber crime relating to violation of directions of government or other competent authority -intermediaries , certifying and authorities followed by Monitoring , regulating and blocking of content , encryption or decryption of content . Unauthorized access to a protested system , critical information violating the direction of CERT-IN , Offences relating to digital signature and electronic signature certificate

Section 43 cover penalty and compensation Sector 43(a) secures access comprising tracking computer , computer trespass and violation of privacy , banks are generally found liable under this section , Section 43(b)-covers downloads m copies or extract any data , data base or information , this clause is applied against former employers who are suspected to have copied data from the previous company , Section 43(c) includes introduces or causes to be introduced any computer containment or virus . Section 43(d) -damage or cause to be damaged any computer , computer system , network data , data base or any abuse . Section 43(e)-disrupts or causes disruption , section(f)-denies or caused denial of access to any authorized person , followed by which we have section 43(g)(i)(j) dealing with delete and steal of important documents .Section 44 deals with penalty for failure to furnish information ,return etc .Section 45 covers residuary penalty .

The IT Amendment Act 2008 which was a new version of Information Technology Act 2000 focus on data security , info security , defining cyber café , reasonable security protectors , Intermediaries and their role , NCCIIPC and

CERT-IN , Additional crimes like pornography and cyber terrorism and inspector to investigate not DSP .We know the cyber crime and all the laws that prevent or punish criminal ,along with that lets have a look at the different instruments of cyber crime which includes Pornography/CSAM , sexting /Sextortion, DOS attacks , Virus ingestion , Vandalism , privacy , cyber squatting , cyber stalking , cyber grooming , cyber bullying , cyber terrorism , online job fraud , smishing , ransomware , spamming , phishing , Hacking . The types of cyber attack has in India are Financial fraud , employee abuse , inside access , viruses , outsider penetration , theft of property information and sabotage of data/network. Here the targets are individuals , organization and property .



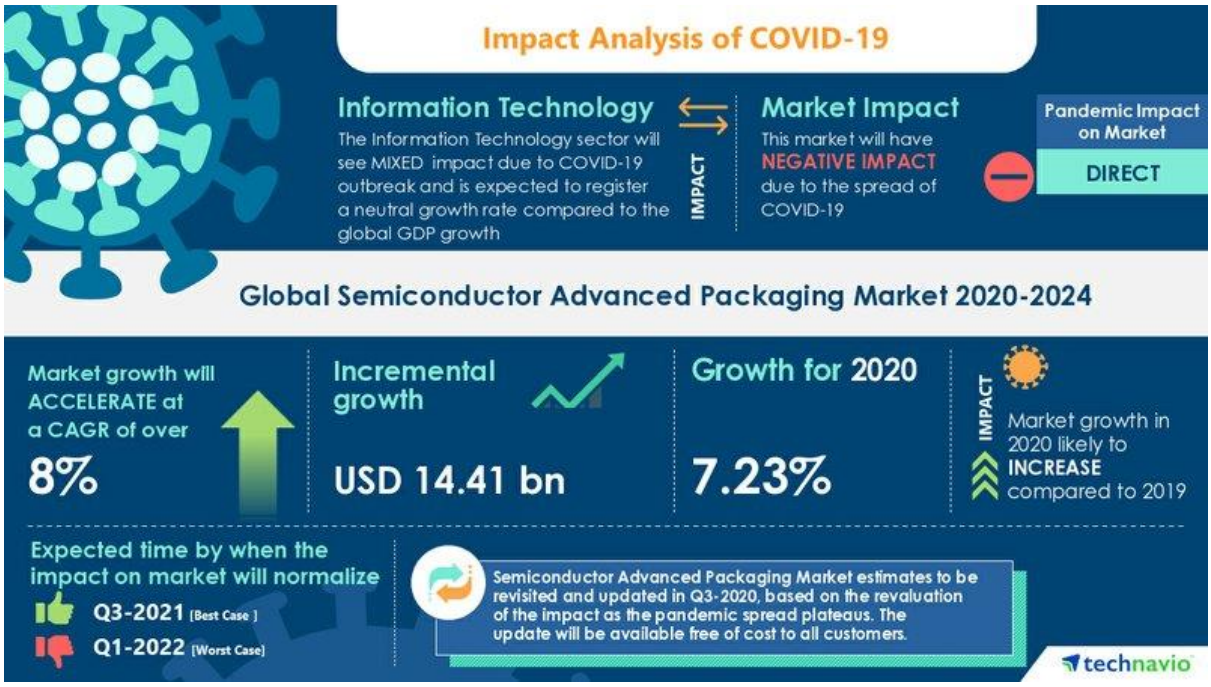
In 2019 , India had 131.2 million victims of cyber crime .In 2020 , 1.24 trillion amount was lost due to cyber crime . 81% of Indian are made aware of privacy .70% of the Indian are worried about their stolen identities . Men are more vulnerable to cyber crime then women, 84% of the men experienced cyber crime and 76% of the women , 63% of the Indians of the 131 million cyber crime victims were impacted financially , 80% of the Indian were victim of cyber crime in some point in their life and 66% were victims in the past year . 41% of the people are concerned about their personal information will reach out to a third person and 86% of Indian are looking for better ways to protect their privacy where as 65 % are globally .Digital India has seen an increase in crime cases , in 2019 -4,4556 cases of cyber crime were reported , 2018 the number was 28248. There has been an increase of 63.5% . With

COVID-19 pandemic taking place we have seen a rise in cases . Every minute there has been cyber crime happening , with the concern of work from home and pandemic , criminals have given rise to fraud jobs where majority of the people have explained financial fraud . As 90% of the people are digitally illiterate they have no clue that the data is vulnerable and what information they should share on the phone related to their bank accounts or asking for OTP .

Highest cases of crime was reported in Karnataka accounting to 12,020 , followed by Uttar Pradesh 11,416 Maharashtra has 4967 , Delhi accounted 78% of the cyber crimes , Telangana had 2691 cases , Assam had 2231 .Digital India concept has brought in new options for criminal , there is online shopping fraud where there is no return policy , sharing of card details while purchasing products

While the act has been successful in setting down the framework of regulation in cyber space and addressing the pressing concerns and misuse of technology , there are certain areas of cyber laws which need attention .First of all according to expert they say that the act have not been completely effective in giving penalties or sanction against preparators .Spamming can be defined as unsolicited Bulk e mail . it was early taken as normal thing but now it is creating major economic problems . In the absence of any adequate technical protection , a stringent legislation is

required to deal with the problem , where the information technology act does not talk about spamming . Phishing is a very common cyber crime activity where sensitive information is like username , password ,documents the activity is an example of social engineering and the crime is done using email , the law does take about phishing , it just means cheating which is not enough to control the activities of phishing .There is no law which talks about data protection , specially in the cases of banks were at a lot of details are exchanged and there is an involvement of a third party . It is not possible for the banks to retain all the information within their network , high risk is involved in preventing leakage . Privacy and data protection are important issue to be addressed and we require more techanical legal protection as every activity happening on online today be it individual , professional and commercial , due to the absences of a specific privacy law , India has lost many foreign investment and other business opportunities .Cyber wars has not been mentioned in the law , India is facing cyber attacks from China for the recent years and there exist no law for such perpetrators liable for their actions.



We have seen a rise in the demand of Electronic products during and post COVID -19 pandemic , the sale of mobile phones have tripled with every 3 mins there is a sale of a phone , companies like realme and one plus have gained tremendous profit , followed by huge demand for laptops , tablets and head phones , companies like HP and Acer has received the maximum profit and demand of laptops . The electronic industry is the future and for a country like India where the cyber security system is still under developed cyber crime is a major issue . Current cyber laws can provide much security to the victims and customers of India , with gaming industry ruling the world are data is becoming more and more vulnerable .

Way Forward

Cyber crimesactivities is happeing every minute in India , with everything going online , with India experiencing digitalization we see a rise in number of cases . There is lack of cyber space knowledge among the Indian in particular among those who live in the semi urban and rural region , including the old age community . India has been a victim of cyber attacks a number of times still we don't have a law for protection . We require a reformation in the cyber law ,where concept like cyber is given utmost importance which is affecting the economy of India and national security , followed by Phishing should be given legal important , an activity which is growing and majority are a victim of this . Laws should focus on cyber privacy . India data is vulnerable and there is no privacy , policy and law for data privacy is the need of the hour in India , followed by new bank cyber facilitates and protection where credit and debit cards fraud is eliminated . We require more cyber professional in the country , where at the school and college courses and chapter in school have in depth study on cyber crime and cyber security , as cyber space is the further of the world and in no time everything will turn digital . Technology advancement will bring in

both positive and negative impact on the society . India in order to protect itself for the further crimes should strength its cyber laws and cyber security measures in specific legal protection for privacy of sensitive information.

Conclusion:-

Cyber crime is very common today , with passing years instruments of cyber crime and types of cyber crime is increasing , playing video games online has provided criminals with the opportunity to get gather more and more information about the person and games where payment is required , they land up in huge lost as small children don't have much clue of cyber crime , using of dark web for the purchase of drugs , made get profit during this COVID-19 situation from YouTube to other websites say great profit . Video gamers industries is running in billions and so is the cyber crime Industry . Young youth is being the victim while some have joined hands with criminal to earn money in a better way . Cyber laws in India need upgradation to stop these activities as it can widely affect thee economy of India through Acts of cyber terrorism and cyber warfare followed by bank frauds , where money is lost in lacs per person and the offence is somewhere outside the country .

Reference:-

1. 1.Digtal Desk , 2020 , September , 63.5% increase in cyber crime cases in India in 2019 , most cases in Karnataka :Republic world .com.
2. 2.Pinto Deepak , 2020 , February , India stands third position among top 20 cyber crime victims. The Indian express.
3. 3.Gunjab Chhabra , Kanika Chhabra, 2014 , November , A study on emerging issue on cyber law , ResearchGate .
4. 4.Jiger shah , 2016 , December , A study of awareness about Cyber laws for Indian youth , Volume 1 , Issue 1 ,International Journal of trends in Scientific research and development .
5. 5.Apoorva Bhangla and Jaganvi Tuli , A study on cyber crime and its legal framework in India , Volume 4 , issue 2 , International Journal of law management and humanities.