iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** II **Month of publication:** February 2018

DOI: http://doi.org/10.22214/ijraset.2018.2084

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

A Study on Cybercrime in Jammu & Kashmir

Abhishek Gupta[1], Dr. Jatinder Singh Manhas[2]
[1]P.hd Scholar Aisect University Bhopal,[2] Sr. Asstt. Professor University Of Jammu

Abstract: Cybercrime is also called as dependent crimes (or 'pure' cyber crimes) are offences that can only be committed using a computer, computer networks or other form of information communications technology (ICT). These acts include the spread of viruses or other malware, hacking and distributed denial of service (DDoS) attacks. The aim of this research paper to discuss following aspects of Cybercrimes: the definition, methods of committing cybercrimes, and cybercrime prevention procedures. More specifically, this paper will describe the one main example of cybercrime i.e "hacking". In this paper we will describe how the cybercrime in Jammu and Kashmir spread very fast.
Keywords: Cybercrime, Hacking, Virus, Security, Terrorist .

I. INTRODUCTION

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime. The "cyber" environment includes all forms of digital events, regardless of whether they are conducted through networks and without borders. Computer oriented crime, is crime that involves a computer and a network.[1] The computer may have been used in the commission of a crime, or it may be the target.[2] Cyber crimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".[3] Cybercrime may threaten a person or a nation's security and financial health.[4] Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones".[3] Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare.

II. CLASSIFICATION OF CYBER CRIMES

Computer crime encompasses a broad range of activities.[4]

A. Fraud and financial crimes

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

1) Altering in an unauthorized way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;
2) Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect;
3) Altering or deleting stored data;

B. Cyber Terrorism

Cyber terrorism in general can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda piece in the Internet that there will be bomb attacks during the holidays can be considered cyber terrorism. There are also hacking activities directed towards individuals, families, organized by groups within

networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc [5].

Other forms of fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information.

A variety of internet scams, many based on phishing and social engineering, target consumers and businesses

C. Cyber-Extortion

Cyber-extortion can come in many different forms, but at its simplest, it is when someone online threatens some sort of harm unless you meet their demands. The demand is usually for money (commonly in the form of bitcoins), but an extortionist could conceivably demand just about anything. Cyber extortion has different categories. One of the categories is using data as the new "hostage". Holding data hostage can be as simple as stealing the most recent backup and wiping the original version from the server, or it may be as complex as changing the encryption key within a database and holding the new key hostage. The data is then held "hostage" while the company is put into a limbo while negotiating with the cyber extortionist.

D. Cyber-Warfare

1) *Cyber-warfare* : involves the battle space use and targeting of computers and networks in warfare. It involves both offensive and defensive operations pertaining to the threat of cyber attacks, espionage and sabotage. There has been controversy over whether such operations can duly be called "war". Nevertheless, nations have been developing their capabilities and engaged in cyber warfare either as an aggressor, defendant, or both. Cyber warfare can present a multitude of threats towards a nation. At the most basic level, cyber attacks can be used to support traditional warfare. For example, tampering with the operation of air defences via cyber means in order to facilitate an air attack[6]. Aside from these "hard" threats, cyber warfare can also contribute towards "soft" threats such as espionage and propaganda.

E. Computer as Target

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have—which explains how unprepared society and the world in general is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet:Crimes that primarily target computer networks or devices include:

Computer viruses

Denial-of-service attacks

Malware (malicious code)

F. Denial of Service Attack (DoS attack)

In computing, a denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DDoS attack is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations. Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Revenge, blackmail[2][3][4] and activism[5] can motivate these attacks.

III.GROWTH RATE OF CYBER CRIME IN JAMMU AND KASHMIR FROM LAST 3 YEARS:[7]

The cyber crime in Jammu and Kashmir is witnessing a sudden surge with as many as 51 such cases recorded in the state during the year 2017.The official figures reveal that in the year 2017, 51 cases of cyber related crimes have been witnessed in Jammu and Kashmir while as 48 such cases are under the investigation. According to the figures, in the year 2015, there were 38 cases related to the cyber crime recorded in the state while as in the year 2016, the number of such cases was 25. However, cyber crimes witnessed a

sudden spike in the year 2017 when no less than 51 cases have been registered by the police in Jammu and Kashmir. A proposal for notifying Cyber Crime Police Stations along with creation of manpower is at present under consideration in consultation of the Finance Department of the state and the government on floor of the house recently claimed that all the Police Stations have been provided with latest IT Gadgets/technologies to handle Cyber Crimes effectively. The government have stated that to tackle the cyber crimes in the State, three Cyber Crime Police Cells one each at Jammu, Srinagar and Crime Headquarters, have been established and that sufficient number of trained officers and staff has been deployed at Cyber Police Cells to investigate and monitor all crimes related to cyber offences.

IV. CYBER ATTACK BY HACKER IN J&K

[8] On June 05 2017 ,a day after Pakistan's defeat in the ICC Champions Trophy against India, a hackers group from Pakistan called Pak Cyber Skullz hacked the website of the National Institute of Technology (NIT) Srinagar on Monday. The institute has launched a new website and the old link of the old website has been hacked. A message demanding “freedom for Kashmir” has been put up. The website was hacked at around 3:30 pm on Monday. The hackers have put “GO MODI GO” message and said, “Do you know why you got hacked? Free Kashmir. Freedom is our goal. ”Calling Kashmir “militarised governance” the hackers have said that they (Kashmiris) just want “freedom from evils of the Indian Army.” “Stop killing children, raping women and imprisoning the men. Every day 100s of innocent people are abused raped and even killed in Kashmir by the Indian Army, a third of the deaths are children. We don’t want war, take back your men, your guns and go back where you came from,” the hacked website reads. The students of NIT believe that the website was hacked in the frustration of the ICC Champions Trophy defeat to India.

V. HOW TO PREVENT FROM CYBER CRIME

A. Cyber Forensics can be use to detect cyber Evidence.
B. To make necessary amendments in Indian laws to control on Cyber Crimes.
C. There is strong need to harmonize some sections of IT act 2000 to curb cyber crimes and Individuals to prevent cyber stalking avoid disclosing any information pertaining to one. This is as good as disclosing your identity to strangers in public place .
D. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
E. Always use latest and up date anti virus software to guard against virus attacks.
F. Always keep back up volumes so that one may not suffer data loss in case of virus contamination.
G. Never send your credit card number to any site that is not secured, to guard against frauds.
H. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
I. It is better to use a security programmed that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
J. Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
K. Web servers running public sites must be physically separate protected from internal corporate network.

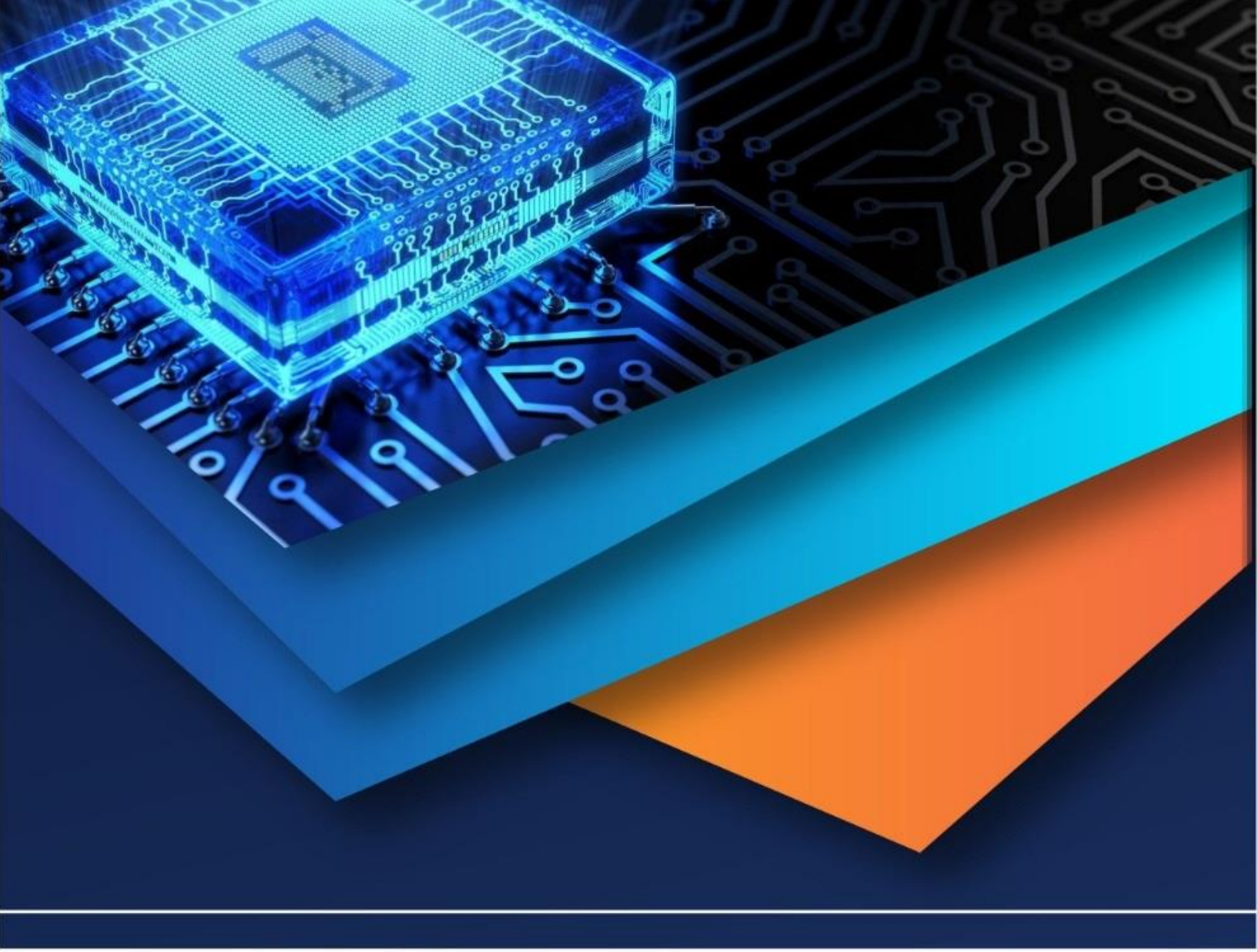
IV. CONCLUSIONS

Though not all people are victims to cyber crimes, they are still at risk. Crimes by computer vary, and they don’t always occur behind the computer, but they executed by computer. The hacker’s identity is ranged between 12 years young to 67years old. The hacker could live three continents away from its victim, and they wouldn’t even know they were being hacked. Crimes done behind the computer are the 21st century’s problem. With the technology increasing, criminals don’t have to rob banks, nor do they have to be outside in order to commit any crime. They have everything they need on their lap. Their weapons aren’t guns anymore; they attack with mouse cursors and passwords. It can be seen that the threat of computer crime is not as big as the authority claim. This means that the method s that they introducing to combat it represents an unwarranted attack on human rights and is not proportionate to the threat posed by cyber-criminals. Part of the problem is that there are no reliable statistics on the problem; this means that it is hard to justify the increased powers that the Regulation of Investigatory Powers Act has given to the authorities. These powers will also be ineffective in dealing with the problem of computer. The international treaties being drawn up to deal with it are so vague that they are bound to be ineffective in dealing with the problem. It will also mean the civil liberties will be unjustly affected by the terms of the treaties since they could, conceivably, imply that everybody who owns a computer fitted with a modem could be suspected of being a hacker. The attempts to outlaw the possession of hacking software could harm people who

trying to make the internet more secure as they will not be able to test there systems; therefore the legislation could do more harm than good.

REFERENCES

[1] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
[2] Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.
[3] Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN
[4] Gordon, Sarah (July 25, 2006). "On the definition and classification of cybercrime" (PDF). Retrieved January 14, 2018
[5] "Cybercriminals Need Shopping Money in 2017, Too! - SentinelOne". sentinelone.com. Retrieved 2017-03-24
[6] "Critical infrastructure vulnerable to attack, warned cyber security expert". gsnmagazine.com. Government Security News. 2014. Retrieved 6 June 2015
[7] http://www.knskashmir.com/Cyber-Crimes-witness-surge-in-JK--51-cases-registered-in-2017-alone-23017.
[8] http://www.tribuneindia.com/news/jammu-kashmir/pak-based-group-hacks-nit-srinagar-website/417853.html.
[9] "Understanding Denial-of-Service Attacks". US-CERT. 6 February 2013. Retrieved 26 May 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY