Journal of Advances and Scholarly Researches in Allied Education
Vol. XIV, Issue No. 2, January-2018, ISSN 2230-7540

The Cyber Crime and Security Scenario in India

Navpreet Kaur[1]* Yogesh Sharma[2]

[1]Research Scholar, Computer Science, JJT University, Jhunjhunu, Rajasthan

[2]Associate Professor, Computer Science, JJT University, Jhunjhunu, Rajasthan

Abstract – Cybercrime is a borderless issue, comprising of criminal acts that are perpetrated online by utilizing electronic interchanges systems and information frameworks -, for example, crimes particular to the Internet, online extortion and imitation and illicit online substance. While the estimation of the cybercriminal economy all in all isn't exactly known, the misfortunes are thought to speak to billions of Euros for every year. The size of the issue is itself a danger to law authorization reaction ability. These dangers can have distinctive starting points - including criminal, politically propelled, psychological oppressor or state-supported assaults and additionally catastrophic events and unexpected oversights. Cybercrime is expanding in scale and effect, yet there is an absence of dependable figures. Be that as it may, patterns recommend significant increments in scope, complexity number and kinds of assaults, number of casualties and monetary harm. Digital security occurrences, purposeful or coincidental, are expanding at a disturbing pace. This examination breaks down present issues &technical challenges for examination and avoidance of Cybercrimes in India.

Keywords: Cybercrimes, Digital Security, Internet

----------X----------

1. INTRODUCTION

Cyber-crime is a prudence having its beginning in the developing dependence on information technology. In this modern innovative world where computer run technologies and large progressively utilized as a part of different activities running from basic entryway security framework to atomic power plants, Cybercrimes has guaranteed rather low implications. Cybercrimes can be divided into three noteworthy categories cybercrimes against people, property and government. The parliament of India passed the Information Technology (IT) Act in 2000. It not just gives the legal foundation to E-Commerce in India yet additionally in the meantime, gives draconian forces to the police to enter and seek with no warrant in any open place to nab digital hoodlums and averting Cybercrimes.

Cybercrimes is not quite the same as Conventional crime ("a legal wrong that can be trailed by criminal procedures which may come about into punishment."

(1) Cyber-crime is the most recent and maybe the most muddled issue in the digital world. It is characterized as "Any criminal action that uses a PC either as an instrumentality, target or a methods for propagating further crimes comes surprisingly close to Cybercrimes"

(2) A summed up meaning of Cybercrimes might be "illegal acts wherein the PC is either a device or target or both"

(3) Cybercrime is additionally generously unique in relation to PC crime. It resembles the contrast between individuals who utilize PCs for everything they can be versus individuals who utilize PCs.

Cybercrimes is difficult to distinguish, along these lines giving the culprits a lot of time to escape the zone in which the crime was carried out, as a result of this reality the hoodlum can be in another nation far from the scene of the crime when it is recognized. PC is a noteworthy hotspot for Cybercrimes. Cybercrimes is any illicit movement emerging from at least one Internet parts. Cybercrime can incorporate everything from non-conveyance of products or administrations and PC interruptions to licensed technology rights manhandle financial reconnaissance, online blackmail, worldwide illegal tax avoidance, and a developing rundown of other Internet-encouraged offenses. Further, it is difficult to recognize promptly about the crime technique utilized, and to answer questions like where and when it was finished.

Digital violations—destructive acts perpetrated from or against a PC or system—contrast from most earthly crimes .They are anything but difficult to

figure out how to confer; they require couple of assets in respect to the potential harm caused; they can be conferred in a locale without being physically present in it; and they are frequently not unmistakably illicit. Existing earthbound laws against physical demonstrations of trespass or breaking and entering regularly don't cover their "virtual" partners. Website pages, for example, the web based business locales as of late hit by broad, circulated foreswearing of administration attacks4 may not be secured by obsolete laws as ensured types of property.

Cyber Crime - Cyber Crime comes in many structures and from numerous points of view. Beneath specified are the distinctive sorts of Cyber-crime:

1) Communications in Furtherance of Criminal Conspiracies Just as real associations utilize the information systems for record keeping and correspondence, so too are the activities of criminal associations improved by the appearance of information technology. There is proof of information frameworks being utilized as a part of medication trafficking, betting, tax evasion and weapons exchange just to give some examples.

2) Telecommunications Piracy Digital technology grants consummate propagation and simple dispersal of print, designs, sound, and interactive media mixes. This has delivered the impulse to imitate copyrighted material either for individual utilize or available to be purchased at a lower cost.

3) Electronic Money Laundering For some time now electronic assets moves have helped with hiding and moving the returns of crime. Rising advances make it less demanding to conceal the inception and goal of assets exchange. In this way illegal tax avoidance goes to the front room.

4) Electronic Vandalism and Terrorism All social orders in which PCs assume a noteworthy part in regular day to day existence are powerless against assault from individuals inspired by either interest or malignance. These individuals can cause burden, best case scenario and can possibly incur gigantic damage.

5) Sales and Investment Fraud As electronic trade or online business as it is called turns out to be increasingly prominent; the use of advanced technology to fake crime will turn into that significantly more noteworthy.

6) Illegal Interception of Information Developments in broadcast communications and information exchange over the net has brought about more prominent speed and limit yet additionally more noteworthy helplessness. It is presently less demanding than at any other time for unapproved individuals to access delicate data.

7) Cyber Pornography Spread of Child smut and sexually understood material.

8) Information Piracy and Forgery Digital technology licenses consummate propagation of the first records, cases are birth authentications, international ID, false personality, falsifying of cash, debatable instruments and so forth.

9) Hacking Information robbery from PCs hard circle, expulsion stockpiling and so on. Information robbery, information devastate, taking and changing data.

10) Internet time robberies by taking client name and watchword, hoodlums use for themselves and take the web time designated to the buyer.

11) Hate/Communal Crimes As building a site page isn't costly and compasses to billions of individuals, hoodlums spread detest or common information or gossipy tidbits, by building a site and furthermore enrolls individuals for their operation through promotion.

12) Altering Websites The programmer erases a few pages of a site, transfers new pages with the comparable name and controls the messages passed on by the site.

Cybercrime must be viably countered when there is an appropriate coordination and direction accessible for different partners, for example, occupants of a country, ventures and additionally the neighborhood, state and local governments. To encourage such collaboration and additionally to give driving force and to represent the viable usage of different activities, we need sufficiently entrusted and staffed organizations working at different levels. In India, the administration had set up an Inter Departmental Information Security Task Force (ISTF) with the National Security Council as the nodal organization to facilitate all issues related with compelling usage of its digital security technique. Indian Computer Emergency Response Team (CERT-In) is the national nodal office set up to react to PC security episodes as and when they happen. A portion of the activities attempted by CERT-In toward digital security incorporate coordination of reactions to security occurrences and major

events3 issuance of warnings and convenient counsel with respect to unavoidable dangers item vulnerabilities examination direct trainings on specific themes of digital security and improvement of security rules on real technology stages. Another significant activity is by methods for the formation of specific groups at various departmental levels, for example,

- National Cyber Coordination Center (NCCC)
- National Critical Information Infrastructure Protection Center (NCIIPC)
- Grid Security Expert System (GSES)
- National Counter Terrorism Center (NCTC)
- Cyber Command for Armed Forces
- Central Monitoring System (CMS)
- National Intelligence lattice (NATGRID)
- Network and Traffic Analysis System (NETRA)

2. REVIEW OF LITERATURE:

In the present setting, utilization of PCs is known to a substantial level of populaces. Yet, backpedaling to 1960s their utilization was not normal. Just chose parts of the populace approach these cumbersome machines. —IBM's presentation of its stand – alone 'PCs' in 1981, PCs starts to go into the life of the people, Today it is assessed that 53.7 million family units have PCs. With the quick scale advancement and change in the technology an ever increasing number of people start to utilize PCs as a medium both for constructive and antagonistic reason. This prompted the advancement of PC crimes on a huge scale.

Year 1820 was the benchmark in the PC crime wherein the principal such crime occurred. In 1820, Joseph-Marie Jacquard, a material plant proprietor in France, delivered the linger. This assistance gadget permitted the redundancy of a progression of ventures in the weaving of uncommon textures. As an outcome, there was fear among the Jacquard's workers that their conventional business and vocation were being undermined. They submitted the demonstrations of treachery to demoralize Jacquard from additionally utilization of the new technology. This is the principal recorded Cybercrime.

Digital Crime:

A General meaning of Cybercrimes might be —unlegal act wherein the buyer is utilized, either as a device or an objective or both. Any criminal movement that uses a PC either as an instrumentality, target or a method for sustaining further crimes comes surprisingly close to Cybercrimes s.

The Internet is quick changing the way of life of each individual whether be it understudies, businesspeople, specialists, legal advisors, engineers, and so on it is turning into a lifestyle for many individuals. With this, the crooks are likewise not falling behind. Their territory of operation has additionally broadened with such innovative advance.

There are challenges in giving a portrayal of cybercrimes, as there is no uniform or all around acknowledged meaning of cybercrime. It is utilized as an umbrella term for an arrangement of activities that still can't seem to be fused completely into the national legitimate administrations around the globe and is utilized conversely with —computer crimes‖, —computer misuse‖, or —IT violations, regardless of the successive utilization of the term, there is no regularly acknowledged definition. Cybercrimes is identified with PCs, be that as it may, there is no accord on whether those PCs must be interconnected or not.

a. The UN Manual on the Prevention and Control of Computer-Related Crimes:

—Computer crime can include activities that are conventional in nature, for example, robbery, misrepresentation, falsification and underhandedness, which are all for the most part subject wherever to criminal approvals. The PC has likewise made a large group of conceivably new abuses or misuse that may, or ought to be criminal as well‖

b. UK National Criminal Intelligence Service:

—An offense in which a PC is specifically and essentially instrumental in the commission of the crime

c. Pavan Duggal

Digital Crime alludes to every one of the activities finished with criminal plan in the internet or utilizing the medium of web. These could either the criminal activities in the customary sense or activities, recently advanced with the development of the new medium. Any action, which fundamentally annoys human sensibilities, can be incorporated into the ambit of cybercrimes.

Contrast between Cyber Crime and Conventional Crime

1. Cyber-crimes dependably include utilization of PCs and technology.

2. Cyber-crimes can be carried out in the ward without the criminal being physically present in it, i.e. it knows no topographical constraints, limits or separations.

3. Cyber-crimes isn't generally plainly illicit when contrasted with traditional violations. This is a direct result of absence of law rebuffing them.

4. It requires just little assets when contrasted with the resultant harm caused by the commission of the crime.

Sorts of Cyber Crimes

1. **Hacking: -** Hacking implies unapproved access to a PC framework. As characterized in Section 66 of the Information Technology Act, 2000, hacking is ―whoever with the expectation to cause or realizing that he is probably going to make wrongful misfortune or harm the general population or any individual pulverizes or erases or adjusts any information dwelling in a PC asset or lessens its esteem or utility or influences it damagingly by implies confers hacking

2. **Virus, Trojans and Worms: -** A Computer infection is a program intended to influence the soundness of the PC. They pulverize or hampers the PC frameworks. Trojan is characterized as a ―maliciously, security breaking program that is veiled as something benign‖, for example, a catalog lister, chronicle, amusement, or a program to discover and crush infections.

3. **Cyber Pornography: -** Cyber obscenity is smut's which is disseminated through the web, basically sites, distributed document sharing or Usenet newsgroups. This is a crime that is unmistakably unlegal, both on and off the web

4. **Cyber Stalking: -** Cyber Stalking is characterized as the rehashed demonstrations of badgering or undermining conduct of the cybercriminal towards the casualties by utilizing web administrations.

5. **Cyber Terrorism: -** Cyber psychological oppression might be characterized to be ― the planned utilization of troublesome activities, or the danger thereof, in the internet, with the expectation to encourage social, ideological, religious, political or comparative goals, or to imply any individual in assistance of such targets

6. **Cyber Crimes identified with Finance: -** Crimes over web for procuring money related or fiscal increase careful unlegal means. It might happen in many structures, yet the most perceived strategy is online extortion and ridiculing. This would incorporate swindling, Visa cheats, illegal tax avoidance, and so on.

7. **With versatile and Wireless Technology: -** because of the advancement in portable and remote technology, much work can be completed on mobiles telephones, which was prior conceivable just on PCs. Rise of versatile cash, phone saving money, and so on has raised the danger of crimes submitted through this medium.

8. **Information Diddling: -** This sort of an assault includes modifying the crude information just before a PC forms it and after that transforming it back after the handling is finished.

9. **Internet time burglaries: -** This suggests the utilization by an unapproved individual of the web hours paid for by someone else. This sort of crime was unheard until the point that the casualty announced it.

10. **Logic bombs: -** this is an occasion subordinate program. This infers this program is made to accomplish something just when a specific occasion happens.

Statuary Provisions (Information Technology Act, 2000)

11. The initial phase in the field of digital law was the Model Law which was drafted under the United Nations Commissions on International Trade law, 1986. At that point, the United Nations general get together on 30th January, 1999 passed a determination to manage web based business through uniform arrangement of laws material to its part's nations.

Being a signatory to the determination, Parliament of India has a passed the Information Technology Act, 2000 on seventeenth may, 2000.

12. The introduction of the Act expresses that the goals of the demonstration is to authorize internet business and further change the Indian correctional Code, 1860, the India Evidence Act,182, the Banker's

Book Evidence Act, 1891and the Reserve Bank of India Act, 1934 to make good with this Act.

13. The Act comprises of 13 Chapters and oversees laws identifying with Electronic Contract, Electronic Record, Digital Signature and the utilization of the electronic records and mark in Government records. It additionally manages the activities of the Network Service Providers, Internet Service Providers (ISPs).

14. Punishments and Offenses:- The principle point of the demonstration is to authorize the advanced dialect so individuals can undoubtedly and without fear utilize the electronic gadgets for their own particular purposes like working together or for excitement. It endorses certain offenses and punishments to keep a beware of the Cybercrimes , the principle of them are:

Area 65: Tampering with Computer Source Documents

Area 66: Hacking with Computer System

Area 67: Publishing of disgusting information which is profane in electronic shape.

Area 70: rupture of secretly and security

Notwithstanding above, Section 77 of the Act expresses that "No punishment forced or seizure made under this Act might keep the inconvenience of some other punishment to which the individual influenced in this manner is at risk under some other law for now in constrain." which implies the common crimes can likewise be made as Criminal Act, as

- Computer Network Breaking and Hacking: - S. 66(2) of I.T. Act and S. 441 of IPC

- Child Pornography: - S. 67 of I.T. Act and S. 294 of IPC

Email-besieging: - S. 43(e) of I.T. Act and S. 425-441 read with S447 of IPC

- Password Sniffing: - S. 43(a), (g) of I.T. Act and S. 419 of IPC

Charge card Fraud: - I.T. Act and S. 443 (an) and (g) read with 426, 427 and 447 of IPC.

As per a Study by Internet Security Providers, Symantec Corp. Cyber-crimes and assaults cost Indian organizations Rs 58 lakh in income in 2009 and influenced more than 66% of Indian undertaking.

Denning (1999) other than this, nonappearance of any fused and made course out of the virtual condition furthermore speaks to the most concerning issue. In the year 1999 Ethnic Tamil Gurillas overpowered Srilankan global places of refuge with lakhs of electronic mail messages.

The Economic Offenses Wing (EOW)(2006), Crime Branch, Delhi Police, revealed a significant phishing trap including fake messages and destinations of UTI Bank. An examination of the records of the four caught Nigerian nationals demonstrated cash related trades of over Rs 1 crore in an eight-month time period till December 2006. This shows the evaluated totals included. Examinations revealed that the trap is multi-layered with compartment India and worldwide traits. This trouble is clarified by a current report which uncovered that half of the offices associated with the investigation – 62 of 124 – didn't have formal PC crime units. Also, three-fourths of the organizations didn't have the apparatuses to distinguish and examine PC crimes, and almost 66% confronted staffing and preparing issues.

3. PRESENT SCENARIO OF CYBERCRIME IN INDIA AND ITS PREVENTIONS

Cybercrime is the most recent and maybe the most muddled issue for the digital world. The Indian Law has not given any definition to the term 'cybercrime'. Truth be told, the Indian Penal Code does not utilize the term 'cybercrime' anytime even after its revision by the Information Technology (change) Act 2008, the Indian Cyber law. "Digital fear based oppression is the planned, politically inspired assault against data, PC frameworks, PC projects, and information which result in brutality against property, government and individuals on the loose." OR "Acts those are deserving of the Information Technology Act". In India Information Technology Act, 2000 manages the cybercrime problems.it covers following zones—business exchanges on the web, utilize advanced marks characterized different cybercrimes, electronic trade.
sourcehttp://deity.gov.in/destinations/upload_files/dit/documents/downloads/ita ct2000/itbill2000.pdf

Following are the couple of cases of cybercrime:

Email shelling: this is a genuine crime in which a man sends a quantity of messages to the inbox of the objective framework/individual. Mail bombs will more often than not fill the dispensed space on an email server for the clients email and can bring about slamming the email server.

Hacking: among the wide range of cybercrime it is the most unsafe and serous string to the web and

internet business. Hacking just alludes to the breaking into the PC framework and takes profitable information (information) from the framework with no consent. Hacking is finished by programmers now the inquiry emerges who are programmers; programmers are in b/w customer and server and ready to parody the information/data. Duplication the IP address unequally.

Spreading PC infection: It is an arrangement of direction which can play out some noxious operations. Infections stop the typical capacity of the framework projects and furthermore to the entire PC framework. They can likewise demolish/botch up your framework and render it unusable without reinstallation of the working framework A PC infections can be spread through—Emails, Cds, Pendrives (optional storage),Multimedia, Internet.

Phishing: phishing just alludes to take information like passwords, Visa points of interest; usernames and so on finished the web. Phishing is ordinarily completed by email satirizing and texting. In this sort of crime programmers make an immediate connection which coordinates to the phony page/site which looks and feel like indistinguishable to the true blue one.

Wholesale fraud: It just alludes to misrepresentation or cheat others by make their wrong personality of others. It includes taking cash or getting different advantages by putting on a show to another person Information Technology (Amendment)Act, 2008, crime of wholesale fraud under Section 66-C.Whoever, falsely or insincerely make utilization of the electronic mark, watchword or some other special recognizable proof component of some other individual, known as information fraud For which criminal should be rebuffed with detainment of either depiction for a term which may reach out to three years and might likewise be at risk to fine which may stretch out to rupees one lakh. Source-https://cybercrimelawyer.wordpress.com/classification/66c-punishment for-wholesale fraud/Internet extortion: Internet misrepresentation can happen in visit rooms, email, message sheets or on sites. In web extortion criminal can send counterfeit information to the casualty in cases like internet acquiring, land, pay BAL, Work-at-home gift handling and so on.

Malevolent Software: These are Internet-based programming or projects that are utilized to disturb a system. The product is utilized to access a framework to take touchy information or information or making harm programming present in the framework.

Digital fighting: It is Internet-based clash including politically roused assaults on information frameworks. Digital fighting assaults can incapacitate official sites and organizes, upset or impair basic administrations, take or change arranged information, and disabled person monetary frameworks - among numerous different conceivable outcomes.

Area commandeering: It is the demonstration of changing the enrollment of a space name without the authorization of its unique registrant.

SMS Spoofing: SMS Spoofing permits changing the name or number instant messages seem to originate from. IJSER

Voice Phishing: The term is a mix of "voice" and phishing. Voice phishing is use to obtain entrance of private, individual and money related information from general society. Voice phishing utilizes a landline phone call to get data.

Digital trafficking: It might movement in weapons, drugs, individuals, which influence the extensive quantities of people.

4. CYBER SECURITY: CASE OF CYBER CRIME

Remain Safe! Today the greatest test for you is to remain refreshed with late technology and still shield yourself from the expanding digital danger. Here are the genuine stories; these stories will influence you to rethink your sentiment of online security.

Upwards of 11,592 instances of cybercrime were accounted for crosswise over India in 2015, almost 26 times over 10 years back, when 453 cases were accounted for in 2006, as per information discharged by the National Crime Records Bureau.

Online Games: Blue Whale Challenge has become life threatening game

A risk that many children fall for, particularly young people, are those coming through visit rooms. Unknown visit rooms are well known among youngsters to make new companions, and converse with various types of individuals. In any case, this

modern bend to friends through correspondence accompanies grave dangers. Spooks take cover behind the namelessness statement of sites to regularly target kids, either to make sexual and lascivious remarks or even send wrong substance without their insight.

Blue Whale Challenge and other viral difficulties like the Choking Game and the Cinnamon Challenge are by all account not the only types of digital dangers out there. Digital tormenting can extend from only a discourteous remark on a web-based social networking presents on out and out trolling and badgering.

How to save yourself from such attacks?

Ransomeware attack locked computer system

A ransomware attack locked computer system, an encryption malware so powerful it is technologically impossible to break open.

The impact of ransomware was underlined by a study that **one in 5 business hit by ransomware are forced to close**. Despite this harsh reality, another study found that **almost two-thirds of US office workers were unaware of ransomware threat**, emphasising the need for cyber security awareness training.

What is Ransom ware and how to save you from such attacks?

Blackmailed using hacked account

Sometimes it's not your fault. The websites you use get hacked and your information is exposed. Your instinct will be to say: "but I don't have anything to hide!" Well, *that's not exactly true, is it?*

How to save yourself from such identity thefts?

412 million user accounts exposed in Friend Finder Networks hack

User details of more than 412 million accounts were exposed in a information breach at Friend Finder Networks that once again confirmed poor user information protection and poor password practices.

Some other breaches, including the Daily motion breach, which prompted calls for password alternatives.

How to set passwords:

Just one of many phishing examples, but this happened to a seasoned Internet user

Ananda is more than your customary Internet client. She works for a major audit site and has perused a lot of preventative stories about digital security occurrences. She knows and takes after some fundamental advances that can shield her from digital assaults, however regardless she succumbed to a standout amongst the most widely recognized tricks out there: a phishing email.

Subsequent to clicking a maverick connection in a phishing email, digital culprits figured out how to get hold of her record subtle elements. They called her bank and figured out how to remove £240 before her card was solidified. A frightful affair, particularly since Amanda knew something wasn't right the second she tapped the connection, yet by then it was simply past the point of no return.

CONCLUSION:

Society as on today is occurring increasingly subordinate upon technology and crime in light of electronic offenses will undoubtedly increment. Try of law making hardware of the country ought to be as per mile contrasted with the fraudsters, to keep the crimes most minimal. Consequently, it ought to be the industrious endeavors of rulers and administrators to guarantee that representing laws of technology contains each perspective and issues of Cybercrimes and further develop in ceaseless and solid way to keep steady vigil and check over the related violations.

At the point when Internet was produced, the establishing fathers of Internet scarcely had any slant that Internet could change itself into an all plaguing unrest which could be abused for criminal activities and which required control. Today, there are many irritating things occurring in the internet. Because of the mysterious idea of the Internet, it is conceivable to connect with into an assortment of criminal activities with exemption and individuals with insight have been horribly abusing this part of the Internet to sustain criminal activities in the internet.

REFERENCES:

Anderson, M., (2004). Spamming for dummies. The Register, 27 July, 2004. Retrieved from *http://www.theregister.co.uk/2004/07/27/spamming for dummies/*.

Association for Information Service Industries: International Branch. "International trends in measures against cybercrime and the establishment of information security." *JISA Bulletin* 63 (October 2001): pp. 77–90.

CSI Computer Crime and Security Survey. (2008). Retrieved May 25, 2009 from *http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf*

Deci, (E.L.) and Ryan, R.M.(1985). Intrinsic Motivation and Self- Determination in Human Behavior, Plenum Press.

Edwards, L., Code and the law: The next generation. Paper given at the LEFIS workshop

Ermert, M., (2004). Good spam: Bad spam. The Register, 5 February. Retrieved from *http://www.theregister.co.uk/content/55/35353.html.*

Foucault, M., Afterword (1983). The subject and power. In: H. Dreyfus and P. Rainbow (Eds.), Michel Foucault: Beyond Structuralism and Hermeneutics, 2nd ed., pp. 208–226 Chicago, IL: University of Chicago Press.

G. Wang, H. Chen, and H. Atabakhsh, (2004). "Automatically Detecting Deceptive Criminal Identities," *Comm. ACM*, Mar., pp. 70-76.

Garland, D. (2000). The culture of high crime societies: Some preconditions of recent "Law and Order" policies. *British Journal of Criminology*, 40(3), pp. 347–375

Gaudin, S., (2004). U.S. sending more than half of all spam. Internetnews.com, 1 July. Retrieved from http://www.internetnews.com/stats/article.php/337631.

Geer, D., (2004). The physics of digital law, Plenary Speech at the Digital Cops in a Virtual Environment Conference, Yale Law School, 26–28 March. *Information Society Project.*

Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2006). CSI/FBI Computer crime and security survey. Retrieved November 10, 2009 from *http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf*

Gray, P. Sallis, & MacDonell, S. (1997). "Software Forensics: Extending Authorship Analysis Techniques to Computer Programs," Proc. 3rd Biannual Conf. Int'l Assoc. Forensic Linguistics, Int'l Assoc. *Forensic Linguistics,* 1997, pp. 1-8.

Greenleaf, G., (1998). An endnote on regulating cyberspace: Architecture vs. law? *University of New South Wales Law Journal*, 21(2) (reproduced in D.S. Wall (Ed.), Cyberspace Crime, 89–120. Aldershot, UK: Ashgate/Dartmouth, 2003)

Haggerty, K. and R. Ericson, (2000). The surveillant assemblage. *British Journal of Sociology,* 51(4), pp. 605–622.

Hashimoto, Naoki (2007). "Current issues and measures for prevention of cybercrime." Sōsa kenkyū [Investigation research] 56, no. 2 (February 2007): pp. 20–22

Hauck, R.V. (2002). "Using Copy link to Analyze Criminal- Justice Data," *Computer*, Mar., pp. 30-37.

Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 July - December 2009, Vol 3 (2): pp. 590–591

Kallman, E.A. and Grillo, J.P. (1996). Ethical Decision Making and Information Technology, 2nd ed., McGraw Hill.

Kato, Masayasu (2007). "Current issues on security measures for illegal information and hazardous information on the Internet." In "Cybercrime." Special issue, *Keisatsu koron* [Police public opinion] 62, no. 12 (December 2007): pp. 23–29.

Lipson, H. (2002). Tracking and tracing cyber-attacks: technical challenges and global policy issues.

Maanen (Eds.) (1978). *Policing: A View from the Street,* pp. 7–32. New York: Random House.

Marx, G.T. (2001). Technology and social control: The search for the illusive silver bullet. *International Encyclopaedia of the Social and Behavioral Sciences*, Amsterdam: Elsevier.

National Police Agency (2008). "On the prosecution of cybercrime." *Heisei 19th [19th Conference] of the National Police Agency, 2008.*

Corresponding Author

Navpreet Kaur*

Research Scholar, Computer Science, JJT University, Jhunjhunu, Rajasthan

E-Mail – virk.navpreet@gmail.com