INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 4

2021

A Brief Study on the Present Position of Hacking and Legislative Approaches for Its Prevention in U.K, U.S.A and India

ABHIRUP BHATTACHARJEE[1]

ABSTRACT

Hacking is one of the most common forms of cybercrime. The truth is that no computing device on the planet is really safe from hackers. Any device on the planet can be compromised. According to Section 66 of the IT Act, 2000. hacking is classified as any person who removes, deletes, or alters any information residing in a computer resource or diminishes its value or usefulness or affects it injuriously by any means with the intent to cause or knowing that he is likely to cause unlawful loss or harm to the public or any person who destroys, deletes, or alters any information residing in a computer resource or diminishes its value or utility or affects it. In today's world, crime on the computer-generated superhighway is a modern phenomenon. We cannot imagine any intellectual or necessary job in our everyday lives without Information Technology. However, deviants and terrorists are abusing and misusing this new multimedia technology. Cyber hacker attacks on the Bhaba Atomic Energy Centre, AIIMS, and the World Trade Center, for example, have resulted in more human life being lost than conventional offences. As a result, in order to protect our everyday lives, businesses, and intellectual property, we must consider the protection and regulation of cyber crimes, especially the most dangerous of which is cyber hacking.

Keywords: *Hacking, Legislative approaches, cyber- crime.*

I. MEANING

It can be defined **as** an attempt to exploit either any computer system or a private network inside a computer. In simple words it is the unauthorised access to control over computer network security systems with a view to fulfil unlawful purpose.

[1] Author is a LLM student at Cooch Behar Panchanan Barma University, India.

 [ISSN 2581-5369]

Hacking in cyberspace is not only a national but also an international legal issue that necessitates global norm protection policies and regulatory enforcement based on extensive worldwide analysis and review.

II. HACKERS

Hackers are those persons who commits the offence of hacking.

- Hackers often portray themselves as –
    - the guardian of fragile and unreliable data;
    - that their actions are legal; and
    - that they are not always lawbreakers.
- This may be because they believe that –
    - Only a small number of claimants are involved in filing a lawsuit against them.
    - Victims are often unable to recognise them. This is attributable to the cyber world's ambiguous and uncertain authority. The victims was usually found guilty of crimes committed thousands of miles apart.
    - Another benefit for hackers who commit crimes repeatedly is that it is very difficult to comprehend violence in cyberspace. For example, hackers view one webpage and, using deep linking, obtain information that is highly confidential without the consent of the owner and download it intentionally and dishonestly; this is a complete case of theft under section 378 of the Indian Penal Code, 1860, which states that any person who takes away any movable property from one place to another without the consent of the owner or possessor is guilty of theft.
    - Illegal use, which is criminal trespass under section 441 of the Indian Penal Code, 1860, as well as hackers that inflict harm, after data, or alter data, are both difficult to detect and understand. As a result, expert hackers believe that cyberspace is their sole domain, and that they can do anything they want in a very discrete manner. They harm not only technological and economic dominance, but also social, cultural, and political values.

Richard Gill, played by Wendell Pierce, the Chief law enforcement officer in the 1995 film 'Hackers,' says "Hackers penetrate and ravage delicate private and publicly owned computer systems, infecting them with viruses and stealing sensitive materials for their own ends. These people …. are terrorists."[2]

[2] Thomas .D and Loader. B.D, *Cyber Crimes, Law Enforcement, Security & Surveillance in the Information Age*, Hackers (united Artists, 1995); 2000, p. 56.

 [ISSN 2581-5369]

R. v. Gold,[3] in the United Kingdom; Mr. Verma IIT, Kharagpur hacking of ex-source employer's code and subsequent arrest by the Central Bureau of Investigations in India with the help of the Federal Bureau of Investigations in the United States; Ankit Fadia's Denial of Service Attack case in India, etc. are examples of how hacking threatens social mechanisms and halts social progress.

- The below are two fundamental rules that hackers abide by, according to the latest Hackers Dictionary:
    - The conviction that sharing knowledge is a strong beneficial good, and that it is a hacker's ethical responsibility to share their skills by writing free software and promoting access to information and computer tools whenever possible.
    - The assumption that machine cracking for entertainment and profit is ethically acceptable as long as the cracker does not steal, vandalise, or disclose sensitive information.[4]

III. PROBABLE WAYS OF HACKING

1. One method of hacking is for a malicious hacker to physically access the premises of another entity containing the device and impersonate the user. That is equivalent to criminal trespass under Section 441 of the Indian Penal Code. Such impersonation is very simple if the owner does not have a protective and security mechanism in place, as well as a hidden password to activate or trigger the operating system.
2. Using a password cracking technique, even an intelligent hacker can be able to guess the password where it is necessary. Password cracking software checks a large number of passwords, finds them if they are written anywhere else, and observes them while in operation, i.e., shoulder surfing.
3. If this fails and the hacker is unable to start the machine without a valid password, the hacker will reinstall the operating system. This hacking process is a bit more complex and time intensive, but it is not impossible.
4. Another method for the malicious hacker to gain access is to trick the rightful user into accessing and running a Trojan horse programme in the machine. A Trojan horse software includes programming commands that are unfamiliar to the user and are used to carry out the hacker's attack.

[3] *R.* v *Gold*, [1988] 2 WLR 984
[4] Parker .D.B, *Fighting Computer Crime*, (Wiley Computer Publishing) 1998, p. 160

 [ISSN 2581-5369]

5. Once again, the hacker can exploit a known flaw in a computer operating system such as UNIX or Microsoft Windows, which is the most technical approach and requires detailed knowledge of the operating system unless a prepackaged search tool such as SATAN is used.[5]
6. Hacking can be accomplished by sending messages via e-mail, blogs, or mobile devices with various deals and sexual accesses and requesting their passwords, social security numbers, and personal information.
7. Rather than their clients' computers, hackers often attack servers because vital information is stored on them. Initially, a hacker attempts to operate the internet and mobile networks. Hackers often use the scanning method to examine hosts' internet behaviours for remote vulnerabilities through a fast fiber-optic link.
8. Another method of breaking and protecting the password is to use mathematical algorithms to try to smash the password hash or cryptographic scheme.
9. Jim Falls[6] Worth collaborated with hackers to consider the aims of penetration testing, also known as fun hacking. And he reveals certain measures and techniques that malicious hackers use without the owner's permission. There are the following:
    i) They evaluate the strengths and disadvantages of a bank's new offerings, as well as their relationship to the rest of the bank's activities.
    ii) They attempt to identify any bugs in those programmes.
    iii) They have solutions to improve device security.
    iv) They explain the risk of bank or customer risks by breaking into the bank.

IV. CRACKING, PHREAKING AND HACKING

Crackers are hackers who inflict severe or dangerous damage to computers and operating networks, as well as network security systems, and smash systems. They conduct not only illegal trespass or unlawful entry, but also other offences. Crackers usually attempt to target servers where they can quickly obtain vital information from a large number of people. As a result, they aim through the internet and telecommunications network. Phone hackers became the most common kind of phreakers. They gain unauthorised access to the computer system via phone.

They unlawfully access computer networks for a variety of reasons, such as gathering information and selling it for the sake of curiosity or as a game. Phreakers commit

[5] Parker .D.B, *Fighting Computer Crime* (Wiley Computer Publishing) 1998, p. 165
[6] Schwartau. W, *Cyber Shock*, Thunder's Mouth Press, NY, 2000, p. 182

pranks/phreakes by changing phone systems, redirecting calls, and rearranging web sites. They do so without really intending to benefit financially, even though their actions result in losses for corporations, industries, government departments, individuals, and so on.

Ethical Hacking

When a company has someone from the outside to inspect their networks for illicit hacking, they recruit certified ethical hackers. Ethical hacking is practised by software developers, B.Sc. (Computer Science) majors, and everyone who understands programmes and codes and knows how to manipulate a machine. They provide IT businesses with online surveillance, patrol internet highways, plugging holes and stopping online crime.

V. POSITION OF CYBER HACKING IN UNITED KINGDOM AND THEIR LEGISLATIVE APPROACHES

While highliting the situation of hacking in United Kingdom (UK), Professor L. Lloyd says,[7] "the stereotypical depiction of a cyber hacker tends to be that of a male teenager in a greasy T-shirt and torn jeans who spend hours slumped over a terminal, eyes gazing fixedly at the green glow of the VDU monitor. No where is safe, no one can keep him out, no one knows of the scale of the threat, the silent deadly menace stalks the networks as seen in R v. Gold."[8]

Prior to the Computer Misuse Act of 1990, there were regulations in the United Kingdom banning the misuse of public networks, such as the Theft Act and the Telecommunications Act of 1984. The Interception of Information Act of 1985 bans forgery and other illegal acts in the process of public telecommunications transmission. The Data Protection Act of 1984 was enacted to protect electronic data and databases from unauthorised access or destruction.

The Computer Misuse Act of 1990 creates the following three additional felony offenses[9]:

- Unauthorized use of electronic content This is analogous to accessing a device without authorization, i.e. hacking with the purpose or awareness of connecting to another computer.
- Unauthorized access to electronic content with the intent to perform or assist in the committing of additional offences. This is referred to as malicious hacking or breaking.
- Unauthorized alteration of electronic content This are banned under Section 3 of the Act. Section 6 of the Act makes it a crime to conspire to commit the aforementioned

[7] Lloyd. L.J. *Information Technology Law*, 3rd Ed., 2000 (BW), p. 27.
[8] (1988) AC 1060.
[9] CP3349&CP4018 unauthorized access. For detail see http://www.apcomms.org.uk/apig/ archive/ activities- 2004 /computer-misuse-inquiry.html visited on 09.05.2021

offences.

- According to a survey conducted by the Confederation of British Industry (CBI), with the growing scenario of cyber hacking, the growth of e-business in Britain is also facing challenges. The CBI also announced that two-thirds of the businesses have been subjected to cyber threats such as theft, malware infection, credit card fraud, and so on. As a result, they recommended to the British Government to behave cordially and to assist in combating cybercrime, to provide a centre for cybercrime grievances, and to broaden and extend the Computer Misuse Act of 1990 to include attacks that trigger the collapse of an information technology infrastructure.[10]

VI. POSITION OF CYBER HACKING IN UNITED STATES OF AMERICA AND THEIR LEGISLATIVE APPROACHES

The United States of America (USA) passed numerous Federal and State Laws to regulate and deter cyber crimes such as hacking, interfering with source information, cyber theft, cyber fraud, cyber bullying, cyber pornography, and so on, by and by computer, computer device, and computer network.

The Spyware Control and Privacy Protection Act of 2000 is one such Act designed to deter and control hackers in the United States. The Act forbids all misleading acts pertaining to Spyware[11], such as unlawful use of a secure device and committing such crimes as a result. In this scenario, the registered user cannot access the internet browser until all programmes are closed, the device is turned off, or the internet browser is diverted. As a result, this is a kind of Denial of Service (DOS) attack. The Act therefore forbids unwanted changes to device configurations, networks, and web pages. The sentence prescribed by the Act is a fine of $3,000,000 and a penalty of $1,000,000.

In the case of United States v. Amato,[12] Amato was charged with breaking NASA administration rules and directives. He was a NASA contract employee in Ohio who, without permission, downloaded a ‘Zipped computer file' named ‘ZIP-42' from the internet and sent it to an e-mail address on the NASA e-mail server seven times, causing international harm of approximately $ 12,000. The maximum penalty for violating Title 18 USC Section 799 and NASA's Rules and Regulations is seven years in jail and a $100,000 fine, or both.

[10] British E-Business Warned of stifling risks, by Cyber crimes Xin hua General News Service, Art ID: 848

[11] The Spyware Control and Privacy Protection Act, 2000; Section 2(1)

[12] (N.D. Ohio) 13th February 2003, 1A/US Department of Justice, press release

In the case of United States v. A. Lamo,[13] The FBI pled guilty to the Manhattan Federal Court that Lamo had been breaking into the New York Times' internal computing network. The accused have had access to a database containing sensitive details such as phone numbers and Social Security numbers of over 3,000 contributors to the New York Times OP-Ed Page. The Times lodged a lawsuit against Lamo right away. He was prosecuted under Title 18 of the United States Code, Parts 1030 and 1023. The District Court sentenced Lamo to five years in jail and a $250,000 fine.

VII. POSITION OF CYBER HACKING IN INDIA AND THEIR LEGISLATIVE APPROACHES

The server is in one state and the consumer is in another in the globalised, liberalised world of communication fusion and emerging technologies. Owing to the lack of defined jurisdiction, the enforcement of law in cyberspace is extremely complicated. It is a legal challenge on both an international and national level. Following the United Nations Model Law of 1997, India adopted the Information Technology Act of 2000. Hacking and unauthorised access to computers, operating systems, and computer networks was addressed in Sections 43 and 66 of the Information Technology Act of 2000.

(A) India's Legislative Approach

1. Civil Liability

The Information Technology Act of 2000 establishes penalties for causing harm to a device, computer system, or computer network without permission from the user, in-charge, or other designated official, as well as abetment.[14] The word "harm" refers to any action that destroys, alters, deletes, adds, modifies, or rearranges any computer resource. Unauthorized access to infrastructure, the uploading and spreading of malware, destruction, interruption, denial of service, tampering or exploiting, and abetment of these are all punishable by a gross liability of Rs. 1 crore in compensation to the claimant. The Cyber Appellate Tribunal will decide on the legal redress that is open to victims.

2. Criminal Liability

Any legislation is in development in today's progressive and diverse social phenomena, and we hope that this is also so for the Information Technology Law. Several aspects of the Act of 2000 remain unclear, For example wrongful loss is not defined in IT Act, but it is defined in the Indian Penal Code, 1860.[15] It does not define the terms such as destroy, alteration, delete,

[13] (S.D.N.Y.) 8th January 2004, CI 3000 K private, US Department of Justice, press release; For detail see
[14] The Information Technology Act, 2000
[15] Indian Penal Code 1860; Section 193 and 228

hacking. Unauthorized access is relevant in criminal trespass which is defined in the Indian Penal Code, 1860

The Information Technology Act, 2000 define 'hacking' as: "Hacking with computers system (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. (2) Whoever commits hacking shall be punished with imprisonment up to 3 years or with fine which may extend up to Rs 2 lakh or with both."[16]

(B) Judicial Approaches

1. **ATM Hacking:** A private company lodged a lawsuit alleging that money was stolen on July 30th using a login that had been hacked by the accused. Mr. Rajesh Malhotra, a 27-year-old programmer, was arrested by the New Delhi Police on August 10, 2004. He was charged with stealing Rs. 3 lakhs from an ATM computer in Mayur Vihar. The accused was still held responsible for the same sum of money. After that, he was released on parole.[17]

(C) IIT Kharagpur Case

The Central Bureau of Investigation (CBI) in India arrested Mr. Shekhar Verma, a 27-year-old software engineer, for allegedly attempting to unlawfully sell the "Source Code" of a sophisticated software package worth around $70 million, thanks to the FBI's cooperation and successful coordination. "Solid Works 2001 Plus" was the package's name. Kharagpur, the rogue IIT alum, was apprehended while attempting to sell the same package to two undercover FBI officers at the Ashoka Hotel. Undercover FBI agents, he claimed, were members of a single US corporation. As a result, he had made a $ 2,00,000 deal with them in exchange for the stolen source code. He was a former employee of Mumbai-based tech firm Geometric Software Solutions Company Ltd. He took the entire Source Code while in operation and, after resigning, began contacting other tech firms in the United States by e-mail, which was seen as a very shameful act. This is also to be considered a hacker's cyber scam.[18]

(D) Delhi Hacker's case

The case of the Delhi Hackers began on February 6, 2001, when two hackers were apprehended by Delhi Police. 98 The most recent breaking news in India was the arrest of two people by the

[16] The Information Technology Act, 2000; Section 66
[17] *Times of India*, 10th August and 12th November 2004.
[18] Daniel. C, Shameful Crime by Software Engineers Times news Network, Tuesday, 27th August 2002,

 [ISSN 2581-5369]

Delhi Police for allegedly hacking a website. This was most likely the first occasion in which the suspects is apprehended in India. Both hackers were arrested on suspicion of blocking the website www.goZnextjob.com. This website helps prospective employers and job seekers by providing resources and information. The accused wrote a note on that website claiming it was closed, but it was already operational. The hackers were held in judicial detention for 14 days after being charged with criminal breach of confidence under section 406 of the Indian Penal Code, 186o as well as under section 66 of the IT Act for the offence of committing hacking.

(E) Arrest of ISRO's Ex-Scientist

Even on September 21, 2001, an ISRO ex-scientist was arrested for e-mail threats to the Department of Atomic Energy and hacking of an Internet Service Provider, Icenet, in Ahmedabad, India, as well as for sending e-mail threats to the nation's defence, all of which should be considered cyber terrorism.[19]

(F) The Case of Hacker Kalpesh Sharma

On September 26, 2003, media reports revealed that hacker Kalpesh Sharma had been arrested and imprisoned in Ahmedabad. He was arrested on September 24th by Mumbai Police's Cyber Crime Branch on a complaint filed by a UTI Bank official alleging that the accused hacked UTI Banks' website, www.uti.com, on July 11th and sent an e-mail to the bank's authority stating that "the website is vulnerable and they should provide protection." He mentioned that he can provide protection in return for Rs. 15 lakh and provided his contact information. He was arrested in Ahmedabad and charged under sections 66 and 43 (b) of the IT Act 2000, and he was remanded in police custody.[20]

VIII. PROTECTION AGAINST HACKING

Social engineering is a common tactic used by hackers. They also try to learn about the target technologies, use free online resources, and create their own knowledge gathering tools. As a result, we'll need more teeth and claws to deter and manage this highly competitive and complicated situation. Another method of concealing e-mail is cryptography, which requires constant decryption in order to restore the secret letter to usual text or plain text, making cancellation very difficult. As a result, encryption and decryption keys must be used for both transmitting and receiving messages in order to communicate.

[19] Cyber Crimes News, 21st September 2001, for details see http://www.cyberlaws.net and also http://cyberpolicebangalore.nic.in/internetrules2.htm.

[20] http://utcursch.wordpress.com/my-answer-to-kalpesh-sharma's-allegations/.visited on 02.05.2021 at 06.40 P.M

Teenage hackers, such as Ankit Fadia, 14, and Neeraj Pattath, 17, have been selected by the NASSCOM, Mumbai Police, and other Indian committees to advise on how to (1) set up anti-hacking mechanisms, (2) detect hacking, and (3) solve hacking problems. They are to be referred to as ethical hackers, similar to Kevin Mitnik in the United States. A big breach occurred. Denial of service attacks by Pakistani hackers community, for example, were stopped by Mr. Ankit Fadia when he was just 16 years old. He discovered that it came from Pakistan.

IX. CONCLUSION

Since cybercrime as well as hacking is a global phenomenon, it usually affects people who are far away from the crime scene, whether they are in the same country or not. As a result, it necessitates international policing as well as the active participation of the international community. Only a few nations have revised their cyber legislation to effectively combat cyberspace crime like hacking, according to a nation-by-nation study of cyber law, and many more have not yet begun to frame laws for policing against these crimes. This disparity in world nations' views on the importance of cyber law creates a serious challenge in dealing with internet crime while also providing enough opportunities for cyber criminals and hackers to avoid detection and punishment. As a result, all nations should recognise the importance of raising awareness about the dangers of cybercrime like hacking, which is perpetuating illicit online activities in cyberspace. Cybercrime is probably the worst disease of the new century, and it must be combated by implementing a global prevention strategy.

*****

 [ISSN 2581-5369]