Cyber Security: Attacks, Implications and Legitimations across the Globe

Samanjeet Kaur
Student
CSE Department, BBSBEC
Fatehgarh Sahib

Sukhwinder Sharma
Assistant Professor
CSE Department, BBSBEC
Fatehgarh Sahib

Amanjot Singh
Associate Professor
Electronics Department
Gurukul Vidyapeeth, Banur

ABSTRACT
This paper confers the importance of the cyber security and the economic deprivation caused by the flourishing cyber attacks. The review delves into growing exploitation of the computer which has given space to the present-day crimes. In extension to this the legislative framework has been taken up to provide the outline of the laws to curb cyber crime over the globe.

General Terms
Cyber attacks, Implications, legislative measures.

Keywords
Cybercrime, Cyber law, DOS, WSN, FEBRABAN.

1. INTRODUCTION
The tact of the modern nation or the society is the cause of vulnerability in itself. High addiction of information technology made us liable to the cyber attacks that disturb the data that progressively lubricates our economy and the structure of the government. Number of incidents of cyber attacks in form of the email bombing, information or the data theft, DoS attacks, Trojan attacks, hacking the data or the system are being committed. Cyber crime refers to action of carrying out criminal activities by using the medium of internet, computer, cyberspace. Although no other technical definition by any legal or the lawful body for cyber crime. It is being defined by computer research centre as “Crimes committed on internet using the computer either as tool or a target”[1]. Heightened role of information technology and rise of the e-commerce sector has turned cyber security into a very crucial policy issue all over the world. Cyber security means safeguarding information, assets and the computer document or the resources stored. As in the growing era modern thief can steal more with the computer than the gun.

2. HISTORY
The first recorded cyber crime took place in the year 1820 which is not shocking or unpredictable considering the fact that abacus which is considered earlier form of computer, was there in India, China, Japan since 3500 B.C. In the age of the modern computers, however initiated with the analytical engine of the Charles Babbage. In 1820 Joseph Marie Jacquard, a textile manufacturer in France produced the loom. This device allowed the repetition of the series of the steps in weaving of the series of special fabrics. This created fear among the Jacquard’s employees that their traditional employment and livelihood were being threatened, then they committed the acts of sabotage to discourage Jacquard from further using of new technology. This was the first recorded cybercrime [1].

3. CYBER ATTACKS
Various types of cyber attacks are [1,6,11]

3.1 Denial of Service Attacks
Any interference into the system by damaging the network with the motive to deny the service to the recognised or the authorized user. It is the type of attack where the attacker makes the memory resource or computing too engaged to handle appropriate request, and turndown the appropriate user access to a machine.

3.2 Unauthorized Access and Hacking
Unauthorized access means gaining entry or any kind of access without the permission of intended or certified owner, whereas hacking can be defined as any act regarding breaking into other’s computer or network with the intent to steal or destroy important data. Hackers usually make use of the readymade computer programs to target or attack the destined or target computer.

3.3 Trojan Attacks
They are the programs that sometimes looks useful but are damping. These kind of programs are called Trojans.

3.4 Virus and Worm Attacks
The program that is being capable to affect or infect other programs and makes replication of it spread into other programs called virus. Worms are Programs that spread like virus but spread from computer to computer.

3.5 Email Bombing
It is repeatedly sending identical messages to the particular address, sending threatening emails, email frauds etc.

3.6 Cyber Stalking
It is mental or physical threat that create fear through the use of web cam, websites, email, phones, videos.

3.7 Cyber Squatting
It the act where registering the domain name which is identical or same to the trademark which is already registered by another.

3.8 Cyber Trafficking
It is greatest crime attack where trafficking of drugs, arms weapons are done which can effect larger number of population.

3.9 Phishing
In the following attack usually the usernames, passwords, personal details, credit card information, are being acquired by the medium of electronic communication. Bogus or fake emails are being used to provide the link of the bogus
websites or virus prone sites to access the information of the victim.

3.10 Forgery
Postage ,market sheets ,currency notes, revenue stamps are being forged using printer, computer ,scanner with the wrongful intention fake mark sheets or even certificates are being made in the following.

3.11 Salami Attack
This attack is done with extreme intelligence which sometimes goes unnoticed as alteration done is so powerful .Process in attack sometimes includes the program which is inserted by bank’s employ into bank’s server that can deduct small amount of money from each account of employ.

3.12 Cyber Terrorism
It is growing worldwide attack where instead of weapons internet is chosen as the medium to cause harm, exploitation for the personal interest or to terrorize the government or people for political or social objective.

3.13 Defamation
It is mainly done in order to take revenge or for enjoyment purpose to lower the status of the person by hacking his/her account and sending wrong messages or posts from the victims account to the unknown person’s account.

3.14 Cyber War
It is the act where one nation aims to hamper or cause disruption of others nation network and to gain access to the crucial websites, services or to swipe information and cripple the economic system.

3.15 Attacks on WSN
An attack that inhibit sensor from identifying or detecting and transferring data through the network.

4. CYBER ATTACK IMPLICATIONS
Cyber crimes effects Citizens, Business, Government in variety of ways, loss of sensitive business information, loss of customer trust, cost of restoration of business, loss of intellectual property and trade secrets etc are being prevalent .

In the Report of June 2014 taken by Center for Strategic and International Studies stated that yearly cost to the global economy by the incidents of cyber crime is more than $400 billion .Cyber crime implications will progressively increment more and more as business functions are continuously flourishing their business online and more of the company’s and customers of the world are linking to the internet.

In the developed countries cyber crime effects employment rate, studies suggest that damage from cyber crime can cost 200,000 American jobs, nearly a third of 1%full in the employment. 2013 Report regarding the incident where 3000 companies in US were being hacked as notified by the Government.

In the Brazil the condition is more worst as in accordance of 2012 data from FEBRABAN, Brazil losses $1.4 billion from the cyber attacks whereas more than 45% Brazilians are the users of the internet [13].

According to ponemon institute research report of 2013 loss occurred due to cyber crime attacks in France is $5.19 million where as the recent attack reported that France faces 19000 cyber attacks since the terror rampage [12,16].

The Detica report states that about 91% percent of the UK business and 93% households have access to internet and about £27 billion is estimated cost of the cyber crime in UK. Business is highly influenced by the cyber attacks and loss of £21 billion is reported. In the government sector loss incurred is £2.2 billion and stated economic loss to the UK citizens is £3.1 billion per annum [4].

According to the report of Cert-In revealed that they handled 71000 cyber security incidents in 2013 in India, the cyber frauds in 2013 cost $870 million and 69%attacks targeted on large scale companies of India .About 308,371 websites were being hacked in the period between 2011-june,2013.This sometimes may provide the partial picture as most of the incidents goes unreported Income level is the valuable predictable of the cyber crime, the upscale countries are more likely to be targeted ,as the better results are produced by rich targets [10,13].According to the article of The Times of India it was stated that Pune is ranked third among the other cities that are troubled by cyber crimes in 2011[17].

5. LEGISLATIVE MEASURES ACROSS THE GLOBE
To tackle the issues regarding cyber crime and to curb the attacks various nations have enacted different laws on cyber crime

In India to cater the issues of cyber security India has implemented IT (amended) ACT 2000 and IPC (Indian penal code). Cyber security policy 2013 was also introduced. Different crimes like data theft, phishing, identity theft, source code theft, spreading of virus etc have been considered in detail. Several cyber crimes has been depicted as offences, objective of the IT act is to implement legal backbone for enabling e-commerce in country .IT act includes the documents concerned with plagiarism, hacking etc, whereas IPC includes the crimes likes theft, forgery, ,fraud ,CERT-IND can instruct or guide the department of telecommunication to block the website, according to the law passed on 27 feb,2003 regarding the blocking of websites [8,10,17].

Cyber laws in France are enacted to curb unauthorized access to automated data processing system, child pornography ,violation of personal rights resulting from computer processes or files. In 2011 France adopted the law that obliges ISP’s and social network to store personal data of internet user’s for period of 1 year.

In Brazil Carolina Dieckmann Law which named in reference to the actress whose intimate photos were released online. It criminalized theft of email, unauthorized access, and online source of sensitive information. Many others laws like Azeredo law are also present. various government bodies like CEPESC, computer emergency response team brazil whose assignment include receiving ,reviewing ,responding to the computer security incidents ,and all the reports and activity related to network that is linked to Brazilian internet [15].

Legislative measures in UK were enacted against any unauthorized access to the computer material, unauthorized access with aim to facilitate further offences, unauthorized manipulations of computer material. Various penalties are enacted to curb the crime, penalty vary from fine to imprisonment from period of six months to ten years depending on the type or nature of crime.

For the US, the National Cyber Security Division (NCSD) which is Department of Homeland Security liable for securing cyber infrastructure aims to secure cyberspace, it classifies
two objectives first one is to build and maintain the effective national cyberspace response system second one is to implement a cyber-risk management program for securing critical infrastructure. Cyber law is being enclosed in title 18 of US code, which is the criminal and penal code of United States. 18 US code sets the penalties against online theft, child pornography, intrusion into computer system, identity theft. Various acts like electronic communication privacy act of 1986 describes the need for disclosure of data, interception of communication data, condition for mobile tracking devices, also covers oral, interception of wire and the preservation of electronic communication and disclosure of stored wire. Further in 1994 US modernized its lawful capabilities by passing the communication benefit for Law Enforcement Act[9].

6. CONCLUSION
Currently, criminals have alternated the approach and started adopting advanced technology to deal with them, the legal, law enforcement and the society will have to change. Cyber crime is caused due to the lack of awareness. This is the responsibility of the Government, media to educate the people about the critical fields of cyber-world as “prevention is better than cure”. Also, careful measures should be taken appropriately while using internet which will aid in challenging this large scale threat.

7. REFERENCES
[3] Introduction to cyber crime Available:“wsilfi.staff.gunadarma.ac.id/Downloads/files/.../W03Cyber+crime.pdf”.
[7] Jose Nazario “Politically Motivated Denial of Service attacks”.