Cyber Attack and Cyber Law

Deshak Bhatnagar

Abstract-This Research looks at the current and upcoming developments in Cyber world and discloses Cyber Attack and its effects, types. It also illustrates the Laws in context of Cyber Attack. The laws consist components like extent, jurisdiction and IT law 2000 (India). It further consists Analysis and Conclusion and various Ideas or thinking's to counter cyber Attack and to strengthen the Cyber Law.

Index Terms- Factors, Attacks, Laws (keywords)

I. INTRODUCTION

A Cyber Attack is any form of offensive operation utilized by nations, people, groups, organizations that concentrate on laptop data systems, infrastructures, laptop networks and private laptop devices by numerous means that of malicious acts sometimes originating from associate anonymous supply that either steals or destroys a nominal target by hacking into a prone system. These may be Cyber Campaign, Cyberwarfare in several contexts. Cyber Attacks may be from putting in spyware on a laptop to tries to destroy the infrastructure of entire nations. Cyber Attacks became more and more subtle and dangerous because the Stuxnet worm recently incontestable.

Cyber Law or web Law could be a term that encapsulates the legal problems associated with use of the net. it's less a definite field of law than material possession because it could be a domain covering several areas of law and regulation. Some leading topics embody web access and usage, privacy, freedom of expression and jurisdiction. laptop Law could be a third term that tends to relate to problems as well as each web Law and also the patent and copyright aspects of engineering and computer code. conjointly IT Law consists of the law that governs the digital dissemination of each data and computer code itself and legal aspects of knowledge technology a lot of generally [7].

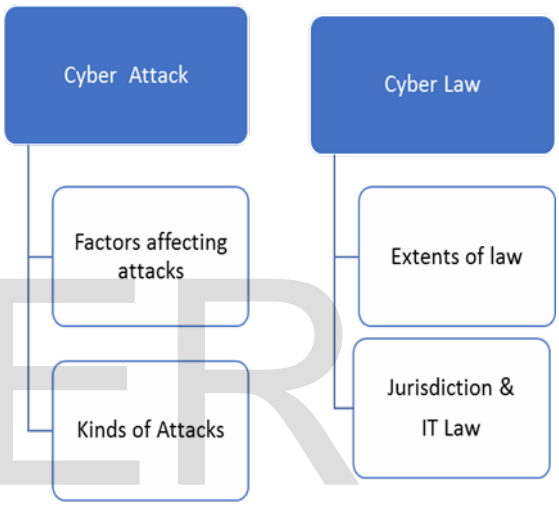

Fig 1. Flowchart on Components of Cyber Attack & Cyber Law

II. FACTORS AFFECTING ATTACKS

Three issues contribute to why Cyber Attacks square measure launched against a state or associate individual: the concern factor, spectacular issue and vulnerability issue:

1. Concern Factor: the foremost common, concern issue, a cyberterrorist can produce concern amongst people, teams or societies. The bombing of a Ball nightspot in 2002 created concern amongst the foreign tourists UN agency often visited the venue. Once the bomb went off and casualties ensued, the inflow of tourists to Ball considerably reduced owing to concern of death. folks argue that act of terrorism isn't terribly totally different than terrorism. Basically, Cyber Attacks square measure geared toward ingraining concern to impose demands or claims of any kind. in sight of

IJSER

that, this professional says that in those societies familiarized to rationalization and planarization, the chances terrorist act surfaces square measure over ancient past-oriented communities. What disturbs the social order is that voters don't grasp once future blow can happen, nor where.

2. Spectacular Problem: - With spectacular factors, it is the particular injury attack, means the attacks which cause losses. In year 1999, a attack was made useless and amazon lost heavily due to suspicious mercantilism and absolutely became known all over the world.

3. Vulnerability Factor: Vulnerability issue exploits however vulnerable a corporation or government institution is to Cyber Attacks. a corporation may be prone to a denial of service attack and a government institution may be marred on an online page. A electronic network attack disrupts the integrity knowledge sometimes through malicious code that alters program logic that controls data, resulting in errors in output.

III. KINDS OF ATTACKS

A. Syntactical Attacks and linguistics Attacks-

There square measure variety of techniques to utilize in Cyber Attacks and a spread of how to administer them to people or institutions on a broader scale. Attacks square measure diminished into 2 categories: syntactical and linguistics Attacks. syntactical Attacks square measure straightforward; it's thought of malicious computer code which has viruses, worms and Trojan horses:

1. Viruses: a virulent disease could be a self-replicating program that will attach itself to a different program or get into order to breed. The virus will hide in unlikely locations within the memory of a computing system and connect itself to no matter files it sees suited execute its code.

2. Worms: A worm doesn't would like the other file or program to repeat itself, it's a self-sufficient running program. Worms replicate over a network exploitation protocols. the newest incarnation of worms creates use of legendary vulnerabilities in systems to penetrate, execute their code, replicate to alternative systems like the Code Red II worm that infected quite 259000 systems in but fourteen hours [11].

3. malicious programs: A Trojan horse is intended to perform legitimate tasks however it conjointly performs unknown and unwanted activity. It may be the idea of the many viruses and worms putting in onto the pc as keyboard loggers and backdoor computer code. during a industrial sense, Trojans may be imbedded in trial versions of computer code and might gather extra intelligence concerning the target while not the person even knowing it happening [13].

Semantic Attack- It's the modification and dissemination of correct and misinformation. data changed might are eluded the utilization of computers even supposing new opportunities may be found by exploitation them. to line somebody into the incorrect direction or to hide your tracks, the dissemination of misinformation may be utilized [12].

B. Infrastructural Cyber Attacks -

Once a Cyber Attack is initiated their square measure several targets that require to be attacked to cripple the opponent. sure, infrastructures as targets are highlighted as essential infrastructures in time of conflict which will severely cripple a nation and a few of those square measure as follows.

1. Management Systems: These square measures liable for activating and watching industrial controls. several devices square measure integrated with laptop platforms to regulate valves and gates to sure physical infrastructures. These square measures sometimes designed as remote measuring devices that link to alternative physical devices through web access or modems. very little security may be offered once coping with these devices, sanctioning several cyberterrorists to hunt out systematic vulnerabilities.

2. Energy: it's the second infrastructure that would be attacked. it's diminished into 2 categories: electricity and fossil fuel. Electricity conjointly referred to as electrical grids power cities, regions, households; it powers machines and alternative mechanisms used daily. Using U.S. as associate example, during a conflict cyberterrorist will access knowledge through the Daily Report of System standing that shows power flows throughout the system and might pinpoint the busiest sections of

IJSER

the grid. Cyber Attacks on fossil fuel installations go abundant constant means because it would attack on electrical grids. Cyberterrorists will pack up these installations stopping the flow or they'll be occupied by one amongst their allies.

3. Finance: money infrastructures may well be hit onerous than the other infrastructure by Cyber Attacks because the economic system is joined by laptop systems. If constant cash being changed in these establishments and if Cyberterrorists were to attack and if transactions were rerouted and huge amounts of cash purloined, money industries would collapse and civilians would be while not jobs and security. Operations would stall from region to region inflicting nationwide economical degradation.

4.Tele-communications: Cyber assaultive tele-communication infrastructures have direct impacts. Telecommunication integration is turning into common apply, systems like voice and information processing networks square measure merging. Everything is being run through the net as a result of the speeds and storage capabilities square measure endless. Denial of service attacks may be administered as antecedently mentioned however a lot of advanced attacks may be created on BGP routing protocols or DNS infrastructures. it's less possible that associate attack would target the normal telephone network of SS7 switches or associate tried attack on physical devices like microwave stations or satellite facilities. the full plan behind these Cyber Attacks is to chop folks aloof from each other [10].

IV. EXTENTS OF CYBER LAW

Cyber Law doesn't represent a separate space of law rather it encompasses aspects of contract, material possession, privacy and knowledge protection laws. material possession is a crucial part of IT Law, as well as copyright, rules on use and special rules on copy protection for digital media, escape of such schemes. the realm of computer code patents is arguable and still evolving in Europe. There square measure rules on the uses to that laptops and computer networks could also be place particularly their square measure rules on unauthorized access, knowledge privacy and spamming [1]. There also are limits on the utilization of coding and of apparatus which can be wonted to defeat copy protection schemes. There square measure laws governing trade on the net, taxation, shopper protection, advertising. There square measure laws on censorship versus freedom of expression, rules on public access to government data and individual access to data prevailed them by personal bodies. There square measure laws on what knowledge should be preserved for enforcement, what might not be gathered or preserved for privacy reasons. In sure circumstances and jurisdictions, laptop communications could also be employed in proof and to ascertain contracts. Some states limit access to the net, by law additionally as by technical means that [3].

Section Under, IT Act 2000	**Offences**	**Penalty**
Sec.43	Damage to computer, computer system, etc.	Compensation not exceeding one crore rupees to the person so affected
Sec.65	Tampering with computer source documents.	Imprisonment up to three years, or with fine which may extend up to two lakh rupees; or with both
Sec.66	Hacking with computer systems, Data altercation etc.	Imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupess or with both
Sec.66A	Sending offensive messages through communication service etc.	Imprisonment for a term which may extend to three years and with fine
Sec.66B	Retains any stolen computer resource or communication device	Imprisonment for a term which may extend to three years or with fine which may extend to rupees one lakh or with both
Sec.66C	Fraudulent use of electronic signature	Imprisonment for a term which may extend to three years and shall

IJSER

		also be liable to fine which may extend to rupees one lakh
Sec.66D	Cheats by personating by using computer resource	Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees
Sec.70	Un-authorised access to protected system	Imprisonment for a term which may extend to ten years and shall also be liable to fine
Sec.72	Breach of confidentiality and privacy	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both
Sec.72A	Disclosure of information in breach of contract	Imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both
Sec.73 & 74	Publishing false digital signature certificate	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

Table 1- Penalties and Offences

V. JURISDICTION & IT LAW

A. Jurisdiction -

If against the law is committed on a laptop or electronic network in Republic of India by someone resident outside India, then will the offence be tried by the Courts in India? in step with Sec.1(2) of knowledge Technology Act, 2000, the Act extends to the full of Republic of India and conjointly applies to any offence or resistance committed outside India by a person. Further, Sec.75 of the IT Act, 2000 conjointly mentions concerning the relevancy of the Act for any offence or resistance committed outside Republic of India. in step with this section, the Act can apply to associate offence or resistance committed outside Republic of India by a person, if the act or conduct constituting the offence or resistance involves a laptop, computing system or electronic network settled in Republic of India. A peace officer not below the rank of Deputy Superintendent of Police ought to solely investigate any offence underneath this Act. (Sec.78 of IT Act, 2000). While not a punctually signed surrender accord or a multipartite cooperation arrangement, trial of such offences and conviction could be a troublesome proposition. Sec.79 deals with the immunity available to intermediaries. The Information Technology (Intermediaries guidelines) Rules, 2011 governs the duties of intermediaries. "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes [6].

B. IT ACT 2000 (India) -

IT ACT 2000 is the first landmark in the cybercrime world by India. It is based on the United Nations Model Law on Electronic Commerce 1996. The original Act contained 94 sections, divided in 13 chapters and 4 schedules. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India. IT ACT provides legal platform for assembling and storing electronic data within the international marketplace. This act comes into play when the disputes arise within the Information technology field that can't be resolved, then a special kind of attorney is required and it is called Information technology lawyer, which specifically deals in these situations. The controversial Section 66A was introduced in 2008, which reprimanded sending of

IJSER

offensive messages. Also, consequences for child porn, cyber terrorism and voyeurism were introduced in 2008. Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 [8]. Section 3 deals with the conditions subject to which an electronic record may be authenticated by means of affixing digital signature which is created in two definite steps. First, the electronic record is converted into a message digest by using a mathematical function known as 'Hash function' which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature [9].

VI. Conclusion

The ability of human brain is profound. It is store to a lot of destructive as well as useful things and Cyber Attack is one of the destructive things or Idea that have been in and around us from long time but several Laws have been made to counter it to some extent. According to my Analysis Cyber Attacks are easy to handle and operate but are very difficult to completely stop or restrict and can be minimized to some extent. From my Research I went to a conclusion that is terrifying that is we actually don't have a strong Global Law or a common Law around the world which can help in stopping the Attacks, but interestingly I found that the IT ACT 2000 that is the law applicable in India in terms of Cybercrime is not so influential or productive in stopping these attacks actually it have some loop holes that have to be addressed as soon as possible, the main problem with this law is regarding the punishment given to the guilty and the duration of punishment and another major problem is not so strict laws for the intermediaries (the people who help the guilty), this is the main loop hole that needs to be addressed. Furthermore, there is a need for a Global Law in regard to Cyber Attacks and other Cyber Offences in order to restrict them or minimize to a large extent. Also, IPC (Indian Penal Code) is applicable to Cyber offences in India which is not so capable law in this context but still useful. Finally I Conclude that there is a urgent need for a strict regulation to control these attacks all around the world but in context of India, it's the need that has to fulfilled as soon as possible and a way that can give this result is to tighten the Cyber Law and a minimum of 5 years or more of Imprisonment should be there for the guilty and at least a penalty of 20 lakhs should be enforced.

References

[1] Williams, Phil. "Organized Crime and Cybercrime: Synergies." Trends, and Responses, Retrieved December 5 (2006).
[2] Halder, Debarati, Karuppannan Jaishankar, and K. Jaishankar. Cybercrime and the victimization of women: laws, rights and regulations. Information Science Reference, 2012.
[3] Allison, Stuart FH, Amie M. Schuck, and Kim Michelle Lersch. "Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics." Journal of Criminal Justice 33.1 (2005): 19-29.
[4] Finkelhor, David, Kimberly J. Mitchell, and Janis Wolak. "Online Victimization: A Report on the Nation's Youth." (2000).
[5] Nagpal, Rohas. "Cyber terrorism in the context of globalization." II World Congress on Informatics and Law. 2002.
[6] DAVID, S. "The Internet as a Conduit for Criminal Activity." Information Technology and the Criminal Justice System (2004): 77.
[7] Olowu, Dejo. "Cyber-crimes and the boundaries of domestic legal responses: Case for an Inclusionary Framework for Africa." Journal of Information, Law and Technology (JILT) 1 (2009): 1-18.
[8] Kshetri, Nir. "Pattern of global cyber war and crime: A conceptual framework." Journal of International Management 11.4 (2005): 541-562.
[9] Lavorgna, Anita. "Criminal Behavior in the Internet Age: The social organization of Transnational Organized Crime." University of Torento–Italy (2003).
[10] Dashora, Kamini. "Cybercrime in the society: Problems and preventions." Journal of Alternative Perspectives in the Social Sciences 3.1 (2011): 240-259.

IJSER

[11] Ramesh, P., and D. Maheswari. "Survey of cybercrime activities and preventive measures." Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology. ACM, 2012.

[12] Dalla, E. H., and M. S. Geeta. "Cyber Crime A Threat to Persons, Property, Government and Societies." International Journal of Advanced Research in Computer Science and Software Engineering 3.5 (2013): 997-1002.

[13] Firdous, Naira. "Optimized Security Techniques in Cyber World."

[14] Steel, Chad. Windows forensics: The field guide for conducting corporate computer investigations. John wiley & sons, 2006.

[15] Broadhurst, Roderic, et al. "An analysis of the nature of groups engaged in cybercrime." (2014).

IJSER