CYBERSECURITY AND CYBER LAWS AROUND THE WORLD AND INDIA: MAJOR THRUST HIGHLIGHTING JHARKHAND FOR CONCERNS

Written by ***Dolly Krishnan* & Mohit Verma*****

** 1st Year LLB Student, Faculty of Law, ICFAI, Ranchi, Jharkhand*

*** 1st Year LLB Student, Faculty of Law, ICFAI, Ranchi, Jharkhand*

ABSTRACT

Cyberspace is the connected Internet Ecosystem and it refers to the virtual computer world, and more specifically,the notional environment in which communication over computer networks occurs.When this cyberspace is compromised, this leads to cybercrime and even Cyberterror which is *intended* to undermine the electronic systems to cause panic or fear and even monetary loss. The techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation is called cybersecurity.As a body of UN, International Telecommunication Union releases *Global Cybersecurity Index (GSI)* in which, by assessing certain parameters, it measures the commitment of countries to Cybersecurity at a global level and it has ranked Denmark, Australia, Republic of Korea, in top ten category. India drastically slipped down from 23rd Ranked in 2017 to 47 th rank in the latest GCI ,2018 which is a matter of grave concern and it seeks immediate attention. Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues.

In most nations globally, there are many legislation governing e-commerce and cyber crimes going into different facets of cyber crimes. In Indian context, the IT Act' 2000 which was amended in 2008 and is known as Cyber Law. Though we have seen many new laws, initiatives and policies from the government of India, there are grave threats despite progress. Here, we want to give a brief overview of the cyberattacks , cyberspace encroachment and security concerns around the world and India with major thrust to Jharkhand which came into limelight when one of its city, Jamtara, earned the title of Cyber Crime Capital of India. We

have tried to explore existing legislative dimensions with regard to its effectiveness in handling Cybercrime and possible future perspective for a more digitised and inclusive social order and economy for global growth.

Keywords: Cyberspace, Cyber Threat, Cybersecurity, Cyberlaw , Cybercrime in Jharkhand

INTRODUCTION

A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers has been termed as cyberspace. ***Cyberterror*** is intended to undermine electronic systems to cause panic or fear. ***Cybercrime*** includes single actors or groups targeting systems for financial gain or to cause disruption. To control computers or networks cyber attackers use viruses, worms, spyware, Trojans, and ransomware. Viruses and worms are usually self-replicating and damages files or systems, while spyware and Trojans are often used for surreptitious data collection. Ransomware waits for an opportunity to encrypt all the user's information and demands payment in return of access by the user. Malicious code often spreads via an unsolicited email attachment or a legitimate-looking download that actually carries malware or other sywares.

To counter attack these malicious practices , certain techniques are used which safeguards the electronic devices. The techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation is called **Cybersecurity.** In the Global Cybersecurity Index (GSI), India slipped down from 23rd rank in 2017 to 47 th rank in the latest GCI , 2018 which calls for upgrading and improvisation in the security domain. Here, we have tried to assess cybersecurity and affiliated laws in India, focusing on Jharkhand and have tried to give critical picture for consideration in near future.

NEED FOR CYBERSECURITY

After the world wars, the world realised that wars are no solution and mutual cooperation is the essence of progress together. Thus to ensure peace, global cooperation and concerns in mind, the United Nations (UN) was born in 1945 which comprises almost all the countries in the world. The United Nations serves as a common platform where countries design framework and a time window to achieve the decided goals. It just completed its Millennium development goals (MDGs) in 2015 and it is now striving for Sustainable Development Goals (SGDs) 2030, adopted in September 2015 which aspires to end poverty in all its forms everywhere, end hunger, achieve food security and improved nutrition and promote sustainable agriculture inclusive of its 17 defined goals.

UNESCO conducted a study emphasizing on correlations between SDGs and ICT (Information and communication technologies) which summarises that ICT is directly related to 6 of the 17 SDGs. Studies from Arizona state University bolds out the role of Cybersecurity in achievement of SDGs. It's not only a single study done pinpointing this fact but there are myriad number of research papers stating the similar tone highlighting the importance of cybersecurity as a foundation in the SGD 2030 attainment thus establishing the fact that Privacy, Data Rights and Cybersecurity are the master player in deciding the economical and social progress around the globe .

CYBERSECURITY IN RELEVANCE TO INDIA

India, being a UN member is also striving for SGD 2030 attainment. The Sustainable Development Goals (SDGs) were adopted in September 2015 as a part of the resolution, 'Transforming our world: the 2030 Agenda for Sustainable Development'.

India is devoted to achieve the 17 SDGs and the 169 associated targets, which comprehensively cover social, economic and environmental dimensions of development and focus on ending poverty in all its forms and dimensions.

At the Central Government level, NITI Aayog has been assigned the role of overseeing the implementation of SDGs in the country. To spread awareness about the Goals, bring together

stakeholders and build capacities for the realization of SDGs, NITI Aayog has organized several national and regional level consultations.

CYBERSECURITY ASSESSMENT AROUND THE GLOBE

The Convention on Cybercrime or the Budapest Convention, 2001-

The Convention on Cybercrime or the Budapest Convention is the first international treaty which seeks to address the issue of Cyber Crime.It was drafted by the Council of Europe along with active participation of Canada, Japan, South Africa and the United States of America. It is the only legally binding international instrument on this issue.It was opened for signature in Budapest from 23 November 2001 and it entered into force on 1 July 2004.The convention was formed with an aim to harmonize national laws, improving investigative techniques, and increasing cooperation among nations.It acts as a guideline for any state developing national legislation against cybercrime.India has not adopted the convention and declined to ratify it as it was not a participant in its drafting.India is also concerned with the sovereignty issue that may arise due to data sharing with foreign law enforcement agencies.

Internet Corporation for Assigned Names and Numbers (ICANN): It is a non-profit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation. It has its headquarters in Los Angeles, U.S.A.

International Telecommunication Union (ITU) -

UN , to ensure connectivity in communication networks around the globe, established a body which would facilitate international connectivity in communications networks, develop the technical standards that ensure networks and technologies seamlessly interconnect and strive to improve access to ICTs to underserved communities worldwide, thus International Telecommunication Union (ITU) came into picture.

The International Telecommunication Union (ITU) is a specialized agency of the UN ensuring connectivity around the world networks. To monitor and to keep a track of global connectivity and its security it releases an index annually called GCI.

To assess the countries worldwide in the matter of cyber safety, it takes 5 parameters into consideration that is – (i) legal, (ii) technical, (iii) organizational, (iv) capacity building, and (v) cooperation – For each of the pillars, country commitment was assessed through a question-based online survey, which further allowed for the collection of supporting evidence. Through consultation with a group of experts, these questions were weighted in order to arrive at an overall GCI score.

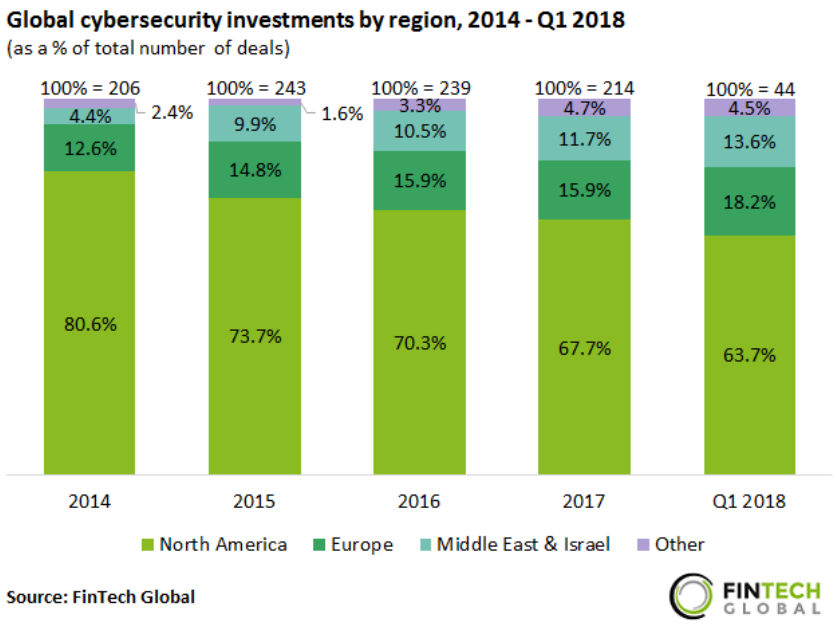
India's ranking-

India is well known as an Information and technological hub proving it very well in the GCI 2017 by landing at rank 23 but in the latest GCI 2018 , released two months ago, it slipped to 47th rank. With this it calls for worry, as we are moving towards a digital cashless and inclusive economy with more caliber.

ASSOCHAM's (Associated Chambers of Commerce and Industry of India) study shows that there is a 350% increase in cyber attacks in the last five years further the 3.2 million debit card data theft in 2016 has hit India hard and can be seen in the GCI ranking.

Cybersecurity Investment around the world-

The U.S. government spends $19 billion per year on cyber-security but warns that cyber-attacks continue to evolve at a rapid pace.

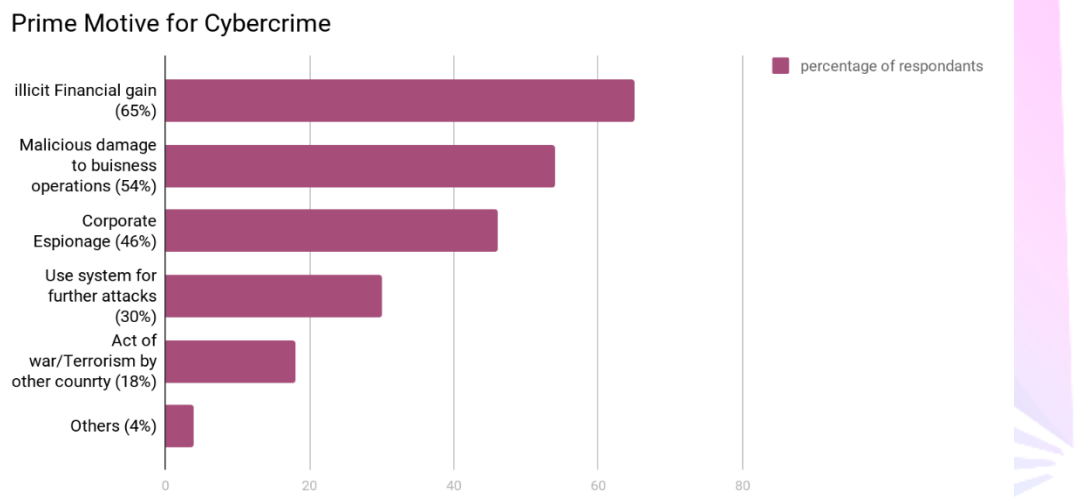


According to Gartner, the rising tide of cyber crime has pushed information security spending to more than $86.4 billion in 2017.

But in India, two out of three companies spend less than 5% of their IT budget for beefing up their cyber security.

CYBERCRIME DIMMING THE LIGHT OF INDIA

A survey by India Today, highlights that Indian consumers lose $18.5 bn in a year due to cybercrime. Also we have seen a 77% increase of cybercrime in the last few years. If we consider the Indian population in this regard, the primary motive includes , financial gains ,malicious damage to other's business due to rivalry or competition, spying on others etc.

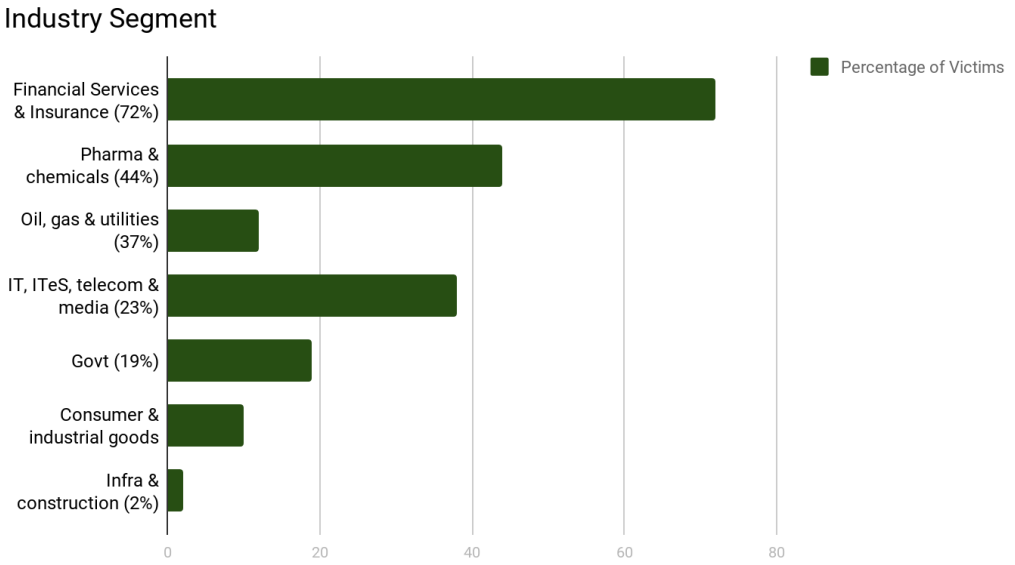


Source : Survey published in Business Today

Business Espionage is one of the major players in the increase of cybercrime. While employers would like to believe that their workers can be trusted, the real situation is that some staff members are ready to sell company data for personal profit. Though data shows that in four out of five cases of cybercrime, there's an external perpetrator, experts feel insiders play a big role in selling secrets.

Cybercrime and Indian Economy

Survey from business today shows the segment of industry affected by cybercrime in the indian



economy.

Source : Survey published in Business Today

With this we could state that the economy also gets affected hugely accounting for huge monetary loss accounting upto 20 billion dollars per year.

CYBER LAWS

After the Internet was made public in the early 1990s , it was soon realised that there is a need to protect the internet based system after the major attack on US based bank, citi bank, leading to loss of billions and billions of dollars to a hacker who never moved from his chair. With this, every state started making certain norms to ensure cybersecurity in this domain. There are laws in India which were designed to tackle the problem of cybercrime which started in 2000 in lieu of such cyberattacks.

Cyber Laws in India:

Mid 90's saw a global impetus towards digitization and computerization and India saw the move towards Liberalization, Privatization and Globalization. With the opening up of indian

market and linking of indian economy with the global economy, the scope of Information and communication Technology (ICT) also grew and with that grew the crime related to ICT.

With the global trade shifting towards electronic form a need was felt to give legal recognition to the electronic records. Responding to this global need the United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations passed a resolution in January 1997 recommending all States in the UN considerations to the said Model Law, which provides for recognition to electronic records and according to it the same treatment like a paper communication and record.

Information Technology Act 2000

It was against this background that the government of India passed **the Information Technology Act 2000** which was made effective from 17 October 2000 and hence India became the 12th Country to have a cyber law.

The Information Technology Act, 2000 gives legal recognition to the transaction done by electronic means. This act also amended Indian Penal Code 1860, the Indian Evidence Act 1872, the Bankers' Books Evidence Act 1891, and the Reserve Bank of India Act 1934 to certain extent.

The main intent to pass the 2000's Act was to provide legal recognitions to transactions carried out by means of electronic data interchange and other means of electronic communications, commonly known as electronic commerce, which involved the use of alternatives to paper based methods of communication and storage of information and to facilitate the filing of documents of government agencies.

The main objective of this Act are :

1. To give legal recognition to the transactions done by electronic means of communication generally used for e commerce.
2. It gave legal recognition to digital signatures.
3. It facilitated the electronic filing of documents with Government agencies and departments.

4. It facilitates the electronic storage of data.

Applicability of the Act : The Act is applicable to all of India.

Legal Applicability **:**

As per Section 1(4) of the Information Technology Act, 2000, the Act is not applicable to the following documents:

1. Execution of Negotiable Instrument under Negotiable Instruments Act, 1881, except cheques.
2. Execution of a Power of Attorney under the Powers of Attorney Act, 1882.
3. Creation of Trust under the Indian Trust Act, 1882.
4. Execution of a Will under the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
5. Entering into a contract for the sale of conveyance of immovable property or any interest in such property.
6. Any such class of documents or transactions as may be notified by the Central Government in the Gazette.

This Act was amended in 2008.

Need for amendment :

Cyber crime was addressed by this Act but there was still need to address the specific cyber crimes that were taking place along with the technological advancement.

With the booming of Software Companies and e commerce there grew a greater dependence on ICT therefore there was need for a strict law to protect the customers and corporates from cyber crimes.

Information Technology Amendment Act' 2008

Thus with the growing cyber crime there was a greater need for a more holistic need to deal with the changing nature of cyber crimes and therefore Information Technology Amendment Act 2008 was passed on 23rd December 2008.

The Salient Features of Information Technology Amendment Act' 2008 :

The Act has been made technology neutral a new section has been added to define Cyber Cafe i.e. any facility from where access to the internet is accessed by any person in ordinary course of business to the members of the public further Intermediaries have been defined in this act. It also added a new section 10A which provided legal validity to contracts concluded electronically even a new section to protect sensitive data or information possessed , dealt or handled by a body in computer resource which such a body owns, controls or operates.If such a body is negligent in implementing and maintaining reasonable security practices and procedures and thereby causing wrongful information loss or gain then such a body is liable to pay compensation to the affected person.In section 66 new section 66A to 66F have been added prescribing punishment for offences like cheating,cyber terrorism etc. Section 67 of the IT Act has been amended to reduce the term of imprisonment for publishing or transmitting obscene materials in electronic to three from five years and the fine has been increased to rupees five lakh from one lakh. Section 69 has been amended giving power to the state to issue direction for intercept and monitoring of decryption of any information through any electronic medium. Section 79 of the act which exempted intermediaries has been modified. A provision has been added in sec 81 of the Act which states that the provision of the Act shall have an overriding effect. The Act authorizes an Inspector to investigate cyber offences (as against the DSP earlier).

Further with the ever changing dynamic of the cyber ecosystem there is a need for certain amendments in the Information Technology Amendment Act 2008 and with this in mind the Government of India has asked for citizen participation for suggestion for the upcoming amendment to the IT Act.

National Cybersecurity Policy, 2013

Since the 2013 NSA spying issue the need for cyber security was felt in India as a response to which the National Cybersecurity Policy was formulated in 2013.Information can be classified into two group one which can be freely flowed and the other that needs to be guarded.The cyber security policy 2013 is formulated keeping in mind both these aspects of the information.

National Cyber Security Policy Vision, 2013

The Vision of this policy is to build a secure and resilient cyberspace for citizens, businesses and Government.

Some other Initiatives by the Government:

National Cyber Security Coordination Centre (NCCC),2017:

Operationalised in 2017 it is mandated to perform real-time threat assessment and create situational awareness of potential cyber threats to the country.

National Critical Information Infrastructure Protection Centre (NCIIPC):

The organisation was created under section 70A of the IT Act. It is designated as a national nodal agency in respect of critical information infrastructure protection and it aims to protect and safeguard critical information infrastructure (CII) against cyberterrorism, cyberwarfare and other threats. The critical Infrastructure includes power and energy, Banking financial service and insurance, telecom, transport, government, strategic and public enterprises.

Cyber Forensic Laboratory*:* In case of cyber crime the Cyber Forensic Laboratory and Digital Imaging Centre assists law enforcement agencies in the collection and forensic analysis of electronic evidence.

Cyber Swachhta Kendra (2017)

It was launched in early 2017,it provides a platform where they can analyse and clean their systems of various viruses, torjants, malwares etc.

Cyber Surakshit Bharat (2018)

Cyber Surakshit Bharat initiative was launched by the Ministry of Electronics and Information Technology (MeitY),in association with National e-Governance Division (NeGD) in 2018.

It was launched with the objective of creating awareness about cybercrime and building capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.

The Cyber Warrior Police Force (2018)

The government has come up with the initiative in 2018 to create a cyber warrior police force. It is proposed to be formed on the lines of the Central Armed Police Force.

Indian Cyber Crime Coordination Centre(I4C), 2020

The centre was inaugurated in 2020 by the Union Home Minister along with the National Cyber Crime Reporting Portal.

I4C has seven major components National Cybercrime Threat Analytics Unit (TAU),National Cybercrime Reporting,Platform For Joint Cybercrime Investigation Team,National Cybercrime Forensic Laboratory (NCFL) Ecosystem,National Cybercrime Training Centre (NCTC),Cybercrime Ecosystem Management Unit,National Cyber Research And Innovation Centre.National Cyber Crime Reporting Portal is a citizen-centric initiative that will enable citizens to report cyber crimes online.

National Cyber Security Policy Mission 2020

The Mission of this policy is to protect information and information infrastructure in cyberspace and build capabilities to prevent and respond to cyber threats,to reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

With the change in ICT ecosystem there was felt a need for amending the existing Cyber Security Polity and therefore the government is in process of coming up with a new cyber security policy in 2020.

Cyber Security issue in Jharkhand

Cyber crimes are mostly bailable offences. Also scamsters often go scot-free for lack of evidence. There is also a shortage of investigating officers as only inspectors and above are allowed to investigate cyber crimes.

Jamtara in Jharkhand has been identified as a new cyber crime capital of India. More than fifty percent of cyber crimes in India are traced back to this town of Jharkhand. The revelation was

made by Union Home Secretary Rajiv Gauba who himself is a 1982 batch IAS officer from Jharkhand.

It takes us to the next question as to why Jamtara, the answer can be lack of education as average literacy rate in Jamtara is around 64% and lack of employment opportunities due to which youth are forced into the cyber crime domain which gives them short term benefits. As Ramesh Kumar Dubey, deputy commissioner, Jamtara says

"It is not uncommon to find people here operating laptops on the roadside. They could be just making fraudulent money transfers. We have arrested hundreds of people, mostly between 20 and 30 years of age, who have taken this up as a profession. As per our estimates, close to 150 gangs are involved in developing cyber fraud as an industry,"

SUGGESTION

Considering the benefits and risks associated the use Information and Communication Technology we authors have tried to throw light on critical assessment and possible recommendations in lieu of need for improvisation in this so called 5th domain ,"Cybersecurity".

Cyber Warfare : India needs to define its stance

Cyber warfare is the use of information and communication technology to attack a nation causing damage comparable to actual warfare.It has emerged as the fifth domain of warfare.In case of a cyber attack the identity of attacker can easily get concealed by use of layering. The problem with cyber attack is that the aggressor can not be traced back easily and therefore it becomes difficult to pinpoint the involvement of any country behind it or even if the origin or attack is traced back the country can easily blame it on non state actors.

The other difficulty comes of how to respond to a cyber attack when a country lacks credible offensive cyber capability that it could use as a deterrent, the question is should it turn to conventional weapons in such a scenario but the problem with use of conventional weapons is that it can become too escalatory and comes with the danger of an escalation to all out war. The policy of showing restrain in such a case can not go very long as restrain when practiced

for too long can encourage the enemy to continue with more attacks and therefore India needs a Cyber Warfare Policy which can take inspiration from India's Nuclear Policy which can act as a deterrent to aggressive counties such as China.

Moving in lines similar to the defence policy India can form a Multilateral Coalition for Cybersecurity consisting of like minded countries, an inspiration can be taken from NATOs approach on cyber defence where NATO supports its members by sharing real-time intelligence on threats and best practices for handling such threats.

More robust Cyber security Infrastructure

The Indian Computer Emergency Response Team (CERT-In) formed in 2004 coming under the Ministry of Information and Technology, Government of India, has been designated as the National Nodal Agency for incident response but CERT itself lacks experts and infrastructure to effective combat the growing cyber crimes in India thus there is need for technological upgradation and capacity building in CERT.

Digital India - The vision of the government is to create ICT infrastructure connecting gram panchayats, providing government services on demand , digital literacy etc. Under it one of the components is about promoting electronics manufacturing in the country with the target of NET ZERO Imports by 2020 which can be seen in the context of government fear of chinese smartphones involved in data stealing.

More involvement of Public- Private partnership

India is one of the few countries to have a cyber security law it even ranks 47 in GCI 2018 index which shows that India is doing remarkable in this front but as the NCRB 2017 data shows that cyber crimes in India jumped by 77% in 2017, many new crime heads such as cyber blackmailing, cyber stalking and dissemination of fake news were introduced. Cybercriminal are ahead of Police in technological advancement. The Investigating officer is generally found lacking in many cases but projects like Cyberdome project in Kerala are showing the way by involving Public private partnership in investigating cyber cases.

Need for Laws to makes banks more responsible

Most of the cyber crimes cases involves frauds related to debit/credit cards ,the card are details are extracted and money siphoned off money through account by extracting opt code and other account related information in all these cases the banks are a major party as the debit/credit cards are ultimately banks property the and account is held in the bank but presently there is no law which makes banks liable in case of cyber crimes thus there is no liability on the banks to make their facility more adapted to tackle emerging cyber crime threats.

Awareness about Cyber Hygiene : Need of the hour

As people are buying mobile phones and other gadgets the vulnerability associated with the cyberworld is increasing since it is an open ecosystem and less resource incentive. Anyone with a good computer, internet connection and computer knowledge can get involved in this domain. India is the 2nd largest consumer of mobile phones in the world, thus , it is high time now to understand the alertness required to build a safety wall between personal data and cyberattack prone realm. Experts feel most victims get conned because of the sheer carelessness about securing their devices. Moreover most of the websites even government websites fail to maintain cyber hygiene which results in leak of user data awareness needs to be created about the need for cyber hygiene.

Cyber hygiene can be easily maintained by the use of legitimate operating systems for your devices and keeping them updated,keep your browsers updated and use the latest version by installing a good anti-virus and anti-malware protection on your devices that you use for your banking transactions when using public Wi-Fi networks, be on your guard by turning on a Virtual Private Network. This will shield your browsing activity and connect securely.

Recruitment of "Ethical Hackers" : Solving youth Unemployment to an extent

With technological evolution to prevent crime , the need is to be ahead of criminals. We can do the same by involving experts who are willing to counter the hackers, they can be from NGO or from private companies or even volunteers.

Looking at the domain of cyber crimes taking place in India it is generally observed that most of the cyber criminals are between 20-30 yrs of age and are unemployed youth who due to lack

of employment opportunity and need for money are attracted into this domain in search of easy money therefore there is urgent need to create awareness about cyber crime in affected areas such as Jamtara and employment opportunities needs to be created to utilise their talent in a constructive way.

As we are moving towards a more digital and inclusive economy , Jan dhan account, National optical fibre etc , it is very important to consider this aspect seriously.

REFERENCE

1. https://www.business-standard.com/article/current-affairs/jharkhand-emerges-hotbed-of-low-tech-cyber-crimes-116110500930_1.html
2. https://www.legalbites.in/salient-feature-of-it-act-/
3. Source: Book on "IT" Security of IIBF Published by M/s TaxMann Publishers
4. https://www.itu.int/en/about/Pages/default.aspx
5. https://www.businesstoday.in/photos/bt-newsflicks/cybercrime-personal-data-protection-loss-consumers/1454.html#photo6