- N.A. Azeez, O. Osunade, Towards ameliorating cyber-crime and Cyber security (IJCSIS) International Journal of Computer Science and Information Security, Vol. 3, No. 1, 2009.
- Neilson Ratings. (2011). Top ten global web parent companies, home and work. Retrieved February 24, 2012.
- Nilkund Aseef, Pamela Davis, Manish Mittal, Khaled Sedky, Ahmed Tolba (2005), Cyber-Criminal Activity and Analysis, White Paper, Group 2.
- S. Hinde, "The law, cybercrime, risk assessment and cyber protection", Computers & Security, vol. 22, issue 2, pp. 90-95, February 2003.
- S.WBrenner, Cybercrime: Criminal Threats from Cyberspace, an Imprint of ABC-CLIO, LLC, Santa Barbara, CA, 2010, ISBN 978-0-313-36546-1.
- Shantosh Rout (2008), Network Interferences, Available at: http://www.santoshraut.com/ forensic/ cybercrime.htm, Visited: 28/01/2012.
- Shantosh Rout (2008), Network Interferences, Available at: http://www.santoshraut.com/ forensic/ cybercrime.htm, Visited: 28/01/2012.
- www.cyberlawportal.com

of forensics personnel/law enforcement agencies. Above all, a comprehensive law to combat computer and cyber related crimes should be promulgated to fight these phenomenon's to a halt. We recommend that before anybody enters into any kind of financial deals with anyone through the internet he/she should use any of the search engines to verify the identity of the unknown.

References:

- Bequai, "A guide to cyber - crime investigations", Computers & Security, vol. 17, issue 7, pp.579-582, 1998.
- Cyber Crimes on the rise in state - Kerala: The Hindu Monday Oct 30, 2006.
- Gordon, L. A. et al., 2003, A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3): 81-85.
- Leagal Info (2009), Crime Overview Aiding And Abetting Or Accessory, Available at: http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory.html, Visited: 28/01/2012.
- N. Leontiadis, T. Moore, and N. Christin. "Measuring and analyzing search - redirection attacks in the illicit online prescription drug trade". In Proceedings of USENIX Security 2011, San Francisco, CA, August 2011.

el for preventing the cybercrime.

- 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.

Conclusions and Recommendations:

From our investigation on cybercrimes we observed its threat to the economy of a nation and even peace and security. Therefore, there is need for a holistic approach to combat these crimes in all ramifications. Our proposal therefore is the need for cyber police who are to be trained specially to handle cybercrimes in Iraq. In addition, the police should have a Central Computer Crime Response to act as an agency to advise the government and other investigative agencies to guide and coordinate computer crime investigation. We are also proposing that the government should set up National Computer Crime Resource Centre, a body, which will comprise experts and professionals to establish rules, regulations and standards of authentication of each citizen's records and the staff of establishments and recognized organization, firms, industries etc. Forensics commission should be established, which will be responsible for the training

back up volumes so that one may not suffer data loss in case of virus contamination.

- A person should never send his credit card number or debit card number to any site that is not secured, to guard against frauds.
- 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.
- Web servers running public sites must be physically separately protected from internal corporate network.
- It is better to use a security programs by the body corporate to control information on sites.
- Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens.
- 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.
- As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international lev-

work being done through websites, S all sectors are equally vulnerable to cybercrime. Cyber Crimes always affects the companies of any size because almost all the companies gain an online presence and take advantage of the rapid gains in the technology but greater attention to be given to its security risks. However, I would say that SMEs in the IT industry are the greatest stake holders. Piracy and copy right protection are the major threats.

Prevention of Cybercrime:

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.

- Identification of exposures through education will assist responsible companies and firms to meet these challenges.
- 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.
- One must avoid sending any photograph to strangers by online as misusing or modification of photograph incidents increasing day by day.
- An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep

website. Many Iraqi minsters or governmental persons fall under this category.

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:

- Child Pornography: In this act there is use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.
- 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.
- 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.

The Effect of Cybercrimes on Businesses:

As all types of businesses in the world there is a rapid development of working in the online mode because most of their

be loss of data as well as computer system.

- 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.
- 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.

3. Cybercrimes against Government:

The third category of Cyber-crimes relates to Cybercrimes against Government. Cyber terrorism is one common type of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by persons and groups to threaten the international governments as also to threaten the citizens of a country. This crime linked itself into terrorism when an individual "cracks" into a government or military maintained

The second category of Cyber-crimes is that of Cybercrimes against all types of property. These crimes include computer vandalism (destruction of others' property) and transmission of harmful viruses or programs.

- Intellectual Property Crimes: Intellectual property includes a bunch of rights. Any horrible act by which the owner is prevented completely or partially of his/her rights is a 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.
- Hacking Computer System: Hackers attacks those included Famous Twitter, blogging plat form by unauthorized access/ control over the computer. Due to the hacking activity there will

- Cracking: It is act of breaking into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.
- SMS Spoofing: Spoofing is a blocking through spam which means the unwanted uninvited messages. Here an 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.
- Cheating & Fraud: It means the person who is doing the act of cybercrime for example stealing password and information storage has done it with having guilty mind which leads to fraud and cheating.
- Child Pornography: In this cybercrime defaulters create, distribute, or access materials that sexually exploit underage children.
- 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- Cypher-crimes against property:

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.

- Harassment via E-Mails: This is very common type of harassment through sending messages, attachments of files and folders for example by e-mails. At present harassment is common as usage of social sites like. Facebook, Twitter, Telegram 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 inter net, 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.

2. Cyber Law Experts: Cyber Law has become a multidisciplinary approach and hence specialization in handling cybercrimes is required. Cyber law experts handle:

- Copyright Infringement of software, music and video.
- General Cyber Law
- Cyber Security for Identity thefts and Credit Cards and other financial transactions
- Patent and Patent Infringements or other Business Cybercrimes, and
- Online Payment Frauds

3. Cyber Law Implementation Professionals: Many organizations 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.

Categories of Cyber Crime:

Cybercrimes can be divided into four major categories:

1- Cyber-crimes against persons:

Cyber-crimes conducted against persons include many crimes like transmission of child pornography, cyber porn, harassment of a person using a computer such as through e-mail,

members of a terrorist cell or criminal organization may use hidden messages to communicate in a public forum to plan activities or discuss money laundering locations.

- It is usually facilitated by installations that do not fit into the classification of crime ware. Like, conversations may take place using Instant Messaging. Clients or files may be transferred using FTP.

Profession of Cybercrime:

There are three types 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:

- Ethical Hackers
- Cyber Security Software Professionals
- Network Engineers
- IT Governance Professionals
- Cyber Forensic Experts, and
- Certified Internet Security Auditors

First Type: Has the following principles: It is usually a solo action from the point of view of the victim. Such as, the victim unknowingly downloads or installs a Trojan horse which installs a keystroke logger on his or her machine. Instead, the victim might get an e-mail including a fake link to a known entity, but in fact it is a link to a hostile website. There is large number of software for keylogger, they are can perform such theft. Samples of this kind of cybercrime consist of, but are not limited to phishing, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud.

Second Type: It consists, but also is not limited to activities such as computer related frauds, fake antivirus, cyber-stalking and harassment, child predation, extortion, travel scam, fake escrow scams, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities. The properties of Type II cybercrime are:

- It is usually continues series of actions, consisting many connections with the target. Like, the target is connected in a chat room by someone who, over time, tries to make a relationship. At the end, the criminal uses the relationship to conduct a crime. Or,

and victims (the person behind it); it just depends on which of the two is the main target. Cybercrime could include anything as easy as downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also can contain non-monetary offenses, like establishing and distributing tiny or huge programs written by hackers known as viruses on other computers or posting confidential business information on the Internet. An important kind of cybercrime is identity theft, in which hackers employ the Internet to steal private data from other users. Various kinds of social networking sites are used for this aim to find the identity of interested peoples. This can be done by two means: phishing and harming, both types cheating users to fake websites, where they are asked to enter personal information. This includes login information, such as usernames and passwords, phone numbers, addresses, credit card numbers, bank account numbers, and other information criminals can use to "steal" another person's identity.

Cybercrimes can be divided into two types, depending on the aim of understanding as First Type and Second Type cybercrime, as follows:

and OECD, are seriously discussing cooperative schemes, but many countries do not share the urgency to fight cybercrimes for many reasons, including different attitudes toward piracy or espionage or the need to address more pressing social problems. Though the case of jurisdiction in cyberspace cannot be settled spontaneously, but still an international effort in this issue is the need of hour.

Iraq has witnessed a tremendous increase in Cybercrimes whether they pertain to Trojan attacks, salami attacks, e -mail bombing, DOS attacks, information theft, or the most common offence of hacking the data or system to commit crime. In spite technological actions being adopted by all organizations and individuals, we have faced that the number of cybercrimes has increased over the last years.

Cybercrime means to the act of doing an illegal act through computer or cyberspace (the Internet network), as the communication mean. Though there is no technical explanation by any statutory body for Cybercrime, it is generally defined by the Computer Crime Research Center as: “Crimes committed on the internet using the computer either as a tool or a targeted victim.” All sorts of cybercrimes include two things they are: computer

'cyberspace'. It becomes a basic for human activities which converge on the internet. The cyberspace generally becomes the most happening place today. Communication now used in a large number via internet like advertising, banking, education, research and entertainment. It is difficult to find someone's activity is not linked with internet. So, technology has something to offer to everybody and in the process it only increases and will not stop. It becomes a place to do all types of activities which are forbidden by law. Rapidly increasing for using in illegal activities such as trafficking in human organs, violating individual privacy, pornography, gambling, and forbidden drugs, hacking, infringing copyright, , money laundering, terrorism, fraud, software piracy and corporate espionage, to name a few.

Crimes of Cyber:

Cybercrime is not a matter of concern for Iraq only but it is a global problem and hence the world should come forward to cut this menace. More difficult cybercrime enforcement is the area of legal jurisdiction. Such as pollution control legislation, Iraq only cannot by itself effectively enact laws that comprehensively address the problem of internet crimes without cooperation from other nations. While the major global organizations, like the G-8

Introduction:

Technology plays an important role in both the consumer's life and in the delivery of the services. Iraqi Government tries to establish digital government which is a step towards ensuring access to technology to all of Iraqis. Services provided by technology made the life easier from many aspects like: E-commerce, Banking, Insurance, etc. technology is can be considered as the bridge to provide better service to the customers. Du to the fast development of Information technology in business, costumers are now facing to many risks. E-commerce becomes a new market and tough competition for interacting between customers and buyers for selling products. Customers are doing online purchases and vulnerable for internet hackers sometimes. Unfortunately many of customers are not aware of such problems. The contrast is that business methods and procedures are improving in everyday but the laws relating business are not changing in the same speed. Costumers' protection may become a myth under these circumstances.

Cyberspace:

The establishment of networks and telecommunications helped the digital technologies to emerge the birth of what is called now

Abstract

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, it is easy to access any information within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. The objective of this paper is to discuss about the cybercrime and its categories, and the mechanism to prevent it, and shade light on professions giving birth to cybercrimes and its impact on businesses and the preventive measures to be taken to control the cybercrime. The result showed that there is a need for cyber police who are to be trained specially to handle cybercrimes in Iraq. In addition, the police should have a Central Computer Crime Response to act as an agency to advise the government and other investigative agencies to guide and coordinate computer crime investigation.

Keywords: Cybercrime, Cyber laws, hacking, Virus

The Mechanisms of Prevent Cybercrimes in Iraq

1. Assistant Professor Dr. Malik Mansi Salih
Mustansiriyah University/College of law.
alqurabylooh@yahoo.com
2. Assistant Lecturer Zinah Younis Hussein
Mustansiriyah University/College of Physical Education and Sport Science .
3. Amera Ghazi Salih
Mustansiriyah University/College of Physical Education and Sport Science .