Hacking- An In-Depth Analysis

Tanushree G L[1]

ABSTRACT

This paper deals primarily with hacking for which there is need to understand the concepts of cyber space and cybercrimes which will give an understanding as to why hacking fits into these concepts. Cybercrimes, being a wider term can never be given a precise definition but hacking can be defined as the essentials of the crime remain the same at any point of time. Looking into history of hacking gives a clarity regarding where and how it started and it was not really a crime when it started. A wide discussion as to how hacking satisfies the essentials of a crime is made in this paper and also briefly explains ethical hacking. This paper deals in detail with jurisdiction issues which not only hacking but all the cybercrimes face. A key question as to why hacking need special attention at this point of time. The paper also discusses few real life incidents wherein the impact created by the hacking can be clearly understood. The paper also discusses the technical and societal issues faced with respect to the offence of hacking. The paper gives statistical data as to the rise of hacking incidents every year in India and proves the point that there is a much needed urge to look into laws regulating hacking in India and suggesting few initiatives to be taken to eradicate this evil. Hacking strikes at the basic foundation of national security as well as the fundamental right of privacy which every citizen has right to enjoy. So the paper discusses on the fundamental rights and how hacking affects those rights.

Keywords: *Cyber Space, Cybercrime, Hacking, Hackers, Cyber Security*

I. AN INTRODUCTION TO CYBER SPACE AND CYBER CRIME:

As Aristotle mentioned "Man is a social animal" and he cannot live in a confined space. The technology has grown to the extent of socialising through the platform provided by internet in the form of social networking websites. In this fast moving world, technology compliments to the growth of humans but that's just one side of a coin. With the growth also comes the repercussions where technology is one of the great contributors to crime rate in any country. There is a need to understand the concept of cyber space in order to capture the essence of the cyber-crimes.

"Cyber Space: A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts … A graphic representation of data abstracted from the banks

[1] *Author is a student of Sastra Deemed To Be University, India*

of every computer in the human system."[2]

The above words first brought the concept of cyber space into English by William Gibson, a science-fiction author. Cyber space, to define it in simple terms, is a domain that exists along with but apart from physical world. It is nothing but a virtual world or a shared conceptual reality.

The cyber-crime is often confused with computer crimes in common parlance. Donn.B.Parker[3] distinguished both by stating that computer crime is a crime in which the perpetrator uses special knowledge about computer technology and in case of cyber-crime, the perpetrator uses the special knowledge of cyberspace. But the distinction did not provide an exhaustive definition for cyber- crimes. Cyber-crimes can be plainly defined as, "crimes directed at a computer or computer system"[4]but it has to be understood that essence of cyber-crime cannot be pigeonholed into a definition as it has many dimensions to it. The Cyber-crime has to be differentiated from traditional crimes. Modus operandi of committing cyber-crimes mainly involves illegal interference in computer, computer system and network operation[5].

II. HACKING- DEFINITION

Basically cybercrimes are categorised into two, one being vandalizing digital information and the other being security related crimes. Vandalizing of digital information takes place in two modes, one being by internal means and the other by external means. So hacking is process of internal means by which digital information is vandalized. So the modus operandi when it comes to hacking is purely technical and invisible.

The word hack at Massachusetts Institute of Technology (MIT) usually refers to clever, benign and ethical prank or practical joke, which is challenging for the perpetrators and amusing to the MIT community. And Hacking was described as a interaction with computer in a playful way and an attempt to explore rather than a goal directed way[6].

According to Wiktionary, Hacking means unauthorized attempts to bypass the security mechanisms of an information systems or network. Under the "means" approach, the "mere" access to a computer system without authorization criminalizes and names it as hacking and the it is of no consequence whether an additional illegal act results from such access. Hence the Information Technology Act, 2000 does not define hacking explicitly.

Hacking is easily and largely possible even by people who are not aware of the programming techniques because of free tools disguised as network tools available on the Internet tools like Ping of Death, Hacker

[2] William Gibson, Cotton and Oliver (1994) 54

[3] Steven Furnell, Cybercrime: Vandalising the Information Society (Addison-Wesley, 2002)21.

[4] Peter Stephenson, Investigating Computer-Related Crime (CRC Press, Washington DC 2000)3.

[5] Vladimir Golubdev, Computer Crime Typology, Computer Crime Research Centre.

[6] Jargon Dictionary, http://minfo.Ast5rian.net/jargon/terms/htmlhack.

Evolution, Netstat Live, Advanced Port Scanner, Ophcrack etc.

Hacker- More Than An Anonymous Criminal

The Collins English Dictionary, (3rd Edition, 1994) defines hacker as a Computer fanatic especially one who through a personal computer breaks into the computer system of a company, government, etc.

Cambridge International Dictionary of English, 1995 defines hackers as a person who hacks into other people's computer system.

New Oxford Dictionary of English, 1998 defines hacker as a person who uses computer to gain unauthorized access to data.

A skilled and enthusiastic computer operator , especially an amateur, an operator who uses his or skill to break into commercial or government computer or other electronic system as defined by Chambers Dictionary,1998.

Analyzing all these definitions we can understand that there is only one common element existing which is nothing but "unauthorized access". Though hackers regard themselves as skillful people who bring to light the vulnerability of the system, almost cyber legislations in all countries regard them as criminals and also it is most important to understand that the technique used by hackers are the techniques used to commit most of the cybercrimes. So hacking is considered to be the mother of cyber-crimes.

III. HISTORY OF HACKING

In 1960, the art of hacking originated for the purpose of modifying the working structure of the train set in MIT by a group of enthusiasts. So hackers were programmers interested in modifying or customizing programme or for learning the working structure of the programme. Then in 1970 s came a new group of people who were phone hackers also known as phreakers. This slowly led the computer enthusiasts to venture into cyberspace to commit crimes.

Steven Furnell in his work has clearly discussed the history of hacking and the origin of the term hacking. His work was not about computer criminals but about the pioneers of 1950s and 1960s computing. At that point of time hacking was not a criminal activity and was just a prank and the hackers were appreciated for their skills.1960s witnessed hackers who were software and hardware geniuses and the term largely referred to persons capable of implementing elegant, technically advanced solutions to technologically complex problems. So Furnell , at that point of time reflected his thought on hackers who were skillful persons exhibiting art of hacking but this present era witnesses hackers who are just using the art to commit crimes. But using hacking

skill for such criminal activities would be frowned upon by the hackers of 1960s because they saw hacking as a tool for liberation.[7]

There is also a need to understand how the term hacking and cracking has been used wrongly in common parlance .Basically hacking was an art form of gaining access into the secured systems as an exhibit to showcase their talent or as a medium of learning the programme . But the Cracking was the one in which computer enthusiasts gain unauthorized access into a system in order to sabotage the data or to commit acts such as vandalizing. But it is used interchangeably.

IV. WHY HACKING REQUIRES A SPECIAL ATTENTION?

A simple question may arise in every one's mind as to why among all cybercrimes hacking is the most destructive cybercrime. There are many reasons to that and the first one would be difficulty in tracing the hacker. Every computer has an IP address just how a person has his own name. So every computer is identified by its IP address. The main essence of hacking a computer and not leaving any evidence can be done when the IP address of the computer used by the hacker is hidden. The hackers use various technologies like intermediate computers and anonymous proxy servers while hacking another device.

Basically using intermediate computer means using one compromised computer and getting connected to another computer and using that another computer to hack the victim computer. Proxy servers manipulate the IP address and location of the hacker. And looking into another important aspect is that log files which also helps the hacker to hide behind his veil. Some computers do not maintain any logs or the hackers usually have their log files deleted frequently so the investigating authorities really don't find any evidence with the log files. And these are technical issues faced when it comes to hacking. So what are the societal issues faced with respect to hacking are dealt with below.

The most important societal issues with respect to hacking is that the victims don't report the hacking incidents. Because the hacking incidents make the people to believe that the servers of that particular company being branded as a weak one and that results in loss of sales. Many companies are of the view that the loss caused by the hackers do not cause a damage equivalent to the loss of sales. And the companies find it very difficult to fight off the negative publicity caused by the hacking incident.

There are many incidents which took place recently in India i.e. in the year 2018 which made the headlines proving how far a hacker can go. Some incident are dealt with to understand the impact of hacking.

Amit Tiwari, a hacker who has hacked nearly 950 accounts since 2003 was arrested in 2014.It took nearly 11 years to bring the accused before the eyes of law and it was found that he used to hack foreign mails and he was

[7] Steven Furnell, Cybercrime: Vandalising the Information Society (Addison-Wesley, 2002)

arrested based on the FBI tip. This shows that it is not that easy to bring a hacker before the eyes of law.

In the month of April 2018, the website of Supreme Court crashed and the screenshots of that were circulated in which the picture indicated that the Supreme Court website was hacked by a Brazilian Team. There were also suspicions about the Indian Defense Ministry websites and Indian Home and Law ministry websites being hacked by Chinese team of hackers.

Gujarat National Law University website was hacked by Pakistani hackers and there was a message in the website stating"Stop firing in Pakistan & stop blaming on us. Everybody know, what happened with your coward army in Kargil War:D. Stop your bullshit movement against Kashmir & Pakistan. Its better foryou to keep away from Kashmir & Pakistan. Our spy pigeons still flying in India: Buahahah: D…"[8]

These kind of hacking incidents raise a question of national security where the term cyber terrorism comes in and it has to be understood that though hacking and cyber terrorism are not one and the same but hacking can be used as a weapon to promote terrorism.

V.STATISTICS ON HACKING CASES IN INDIA:

The statistics always prove the efficiency of the laws in a country. Even if not for the decrease in cyber-crime rate, it would have been appreciable legislation if it is keeping the numbers under control.

India is ranked third after US and China as country with highest amount of cybercrimes happening. Cyber-crime rate in India rose nine times from 2005 to 2014 which was 569 in 2005 to 5752 in 2014. Nearly 22000 websites Indian websites were hacked right from April 2017 and January 2018. Among those 114 websites were government websites.

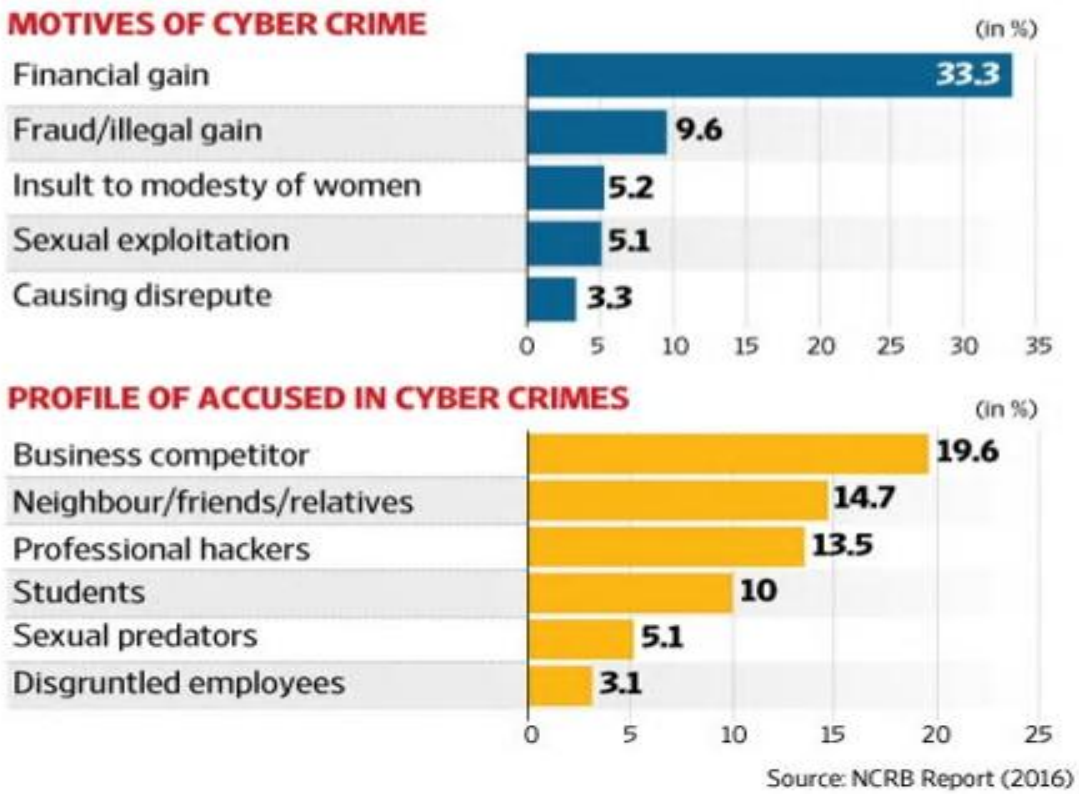
YEAR	NO.OF GOVERNMENT WEBSITES HACKED PER MONTH
2014	13
2015	14
2016	16
2017	19

Source: National Crime Records Bureau

[8] Spy pigeons, cockroach spy and Modi memes: Pakistani hackers hack GNLU website' (*Livelawin*, 2 August 2015) <https://www.livelaw.in/spy-pigeons-cockroach-spy-and-modi-memes-pakistani-hackers-hack-gnlu-website/> accessed 3 February 2019

YEAR	NO.OF HACKING CASES IN INDIA
2011	21,699
2012	27,605
2013	28,481

Source: International Journal on Recent and Innovation Trends in Computing and Communication Volume: 5 Issue: 6



The statistics above published in Live Mint on April 6, 2017 based on the NCRB report clearly suggest that the motive for cybercrime is financial gain and the accused is most likely to be a business competitor. So it can be inferred that a company or any person in order to get rid of their competitor used cybercrimes as a way. The reporting rate of the hacking is also very less when it comes to companies because it makes the competitors reach out to the confidential information that is being hacked. Sometimes professional hackers are also hired to break into the websites of the competitors

The United States of America hackers has nearly 17 per cent of intrusions done in Indian websites. Russia nearly has 15 per cent of intrusions in Indian websites and Pakistan has 9 per cent of intrusions, Canada has 7

per cent and Germany has 5 per cent of website intrusion into Indian websites. Netherlands has 4 per cent of website intrusion done in India while North Korea and France has 2 per cent each contributing to the intervention of Indian websites. Other countries have 4 per cent website intrusions done in Indian websites.

VI. HACKING – PERFECTLY TAILORED CRIME:

Hacking is different from traditional crimes in lot of dimensions like when it comes to understanding the scene of occurrence and there is latency in reporting. Accused in the case of hacking is a person who is well trained computer nerd. And Police are untrained in these kind of crimes and the investigation requires people knowledgeable in that field. How hacking has both the mens rea and the actus reas element which is essential for any crime is explained below:

Mens Rea element:

The element of mens rea is found in Section 1 of UK Act and in Section 66 of the Information Technology Act. The mens rea of the offence under Section 1 consists of the following two elements:

- ***a.*** There must be intent to secure access to any program or data held in any computer.
- ***b.*** The person must know at that time that he commits actus reus because the access he intends to secure is unauthorized[9].

According to Section 1(2) of the Act, the intent need not have to be directed at any particular program, data or computer.

From the above two essentials it is very essential to stress on the word unauthorized. And it is very important to understand that mens rea element can be seen from the state of mind of hacker and his knowledge about the access being unauthorized. It is easier to prove hacking when the access is done by an outsider but when it is done by a person who has been given access to the computer system and has exceeded the limits , it is tough to find out if that amounts to really hacking .

Actus Reus element:

The term Actus Reus clearly means acting according to mens rea. When it comes to hacking it is a very big issue in deciding the actus reus because the act takes place in a surrounding which is not in existence. Only when the hackers end up making a mistake during the process, there can be a chance to pick evidence. And the actus reus needs evidence to be proved and that too especially available in the form of admissible evidence. Every time a computer is made to work by a human is considered an actus reus, any of the following shall be

[9] Ankit Majumdar,"A Practical Perspective on Hyper Linking, Framing and Meta-Tagging" in Nandan Kamath(Ed.),Law Relating to Computers,Internet and E-Commerce (Universal Law Publishing Co. 2002) 272.

considered as actus reus:

a. Trying to do some act using the computer.

b. Either attempting to access data stored on a computer or from outside through the said computer.[10]

c. Every time the computer is used by its user while gaining access, signals pass through various computers which are made to perform some function when the command given by the user pass through it. Each such function falls under the "actus reus".[11]

VII. JURISDICTION ISSUES IN HACKING

Jurisdiction issues faced in case of hacking is similar to all other cyber-crimes. Jurisdiction is basically the authority or power given to courts to decide on a particular issue and give judgements on the issue. Cyber space has no particular geographical location so when it comes to cyber-crimes how does court decide the jurisdiction is the key issue. There is no uniform law or a standard rule to decide on jurisdiction of courts on cyber-crime cases. The traditional law and settled principles of law used as a tool for other cases in deciding the jurisdiction cannot be applied to decide the jurisdiction when it comes to cyber space.

In normal case, there are just two parties the aggrieved one and the defendant while when it comes to cyber-crimes there are three parties. The victim shall belong to one country and the perpetrator may belong to another country with the server host located in third country. Sometimes the issue arises that the perpetrator may not be aware of the fact that a particular activity is crime in the other country. So the key question regarding the jurisdiction and choice of law arises.

There was a school of thought in which jurists totally reject the application of real world laws when it comes to cyber space as they view the cyber space to be just an extension of imagination. But that school of thought failed due to the rise of cyber-crimes. And when looking closely into the concept of cyber space it clearly strikes at the basic tenets of jurisdiction in the real world law.

The Indian Courts rely on the principle of "Lex Fori" which means the law of the forum while deciding the jurisdiction and no reliance is placed on foreign procedural laws. Personal Jurisdiction is taken care by the Civil Procedure Code. Sec.20 of CPC elaborates regarding the jurisdiction by placing reliance mostly on place where cause of action has taken place or place of residence or work of defendant. Cr.P.C lays emphasis on the cause of action and the enquiry and the trial shall take place in that jurisdiction where cause of action arose.

"Minimum Contact" rule and Long Arm Statue are the two prominently used rules when it comes to deciding

[10] C. Gingras , The Laws of the Internet(Butterworth's London 1997) 216

[11] Pretty Lather, Cyber Crimes in India and the Legal Regime to Combat it. Dissertation (unpublished) submitted to the Faculty of Law, University of Delhi, 2006, 15.

the jurisdiction in Indian Courts. Minimum Contact Rule was propounded in 1945 in International Shoe Co. vs. Washington[12] to extend jurisdiction over a defendant who comes from another jurisdiction. The court held that a corporation which enjoys the privileges of conducting activities in a particular state also gets protection. So in this case the minimum contact of the defendant with the particular jurisdiction is to be established.

Long Arm Statute surpassed the minimum contact rule and had a discussion on the term "purposeful benefit" and the following should be ensured to be in conformity in order to have jurisdiction:

1. Purposefully and successfully solicitation of business from forum state residents
2. Establishment of contract with the forum state residents
3. Associated with other forum state related activity
4. Substantial enough connection with the forum state.[13]

"Agreement clause" plays a very essential role as the jurisdiction is decided based of the agreement existing between the parties. Unless a party resists to the clause of forum selection in case of online contracts, the clauses are prima facie valid[14]. Click trap contracts which asks the user to accept to the terms and conditions make the user subject to particular jurisdiction. In rare cases, the jurisdiction is fixed based on the location of the host server location.

The Information Technology Act, 2000 deals with the jurisdictional in Sec.1 and Sec.75.This particular Act provides power to have any nationality booked for a crime. But the evidence is required to be collected from other jurisdiction which is a cumbersome process which takes place in accordance with Sec.166A, Sec.166B and Sec 188 of Cr.P.C. There are high chances of the evidence getting destroyed when the investigation has to go through a lengthy prescribed process.

The Cybercrime Convention provides for mutual cooperation of signatories to decide the jurisdiction when there is a conflict of law and also makes cybercrime an extraditable offence if the act is illegal in both the signatory countries. Article 22(d) of the convention emphasis on the nationality principle that it leaves the jurisdiction to the discretion of the signatory countries. But India is not a signatory to that convention. So the alternative option which India could have availed is to make reciprocal arrangements with different countries which India has not done yet.

[12] 326 US 310:66 S Ct 154:90 L Ed (1945).

[13] International Shoe Co. v. State of Washington, Office of unemployment Compensation and Placement et al, 326 U.S. 310, 316 (1945); See also Hess v. Pawloski , 274 US 352 (1927).

[14] Bremen vs Zapata Off-Shore Co., 407 U.S. 1 (1972).

VIII. ANTI-HACKING LAWS IN INDIA:

Sec. 43A and Sec.66 deals of Information Technology Act deals with hacking in India. When there is no mens rea element present then the hacker will merely be subjected to the civil liability. And Sec.378 of Indian Penal Code (IPC) can also be used to initiate criminal proceeding against the offender. Under Sec.66 of Information Technology Act maximum punishment awarded was upto 3 years whereas other countries like USA awards 10 years maximum imprisonment and China awards maximum 7 years of imprisonment in case of hacking. While India being the third country to have large number of hacking cases, there is a need to have a higher maximum sentence.

In India , none of the legislations defines the word "data". Data and privacy are related to each other. Data in common parlance can be said as information linked to a person's life. But data is also very important to be preserved in a proper form to ensure privacy. To take this concept to a another level, data in one device varies from data contained in other device. In Laptops most people don't store use their phonebook option but in mobile phone it is the most used one. And people use camera option more in their smartphones to take pictures rather than their laptops. So to look into another perspective the data that can be stored in a laptop is comparatively larger than smartphones. The kinds of data stored and the way in which it is stored require different set of laws in order to protect the data. Nowadays mobile phones are susceptible to hacking because the technology has grown to the extent of even providing mobile banking facilities. Hackers find it easier to hack mobile phones as it is very easy to reach a person via mobile phone.

In UK, though computer hacking is taken care by Computer Misuse Act,1990 but the mobile phone hacking is taken care by Regulation of Investigative Powers Act, 2000 with respect to interception of phone calls. So it is essential to understand there is a need for a definition which would be broader to include all the advancements in the future too in India laws . The Information Technology Act, 2000 does not specify the minimum standards of protection to be ensured in protecting the data and hence there is a need for such law where minimum standards are required.

One of the recent methods used by the hackers is by way of links, games , giving away freebies, work from home opportunity etc. There was a wide outburst due to the blue whale challenge. Blue whale challenge which starts as a game where certain tasks are given which makes the player to inflict torture upon themselves and later it was found that players of the game were made to inflict torture upon themselves because they were threatened to publish the data hacked from their mobile phones like personal messages, photos, videos etc.The result of the game was to mentally tormenting the player to commit suicide and many people actually did commit suicide afraid to report the threat. The Hon'ble Madras High Court took this matter into consideration

suo moto[15] and provided direction to both Central and State Government which clearly stated to remove all the links related to blue whale challenge. Many other directions like providing counselling students and also confiscation of mobile phones of victims were provided. The main point of argument was based on right to be forgotten because though at that point of time the game was banned it was still in circulation so it required the action of the social networking sites and others to remove such links. The Personal Data Protection Bill,2018 which in its draft form has provided for the right to be forgotten as a significant provision but right to erasure is not a part of the bill. Mechanism which shall hold the data only for a certain period of time and erasure of it post that period shall help in preventing the hackers from taking control over the complete data right from the scratch.

Ethical hacking- two sides to the same coin:

It is also very important to understand that not all hacking are illegal. Hacking which is not illegal is called as Ethical Hacking. Companies to protect their servers and to find the weakness or vulnerability hire people to protect their systems. The difference is that the computers are hacked in ethical hacking but with the permission of the owners and so it is not unauthorized and no destroying that data or stealing the information is done.

Ethical hacking has no precise definition and it is better to leave it undefined as only facts and circumstances can decide if that particular hacking incident was ethical or not. There is no strict protection given to white hackers under Information Technology Act,2000.

Fundamental right to privacy affected:

Privacy is nothing but the right to be let alone. In India after the Puttaswamy judgement vs. Union of India[16], right to privacy is a fundamental right. And the same judgement when discussing about the kinds of privacy recognizes informational privacy as one of the important aspect of privacy. This right exists not only in the real land but also in the cyberspace. Section 72 of the Information Act, 2000 envisages the breach of privacy as an offence. Hacking strikes at the basic foundation of privacy. In cyber space, right to privacy may be affected by following ways[17],

1. Utilizing private data for a purpose other than that for which it was collected.
2. Unauthorized reading of e-mails of employee, etc.
3. Sending of solicited e-mails or spamming.

[15] The Registrar,Madurai Bench of Madras High Court vs. The Secretary to Government, New Delhi ,SUO MOTU WP(MD) No.16668 of 2017

[16] (2017)10 SCC 1

[17] Yatindra Singh J, "Cyber Laws" (2002) AIR 137.

Privacy in cyberspace is to protect their personal information and not only that but to maintain a secret life and having their own space to do whatever they want provided legally. To look closely we can understand that the other countries have their own data protection laws while India is lacking one. One of the most important aspects of the data privacy is data protection. Hacking from its definition has a nature to be an unauthorized intrusion into the computer system of other person, so it clearly violates the right to privacy of the person whose computer is hacked. Hacking is done to steal data or confidential information of the competitors in order to gain a competitive advantage.

Article 8 of European Convention for Protection of Human Rights and Fundamental Freedom 1950 states that everyone has the right to privacy to protect their personal data. Similarly various treaties and conventions speak of right to privacy with respect to data protection. In Puttaswamy vs Union of India ,clear directions have been given to establish a committee and study the issues relating to data protection and to come up with effective laws but it is tough to come up with such laws because that requires balancing of other rights along with right to privacy. But at present India is in need of data protection laws being one of the fastest growing countries in information technology sector.

IX. SUGGESTIONS

1. There is a need to develop awareness regarding cyber security in India which can be done by training the people who work in that area mostly as to how to protect their computers from hacking. Ministry of Home Affairs has took up nearly 27500 police personnel to be trained when it comes to cybercrime against women and children. But the cybercrime investigation needs a wide attention and should include training the police officials also to understand the cybercrimes and giving some basic knowledge which would help them for their investigation.

2. India not being a signatory to Cybercrime Convention should make reciprocal arrangements with other countries in order to not clash over jurisdiction. This is high time that India should take the initiative to understand the need to recognize the deadly evil called hacking. India is still in talks with 15 countries to enter into bilateral agreements when it comes to seeking cybercrime evidences. So the mutual co-operation between countries in necessary to eradicate this evil.

3. Initiatives should be taken to make the victims to report the cases. As there are only very few people who bring such incidents to the notice of the courts, the laws are not that strict and at the same time hackers are not afraid of being caught. So there is need to have a mandatory reporting of cases of hacking and that would make many people to come forward and report the instances of hacking and by that the aspect of negative

publicity get demolished. A portal to register the cases and making the mechanism to report cases through online and processing the cases within reasonable time is necessary.

4. Awareness as to the laws and the Sec.66 of IT Act dealing with hacking is of very less and the need to make common people understand the hacking process and how they can secure their computer system is very important. And the procedure to report the cybercrimes should be made easier without complicated procedures.

5. Awareness is to be done at all age level as children are more prone to be affected by cybercrimes like hacking. The best example is Blue Whale Challenge and Momo challenge which went to the extent of taking the lives of many innocent children who were targeted and threatened by hacking into the mobile or computers which the children were using. So Cyber security education is very important as future generations have to face issues which will be more than what is present now.

6. Even America is worried about India's development in technology and so they came up with the legislation which restricted outsourcing government contract in Information Technology to a foreign country. So India is in third position when it comes to a country prone to more hacking, the maximum imprisonment period when it comes to hacking should be extended so that it makes people understand the intensity of the crime. Countries like China have minimum imprisonment period of 3 years whereas in India it is the maximum.

7. Since the issues tend to not start and end in one jurisdiction, there is a need for international forum which should be a neutral organization to decide the issues regarding cybercrimes. India is in need of proper precedents or legislations which clearly mentions on what basis the jurisdiction is decided when it comes to cybercrimes like hacking.

8. Being an extraditable offense, nothing can be done without the co-operation of the other countries and the other countries don't really offer to help because hacking into their enemy countries websites is benefitting them in one way or the other. So there is need to protect government websites with strong technical team and employing more ethical hackers.

X.CONCLUSION

The paper has widely discussed on the evil called hacking right from history to its development today. It requires awareness from the people and also the government to strengthen themselves in order to defeat any kind of cybercrime. No citizen can be deprived of his -2 With new technology comes new danger so law should always be prepared to be dynamic and change itself in a way to overcome such danger. Judiciary should be always ready to take judicial activism into its hands as we are all aware that legislature even if it works the entire year cannot match up to the dynamic nature of cybercrimes. Cybercrime being a global crime requires the

co-operation as well as technological support from other countries to ensure the citizens of their own country are protected.

.