RESEARCH ARTICLE OPEN ACCESS

CYBERCRIME – A Threat to Network Security

V.Swarnakamali [1], D.Roshni [2]
Department of Computer Science Engineering
Saranathan College of Engineering, Trichy
Tamil Nadu - India

ABSTRACT

Digital technology is encompassing in all walks of life, all over the world and has brought the real meaning of globalisation. At the one end cyber system provides opportunity to communicate and at the other end some individuals or community exploit its power for criminal purposes. Criminals exploit the Internet and other network communications which are international in scope. Situation is alarming; Cybercrime is an upcoming and is talk of the town in every field of the society/system. Theoretically and practically this is a new subject for researchers and is growing
exponentially. Lot of work has been done and endless has to be go because the invention or up gradation of new technology
leads to the technical crime i.e. the digital or we can say the cybercrime or e-crime. This is because every day a new technique is being developed for doing the cybercrime and many times we are not having the proper investigating method/model/technique to tackle that newly cybercrime.

In the present day world, India has witnessed an unprecedented index of cybercrimes whether they pertain to Trojan attacks, salami attacks, e-mail bombing, DOS attacks, information theft, or the most common offence of hacking. Despite technological measures being adopted by corporate organizations and individuals, we have witnessed that the frequency of cybercrimes has increased over the last decade. Since users of computer system and internet are increasing worldwide in large number day by day, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by all of us while using the internet which will assist in challenging this major threat cybercrime. In this paper, we have discussed various categories of cybercrime and cybercrime as a threat to person, property, government and society and we have suggested various preventive measures to be taken to snub the cybercrime.

Keywords:- Computer crime, e-Crime, cyber fraud, network security.

I. INTRODUCTION

Cybercrime is a fast growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide. Here, computer is a main target but the target also involves mobile phones, PDAs and game consoles. Although there is no single universal definition of cybercrime, law enforcement generally makes a distinction between two main types of internet-related crime. They are **advanced cybercrime-** sophisticated attacks against computer hardware and software and **cyber-enabled crime**- many 'traditional' crimes have taken a new turn with the advent of the internet such as crime against children, financial crimes and even terrorism. In the past, cybercrime was committed mainly by individuals or small groups. Today, we are seeing highly complex cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale. New trends in cybercrime are emerging all the time, with estimated costs to the global economy running to billions of dollars. Criminal organizations are turning increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. The crimes themselves are not necessarily new – such as theft, fraud, illegal gambling and sale of fake medicines – but they are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging.

II. AIMS AND OBJECTIVES

- To determine the impact of cybercrime on networks.
- To determine the advent of cyber-crime.
- To determine the pros and corn of network security.
- To determine how network security reduces the treat of cybercrime.

III. HISTORY

The first recorded cybercrime took place in the year 1820 which is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This was the first recorded cybercrime.

IV. CATEGORIES OF CYBERCRIME

Cybercrimes can be basically divided into four major categories:

1. Cybercrimes against persons:

Cybercrimes committed against persons include various crimes like transmission of child-pornography, cyber porn, harassment of a person using a computer such as through e-mail, fake escrow scams. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important cybercrimes known today. The potential harm of such a crime to humanity can hardly be explained. Cyber-harassment is a distinct cybercrime. Various kinds of harassment can and do occur in cyberspace, or through the use of cyberspace. Different types of harassment can be sexual, racial, religious, or other. Persons perpetuating such harassment are also guilty of cybercrimes. Cyber harassment as a crime also brings us to another related area of violation of privacy of citizens. Violation of privacy of online citizens is a cybercrime of a grave nature. No one likes any other person invading the invaluable and extremely touchy area of his or her own privacy which the medium of internet grants to the citizen. There are certain offences which affect the personality of individuals can be defined as:

Harassment via E-Mails: This is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter, Orkut etc. increasing day by day.

Cyber-Stalking: It is expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.

Defamation: It involves any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

Hacking: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs. Hackers usually hacks telecommunication and mobile network.

Cracking: It is act of breaking into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

E-Mail Spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.

SMS Spoofing: Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another person in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cybercrime against any individual.

Carding: It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account. There is always unauthorized use of ATM cards in this type of cybercrimes.

Cheating & Fraud: It means the person who is doing the act of cybercrime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.

Assault by Threat: It refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

2**. Cybercrimes against government.** The third category of cybercrimes relates to cybercrimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of cyberspace is being used by individuals and groups to threaten the international governments as also to threaten the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website. The Parliament attack in Delhi and the recent Mumbai attack fall under this category. India had enacted its first cyber Law through IT Act 2000. It has been amended and now in 2008 the revised version is under implementation. From the International cyber Law Expert Pauline Reich is an American lawyer and professor at Waseda University of Law in Tokyo, Japan. As hailed by the Japan Times, she is a pioneer in the field of cybercrime. She spoke to SME WORLD on the present state of cybercrime in India and other countries and what are the systems in place for dealing with the menace. When the European Convention drafted the cybercrime Convention, no exact definition of cybercrime was provided. Every country has its own way of defining cybercrime, which is peculiar to its own socio-cultural situations. For instance, in India defamation is a significant and rampant form of cybercrime. The UN is strongly trying to put in place a global mechanism to improve awareness as well as to implement and install effective security measures for cybercrime. The Council of Europe cybercrime convention is also in place. Countries have to bring their own national laws upto the international benchmark and then ratify the convention**.**

Fig.1. Cybercrime against government

3**. Cybercrimes against property**. The second category of Cyber-crimes is that of cybercrimes against all forms of property. These crimes include computer vandalism (destruction of others' property) and transmission of harmful viruses or programs. A Mumbai-based upstart engineering company lost a say and much money in the business when the rival company, an industry major, stole the technical database from their computers with the help of a co-operate cyber spy software. There are certain offences which affects person's property which are as follows:

Intellectual Property Crimes: Intellectual property consists of a bunch of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an crime. The most common type of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

Cyber Squatting: It involves two persons claiming for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously

Cyber Vandalism: Vandalism means deliberately damaging property of another. Thus cyber vandalism means destroying or damaging the data or information stored in computer when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the. theft of a computer, some part of a computer or a peripheral or a device attached to the computer.

Hacking Computer System: Hackers attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer system. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company. As in April, 2013 MMM India attacked by hackers.

Transmitting Virus: Viruses are programs written by programmers that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They mainly affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computer system of the individuals.

Cyber Trespass: It means to access someone's computer or network without the right authorization of the owner and disturb, alter, misuse, or damage data or system by using wireless internet connection.

Internet Time Thefts: Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged Often, despite infrequent usage.

4. Cybercrimes against society at large: An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences include:

Cyber Trafficking: It involves trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cybercrime is also a gravest crime.

Online Gambling: Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. In India a lot of betting and gambling is done on the name of cricket through computer and internet. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

Financial Crimes: This type of offence is common as there is huge growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.

Forgery: It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

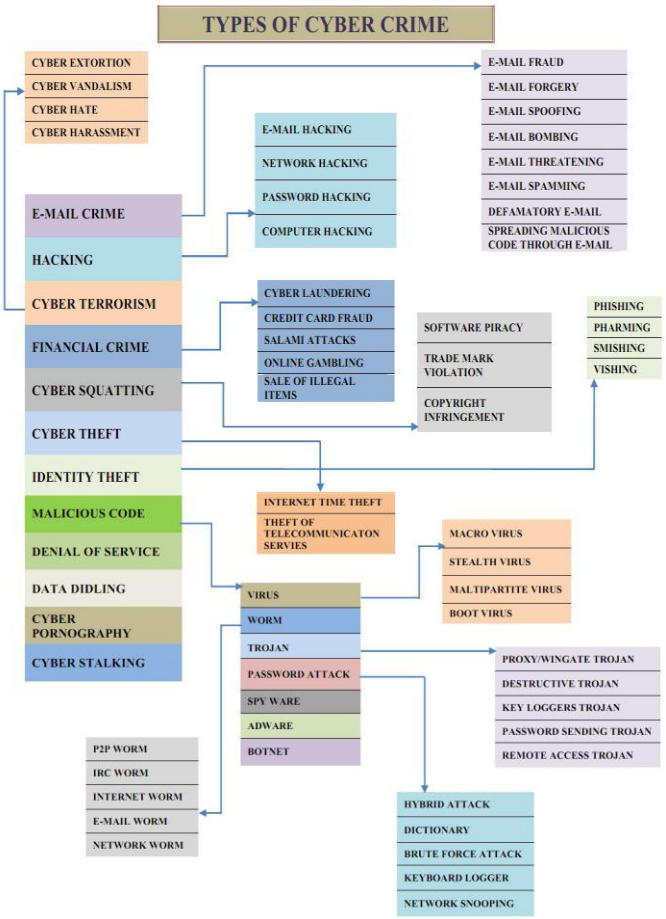

Fig.2. Types of cybercrime

V. SOME PROFESSIONALS GIVING BIRTH TO CYBERCRIME

There are three kinds of professionals in the cyberspace:

1. IT or Tech Professionals Since Cyber Crime is all about computers and Networks (Internet), many types of IT & Technology professionals are quite prominently active in the same, which include but are not restricted to:
   • Network Engineers • Cyber Security Software Professionals • Cyber Forensic Experts • IT Governance Professionals • Certified Internet Security Auditors • Ethical Hackers
2. Cyber Law Experts Cyber Law has become a multidisciplinary approach and hence specialization in handling cybercrimes is required. Cyber law experts handle:
   • Patent and Patent Infringements or other Business Cybercrimes • Cyber Security for Identity thefts and Credit Cards and other Financial transactions • General Cyber Law • Online Payment Frauds •Copyright Infringement of software, music and video.
3. Cyber Law Implementation Professionals Many agencies play a role in cyber law implementation, which include the e-Governance agencies, law and enforcement agencies, cybercrime research cells and cyber forensic labs. Each of these would have a different category of professionals.

VI. TYPES OF HACKERS AND FAMOUS HACKERS

1. **White hackers**- These type of hackers are good they have a genuine license to hack network or a system
2. **Black hackers**- These type of hackers are bad hackers. They are highly skilled and motivated to earn high profits.
3. **Red or Grey hackers**- These type of hackers are someone between the good and bad hackers.

Some famous hackers in history:
1. Ian Murphy
2. Kelvin Mitnick
3. Johan Helsinguis
4. Linus Torvalds
5. Mark Abene
6. Robert Morris

VII. CYBERCRIME CHALLENGES

Endless discussion is there regarding the pros and cons of cybercrime. There are many challenges in front of us to fight against the cybercrime. Some of them here are discussed below:
A. Lack of awareness and the culture of cyber security, at individual as well as organizational level. B. Lack of trained and qualified manpower to implement the counter measures. C. No e-mail account policy especially for the defense forces, police and the security agency personnel D. Cyber-attacks have come not only from terrorists but also from neighboring countries contrary to our National interests.
E. The minimum necessary eligibility to join the police doesn't include any knowledge of computers sector so that they are almost illiterate to cybercrime. F. The speed of cyber technology changes always beats progress of govt. sector so that they are not able to identify the origin of these cybercrimes. G. Promotion of Research & Development in ICTs is not up to the mark. H. Security forces and Law enforcement personnel are not equipped to address high-tech crimes. I. Present protocols are not self-sufficient, which identifies the investigative responsibility for crimes that stretch internationally. J. Budgets for security purpose by the government especially for the training of law enforcement, security personnel's and investigators in ICT are less as compare to other crimes.

VIII. STATISTICS

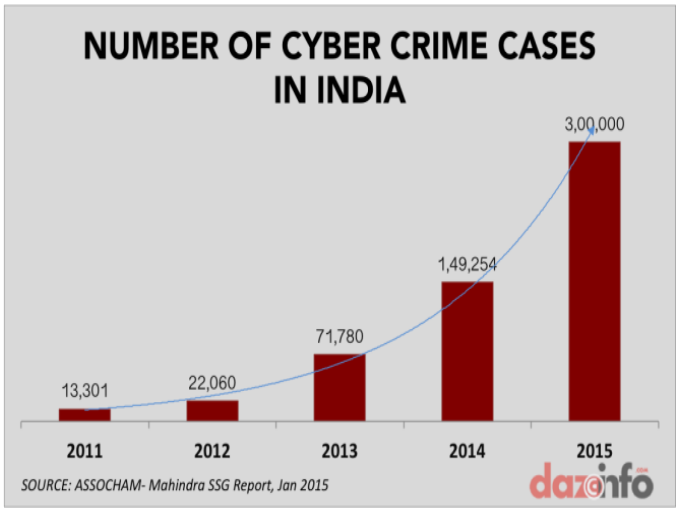

Fig.3. Graph showing cybercrime statistics in India

On account of such cybercrime cases, annually there is a loss of Rs.30000 crores in the world. The number of cybercrime cases in India is keeping on increasing. This can be realized from the above graph. Most number of cybercrimes reported in Maharashtra (5000 cases) and Uttar Pradesh (4900 cases) between 2011 and 2015 and the third affected state is Karnataka (3500 cases). More than 32000 cybercrimes were reported across the country. Those three states are the ones with a greater internet subscriber base. The cybercrime cases are very less in Rajasthan. To address this, our government declared the month October as NATIONAL CYBER SECURITY AWARENESS MONTH.
USA is the most affected country in the world by cybercrime. China ranks second and India ranks 11th.

IX. PREVENTION OF CYBER CRIME

Prevention is always better than cure. It is always better to take certain precautions while working on the net. One should make them a part of his cyber life. Sailesh Kumar Zarkar, technical advisor and network security consultant to the Mumbai Police cybercrime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance.

1. Identification of exposures through education will assist responsible companies and firms to meet these challenges.
2. One should avoid disclosing any personal information to strangers, the person whom they don't know, via e-mail or while chatting or any social networking site.
3. One must avoid sending any photograph to strangers by online as misusing or modification of photograph incidents increasing day by day.
4. An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.
5. A person should never send his credit card number or debit card number to any site that is not secured, to guard against frauds.
6. It is always the parents who have to keep a watch on the sites that their children are accessing, to prevent any kind of harassment or depravation in children.
7. Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cybercrimes as number of internet users are growing day by day.
8. Data security:

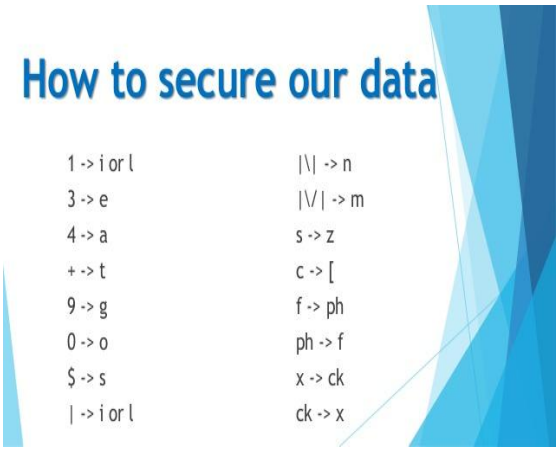

Fig.4. Encoding the data

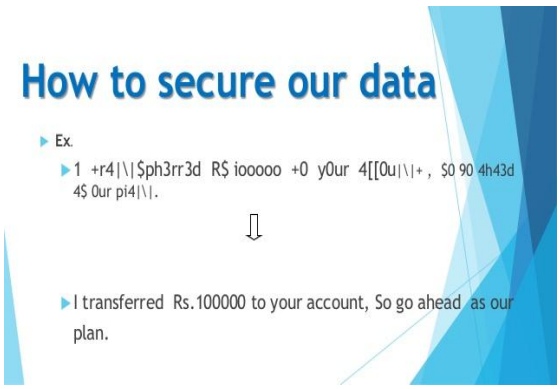

Fig.5. Decoding the data

9. Web servers running public sites must be physically separately protected from internal corporate network.
10. It is better to use a security programs by the body corporate to control information on sites.
11. Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens.
12. IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.
13. As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.
14. A complete justice must be provided to the victims of cybercrimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cybercrime.
15. Recommended antivirus software:

Fig.6. Antivirus software

X. BENEFITS OF NETWORK SECURITY

1.Prevents unauthorized users from accessing your network.

2. Provides transparent access to Internet-enabled users.

3. Ensures that sensitive data is transferred safely by the public network.

4.Help your managers to find and fix security problems.
5.Provides a comprehensive system of warning alarms attempt to access your network.

XI. TERMINOLOGIES RELATED TO CYBERCRIME

1. **Ransomware-** It is a type of malicious software designed to block access to a computer system until a sum of money is paid.
2. **Cyber bullying-** Cyber bullying or cyber harassment is a form of bullying or harassment using electronic forms of contact. Cyber bullying has become increasingly common, especially among teenagers.
3. **Cyber warfare-** Cyber warfare has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption",[1]:6 but other definitions also include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations.
4. **Privilege escalation-** Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.
5. **Click jacking-** It is the malicious practice of manipulating a website user's activity by concealing hyperlinks beneath legitimate clickable content, thereby causes the user to perform actions of which they are unaware**.**
6. **Like jacking-** Like jacking is a variation on click jacking in which malicious coding is associated with a Facebook Like button. The most common purposes of like jacking include identity theft and the dissemination of viruses, social spam and hoaxes.

XII.CONCLUSION

In conclusion, computer crime does have a drastic effect on the world in which we live. It affects every person no matter where they are from. It is ironic that those who in secret break into computers across the world for enjoyment have been labelled as deviance. Many hackers view the Internet as public space for everyone and do not see their actions as criminal. Hackers are as old as the Internet and many have been instrumental in making the Internet what it is now. In my view point hacking and computer crime will be with us for as long as we have the Internet. It is our role to keep the balance between what is a crime and what is done for pure enjoyment. Luckily, the government is making an effort to control the Internet. Yet, true control over the Internet is impossible, because the reasons the Internet was created. This is why families and the institution of education of is needed, parents need to let their children know what is okay to do on the computer and what is not and to educate them on the repercussions of their actions should they choose to become part of the subculture of hackers. In finishing this paper, the true nature of what computer crime will include in the future is unknown. What was criminal yesterday may not be a crime the next day because advances in computers may not allow it. Passwords might be replaced for more secure forms of security like biometric security. Most of the recorded computer crimes cases in most organization involve more than individual and virtually all computer crime cases known so far are committed by employer of the organization. Criminals have also adapted the advancements of computer technology to further their own illegal activities. Without question, law enforcement must be better prepared to deal with many aspects of computer-related crimes and the techno-criminals who commit them. This article is not meant to suggest that programmers or computer users are fraudulent people or criminal but rather to expose us to the computer-related crime and provides ways to prevent them.

Since users of computer system and internet are increasing worldwide in large number day by day, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by all of us while using the internet which will assist in challenging this major threat Cyber Crime.

REFERENCES

[1] Communications Fraud Control Association. 2011 global fraud loss survey. Available: http://www.cfca.org/fraudlosssurvey/, 2011.

[2] F. Lorrie, editor. "*Proceedings of the Anti-Phishing Working Groups*", 2nd Annual e-Crime Researchers Summit 2007, Pittsburgh, Pennsylvania, USA, October 4–5, 2007, vol. 269 of ACM International Conference Proceeding Series. ACM, 2007.

[3] I. Henry, "*Machine learning to classify fraudulent websites*". 3rd Year Project Report, Computer Laboratory, University of Cambridge, 2012.

[4] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. London: Academic Press, 2011:

[5] www.uncjin.org/Documents/EighthCongress.html.

[6] http://www.thefreedictionary.com/Gun+Crime).

[7] Roshan, N., What is cyber Crime. Asian School of Cyber Law, 2008: Access at - http://www.http://www.asclonline.com/index.php?titl e=Rohas_Nagpal,

[8] Govil, J., Ramifications of Cyber Crime and Suggestive Preventive Measures, in International Conference on Electro/Information Technology, 2007 IEEE. 2007: Chicago, IL. p. 610-615.

[9] Jones, A., Technology: illegal, immoral, or Fattening?, in Proceedings of the 32nd annual ACM SIGUCCS fall conference. 2004, ACM: Baltimore