TuijinJishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 6 (2023)

Preventing Computer Devices from Cyber Crimes

Nityash Solanki [1], Prof. S.P.S. Shekhawat[2]

[1] *Ph.D. (Research Scholar), Jagannath University, Jaipur, Rajasthan, India*

[2] *Head & Dean, Faculty of Law, Jagannath University, Jaipur, Rajasthan, India*

Abstract:-Cyber security challenges demands States to be well-equipped with proactive responses to shield information and communication technology against cyber crimes. Newness in computer related criminal offences has empowered hackers to vandalize the digital communication systems causing privacy concerns for business organizations and security concerns for sovereign States. Hackers are perceived as obsessive people who voluntarily disrupt the integrity of computer systems jeopardizing sensitive information stored therein. Emerging cyber security breaches demands complacent legal regimes to implement cyber specific legislations for identifying computer vulnerabilities and to safeguard individuals, business organizations and government from criminal misconducts in cyber space. The concept of 'authorization' or 'unauthorized access' to data needs refinement since lack of 'due care and appropriate measures' would most likely fail to establish the culpability of the accused hackers.

Keywords*: Computer programs, Cyber Security, Digital Communication, Hackers, Unauthorized access.*

1. Introduction

Digital innovations have revolutionized our life on earth. In the last decade, Artificial Intelligence (AI)[1] proved efficient in finding methods to enhance the overall computing power especially to combat complex problems and cyber crimes faced in using blockchain technology. In July 1956, the Summer Research Project of Dartmouth College researched to discipline the essence of intelligent machines through collection of data which led to the growth of AI techniques. Digital currencies, such as Bitcoin that uses blockchain technology to record information related to business transaction to some extent mitigates incidents of cyber crimes.[2]

At present, cyber security challenges demands States[3] to be well-equipped with proactive responses to shield information and communication technology against cyber crimes. In this paper, readers will be directed to comprehend new age cyber crimes to make life untiringly easier in digital world. Criminal behavior in cyber crimes has been categorized by authors around the globe in numerous ways. Making use of computer programs, as a tool or a target for committing criminal offenses such as fraud; computer crimes involving intellectual property incidental and unique to computer environment; intangible activities that distributes computer viruses/malicious programs to attack the integrity of computer systems; are few examples of committing cyber crimes.[4] Newness in computer related criminal offences has empowered hackers to vandalize the digital communication systems causing privacy concerns for business organizations and security concerns for sovereign States.

[1] Selma Dilek, HuseyinCakir and Mustafa Aydin, "Application of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review" (Jan. 2015) 6(I) International Journal of Artificial Intelligence & Applications, available at https://arxiv.org/abs/1502.03552 , last accessed on 30th December 2023.

[2] Michael Crosby et al., "Blockchain Technology: Beyond Bitcoin" (2016) 2 Applied Innovation Review 8, available at https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf, last accessed on 30th December 2023.

[3] "UN Cybersecurity Challenges: Countering Digital Terrorism", United Nations – Office of Information and Communications Technology, 2019, available at https://ideas.unite.un.org/counterdigiterrorism/Page/Home, last accessed on 30th December 2023.

[4] Ian Walden, "Computer Crime" in Chris Reed & John Angel (Eds.), Computer Law (3rdEdn. Oxford University Press) 277, available at https://archive.org/details/computercrimesdi0000wald, last accessed on 30th December 2023; D.S. Wall, "Policing and Regulation of Cyberspace" in Crime, Criminal Justice and the Internet (Special Edn. Crim L Rev, Sweet & Maxwell, London 1998) 79-91, available at https://www.routledge.com/Cyberspace-Crime/wall/p/book/9781138709010, last accessed on 30th December 2023; See also S.K. Verma& Raman Mittal (Eds.), Legal Dimensions of Cyberspace (Indian Law Institute, New Delhi 2004) 229, available at https://openlibrary.org/books/OL22538494M/Legal_dimensions_of_cyberspace, last accessed on 30th December 2023.

2. Response Mechanism to Computer Crimes

A. United Kingdom

Security breaches through cyber crimes are most annoying since contemporary legislations falls short to tackle criminal behavior in computer related crimes. As a matter of fact, in *R vs. Gold*,[5] it was opined that attempts to extend traditional legislations to incorporate instances of computer-related crimes makes things difficult for judges to adjudicate offences in cyber age. Furthermore, a need was felt to reform existing laws that could serve the purpose of safeguarding computer technology from external malwares such as viruses or codes.[6] Hacking or tampering with data stored in internet devices by cyber infiltrators not only creates mischief in business transactions but disturbs the entire equilibrium of the communication system for unlawful gains. Such unauthorized access to confidential information is most annoying when it is targeted towards software used for military purposes. For instance, in 1998, a religious separatist group, commonly known as '*Harkat-ul-Ansar'*, attempted to infiltrate military software for imposing illegal political objectives.[7] Moreover, in March 2000, a cult organization, known as '*AumShrinikyo'*, entered into a contract with hackers to secure access to computer programs/software of more than 10 government agencies for damaging stored data and to intrude into more than 80 Japanese corporations for wrongful financial gains.[8] Thus, the word 'hackers' or 'crackers' is defined in dictionaries based on hacker-type techniques employed or agendas targeted for accessing unauthorized information/data stored in internet devices. Amongst these hackers, the most notorious ones are 'cyber terrorists',[9] who threatens the vital infrastructure of computer systems used for military purposes or financial transactions. The second most dangerous category called 'hacktivist' means and includes persons employed to maliciously attack computer systems for achieving a particular activist's agenda or other related political objectives.[10] Consequently, cyber legislations of hostile nations are crying out for introducing reforms to pinpoint legal hindrances that are showing enforcement difficulties for safeguarding digital infrastructure. To illustrate the difficulties faced by developed yet hostile nations we could examine the short falls of The Computer Misuse Act, 1990 that is in force in the United Kingdom.[11] The origin of the Act can be found under the Law Commission Report on computer misuse.[12] The Computer Misuse Act, 1990 was drafted to safeguard computer systems from cyber criminals, who misbehave to break into computer systems owned by individuals, business organizations and government entities for making money. The offences covered under the Act include 'unauthorized access to computer material', 'unauthorized access with intent to commit or facilitate commission of further offence' and 'unauthorized modification of computer material'.[13] Though The Computer Misuse Act, 1990 specifically highlights criminal offences related to unlawful access to computer programs under various provisions, nonetheless, the law enforcement agencies showed its inefficiency to catch cyber offenders for causing a computer to perform unauthorized/illegal function.

In *R. vs. Sean Cropp*,[14] problems related to inappropriate interpretation of the law emerged since special knowledge of computer programs is essentially required for the judges to adjudicate hacking instances. It is pertinent to note that offences involving illegal access to computer programs have been discounted by the Council of Europe Convention to exclude instances of physically accessing a stand-alone computer without the use of another computer system. As a result, the defendant in this case was acquitted by the court as the facts of the matter established that offence was committed in a stand-alone computer and Section 1(1)(a) lay emphasis on the use of second computer for securing access to computer program or data. In other words, the court

[5] (1987) WLR 803; (1988) 2 All ER 186 (CA).
[6] Ian Walden, Chap 9 "Computer Crime" in Chris Reed & John Angel (Eds.), Computer Law (5thEdn., Oxford University Press 2003) 299; available at https://openlibrary.org/books/OL3318064M/Computer_law, last accessed on 31st December 2023.
[7] Dorothy Denning, "Cyber Terrorism", 24-08-2000, available at https://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc; last accessed on 31st December 2023.
[8] Id.
[9] Clay Wilson, "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress" (CRS Report for Congress received through the CRS Web, 17-10-2003) CRS-4; https://www.semanticscholar.org/paper/Computer-Attack-and-Cyber-Terrorism%3A-and-Policy-for-Wilson/3c1827fda019d32629049707a569b24164c92f06; last accessed on 31st December 2023; See also, Arun Srinivasan, "Combating Terrorism" (Institute for Security and Intelligence), available at https://www.afgen.com/terrorismlhtml; last accessed on 31st December 2023.
[10] Steven Furnell, Cybercrime: Vandalizing the Information Society (Addison-Wesley 2002) 44, available at https://www.semanticscholar.org/paper/Cybercrime%3A-Vandalizing-the-Information-Society-Furnell/705861aa64d6b6de0a681f8999a55874fbd48ebd; last accessed on 31st December 2023.
[11] Owen Bowcott, "Cybercrime Laws Need Urgent Reform to Protect UK", The Guardian Weekly, 2020, available at https://www.theguardian.com/technology/2020/jan/22/cybercrime-law-need-urgent-reform-to-protect-uk-says-report; last accessed on 31st December 2023.
[12] Law Commission Report No. 186, Computer Misuse (Cm 819) (HMSO, 1989); available at https://lawcom.gov.uk/project/criminal-law-computer-misuse/, last accessed on 31st December 2023.
[13] Section 1 and Section 2 of The Computer Misuse Act, 1990.
[14] Snares Book Crown Court, 04-07-1991.

misinterpreted the wordings used in the section and reached an incorrect conclusion that offence is committed only when one computer is used to obtain unauthorized access to data stored in another computer. In any event, interpretation given by the lower court was completely rejected by the Court of Appeals, who was of the opinion that plain and natural meaning to the wordings used in the section must be employed and that the interpretation given to the section by the lower court restricts the purpose and scope of the act. Moreover, unauthorized access to computer programs or data held in computers is not limited to hacking instances of outsiders but also involves commission of offences by insiders or employees working within the business organizations.[15] Consequently, 'Hackers', who were respected for their programming or computing skills[16] are no longer depicted as software experts capable of implementing advance solutions to complex technological issues but are now perceived as obsessive people who voluntarily disrupts the integrity of computer systems jeopardizing sensitive information or data belonging to individuals, business organizations and government through their criminal misconduct.[17]

B. United States of America

Increasing reliance on digital technology has led to tightening the legislative noose on unauthorized access to programs or data held in internet devices. Emerging cyber security breaches demands complacent legal regimes to implement cyber specific legislations for identifying computer vulnerabilities and to safeguard individuals, business organizations and government from criminal misconducts in cyber space. In United States, the Computer Fraud and Abuse Act, 1986 was implemented as a response mechanism to regulate illicit computer activities including unauthorized access, breach of sensitive information, stealing of financial records and other unlawful activities on the internet.

Amongst other wrongful things, criminal conduct involving theft of passwords especially used by United States Government for defense services is specifically barred under 18 USC S. 1030(a)(6). The magnitude of hacking activities in United State is highly severe as compared to any other States in the world. For instance, in 2000, a teenage boy known amongst hackers as '*Mafiaboy*', a resident from Canada, assaulted the entire world wide web by creating Denial of Service (DOS) attacks directed towards well-know websites such as Yahoo.com, Buy.com, eBay.com, CNN.com and Amaon.com, E*TRADE Financial that resulted into loss of millions of dollars in revenue since it denied the internet users of the above-mentioned websites to enter company's home page and conduct business at the market place.[18] It is pertinent to note that unlike United Kingdom's Computer Misuse Act, 1990, the United States' Computer Fraud and Abuse Act, 1986 defines computer since unauthorized access to computer resources is not possible without the use of computer. On the other hand, the definition of 'computer' in India is broader in its scope as it includes words such as computer system and computer programs.

C. India

In India, the Information Technology Act, 2000 (IT Act, 2000) prohibits the breach of security to alter computer system especially when the offence is committed with 'dishonest' or 'fraudulent' intention.[19] Evidently, the IT Act, 2000 lays emphasis on the effect and magnitude of the injury suffered by the computer resource. Under the IT Act, 2000, the specific use of words such as 'unauthorized access' is missing. In any event, the phrase "if any person without permission of the owner […] in charge of a computer" must be exuviated with "unauthorized access", which is found under relevant statutory provisions under computer crimes in United Kingdom and United States. For instance, in 2001, a notorious hackers group from Pakistan commonly known as G-Force breached the security of the computer systems owned by Indian Science Congress, National Research Centre Indian National Information Technical Promotion (New Delhi), IIT (Chennai), IIM (Ahmedabad) Asian Age Newspaper, Agricultural University of Maharashtra, to alter/steal/destroy the sensitive data/information stored in computer resources.

[15] Audit Commission Report, "Ghost in the Machine: An Analysis of Fraud & Abuse (1998)"; available at https://www.goodreads.com/book/show/4650532-a-ghost-in-the-machine, last accessed on 1st January 2024.
[16] Steven Furnell, Cybercrime: Vandalizing the Information Society (Addison-Wesley 2002) 44; available at https://link.springer.com/content/pdf/10.1007/3-540-45068-8_2.pdf, last accessed on 1st January 2024; See also, Steven Levy, Hackers: Heroes of the Computer Revolution; available at https://www.goodreads.com/book/show/56829.Hackers, last accessed on 1st January 2024.
[17] R. vs. Strickland, 1996 Can LII 5566 (NS CA); R. vs. Woods, Southwark Crown Court, March 1993.
[18] "Hack Attack" August 2003 Reader's Digest, 85.
[19] Section 66 and Section 43; See also, Section 24 of the Indian Penal Code, 1860.

One of the most shocking intrusions of cyber security in India was managed by an American boy, who was merely 15-years of age, popularly known as "*t3k-9*". The boy hacked into the computer network of Bhabha Atomic Research Centre (BARC) immediately after the nuclear test that was successfully conducted at Pokhran in May 1998. It is worthy to note that the boy not only hacked into the computer network but shared login and password details of more than 800 BARC employees to hacker channels including "*Iron Logik*", which was owned by an 18-year old immigrant from Serbia. Furthermore, in 1998, a hacker group known as "*Armageddon*" unlawfully accessed sensitive data regarding internal memos and test results stored at Indian Bio-Medical Research Facility making the computer resource vulnerable to cyber menace.[20] Consequently, cyber security threats are becoming serious and the difficulty to bring the culprits into legal scrutiny becomes challenging since burden to prove elements of *actusreus* and *mens rea* to impose liabilities or penalty for computer-related offences on notorious hackers is not just grueling but strenuous due to jurisdictional legal issues.

3. Conclusion

As far as computer crimes are concerned, the difference in the legal attitude of United Kingdom, United States and India is based on pragmatic approach towards: (i) means employed for obtaining accessibility to computer program or data with intent to commit further offence to identify possible injury; (ii) reckless manipulations done to computer resource with an intent to damage or diminish the value, integrity or utility of the sensitive information stored in the computer systems or network; and (iii) classifying elements of dishonesty and fraud for wrongful gain and wrongful loss including the magnitude of damage; to individuals, business organizations and government respectively. In any event, the concept of authorization or unauthorized access to data needs refinement since lack of 'due care and appropriate measures' would most likely fail to establish the culpability of the accused. The accused in such circumstances gets a point of defense for cyber security breaches or unauthorized access to sensitive information or data stored on computer. Furthermore, most hackers use defense of curiosity, in other words, when hackers are charged with computer-related offences, defensive contentions are often made before the law courts to attract the attention of law courts towards absence of mental element i.e. *mens rea* required for establishing commission of cyber crime under relevant provisions.

The true intent of hackers behind intrusions or gaining unauthorized access to sensitive information stored in computer resources becomes challenging especially if these intrusions either portrays no harm or evidentiary proof of lack of altering/destroying computer programs and software. Under such circumstances, hacking activities are apparently perceived as harmless, however, mere presence or traces of an external computer device, which is not authorized to be at that cyber space must be distinguished as 'computer hacking havoc' to create chaos. Therefore, it is highly recommended to book hackers for cyber crimes and security breaches by imputing the concept of strict liability under relevant provisions related to computer laws and internet regimes.

References

[1] Selma Dilek, HuseyinCakir and Mustafa Aydin, "Application of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review" (Jan. 2015) 6(I) International Journal of Artificial Intelligence & Applications, https://arxiv.org/abs/1502.03552.

[2] Michael Crosby et al., "Blockchain Technology: Beyond Bitcoin" (2016) 2 Applied Innovation Review 8, https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf.

[3] "UN Cybersecurity Challenges: Countering Digital Terrorism", United Nations – Office of Information and Communications Technology, 2019, https://ideas.unite.un.org/counterdigiterrorism/Page/Home.

[4] Ian Walden, "Computer Crime" in Chris Reed & John Angel (Eds.), Computer Law (3rdEdn. Oxford University Press) 277, https://archive.org/details/computercrimesdi0000wald.

[5] D.S. Wall, "Policing and Regulation of Cyberspace" in Crime, Criminal Justice and the Internet (Special Edn. Crim L Rev, Sweet & Maxwell, London 1998) 79-91, https://www.routledge.com/Cyberspace-Crime/wall/p/book/9781138709010.

[20] Dr. R.K. Tewari, P.K. Sastry& K.V. Ravikumar, Computer Crime and Computer Forensics (Select Publishers 2002) 301-308; available at https://library.niti.gov.in/cgi-bin/koha/opac-detail.pl?biblionumber=64302, last accessed on 2nd January 2024.

[6] S.K. Verma& Raman Mittal (Eds.), Legal Dimensions of Cyberspace (Indian Law Institute, New Delhi 2004) 229, https://openlibrary.org/books/OL22538494M/Legal_dimensions_of_cyberspace.
[7] Ian Walden, Chap 9 "Computer Crime" in Chris Reed & John Angel (Eds.), Computer Law (5thEdn., Oxford University Press 2003) 299, https://openlibrary.org/books/OL3318064M/Computer_law.
[8] Dorothy Denning, "Cyber Terrorism", 24-08-2000, https://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc.
[9] Clay Wilson, "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress" (CRS Report for Congress received through the CRS Web, 17-10-2003) CRS-4, https://www.semanticscholar.org/paper/Computer-Attack-and-Cyber-Terrorism%3A-and-Policy-for-Wilson/3c1827fda019d32629049707a569b24164c92f06.
[10] Arun Srinivasan, "Combating Terrorism" (Institute for Security and Intelligence), https://www.afgen.com/terrorismIhtml.
[11] Steven Furnell, Cybercrime: Vandalizing the Information Society (Addison-Wesley 2002) 44, https://www.semanticscholar.org/paper/Cybercrime%3A-Vandalizing-the-Information-Society-Furnell/705861aa64d6b6de0a681f8999a55874fbd48ebd.
[12] Owen Bowcott, "Cybercrime Laws Need Urgent Reform to Protect UK", The Guardian Weekly, 2020, https://www.theguardian.com/technology/2020/jan/22/cybercrime-law-need-urgent-reform-to-protect-uk-says-report.
[13] Law Commission Report No. 186, Computer Misuse (Cm 819) (HMSO, 1989), https://lawcom.gov.uk/project/criminal-law-computer-misuse/.
[14] Audit Commission Report, "Ghost in the Machine: An Analysis of Fraud & Abuse (1998)", https://www.goodreads.com/book/show/4650532-a-ghost-in-the-machine.
[15] Steven Furnell, Cybercrime: Vandalizing the Information Society (Addison-Wesley 2002) 44, https://link.springer.com/content/pdf/10.1007/3-540-45068-8_2.pdf.
[16] Steven Levy, Hackers: Heroes of the Computer Revolution, https://www.goodreads.com/book/show/56829.Hackers.
[17] Dr. R.K. Tewari, P.K. Sastry& K.V. Ravikumar, Computer Crime and Computer Forensics (Select Publishers 2002) 301-308, https://library.niti.gov.in/cgi-bin/koha/opac-detail.pl?biblionumber=64302.