The Mechanism of Preventing Cybercrimes in Iraq

آلية منع الجرائم الإلكترونية في العراق

Zinah Younis Hussein
Mustansiriyah University, College of Physical Education and Sports Sciences
drsaifalzweny@gmail.com

DOI: https://doi.org/10.70411/MJLS.4.1.2026269
تاريخ الاستلام: 17-06-2025 تاريخ المراجعة: 06-07-2025 تاريخ القبول: 06-07-2025

Abstract

Despite the adoption of technological measures by corporate organisations and individuals, the frequency of cybercrimes has increased over the last decade. As the number of computer systems and internet users continues to grow rapidly worldwide, accessing any information within a few seconds has become easier through the internet, a vast medium for data exchange and global communication. The objective of this paper is to discuss cybercrime, its categories, preventive mechanisms, the professions contributing to its rise, its impact on businesses, and the necessary measures to be taken to control 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, a Central Computer Crime Response unit should be created to advise the government and other investigative agencies and to guide and coordinate computer-related crime investigations.

Keywords: Cybercrime, Cyber laws, Hacking, Virus.

الملخص

على الرغم من التدابير التكنولوجية التي يتم تبنيها من قبل الشركات والأفراد، فقد شهدنا زيادة وتيرة الجرائم الإلكترونية على مدى العقد الماضي. نظرًا لأنَّ مستخدمي أنظمة الكمبيوتر والإنترنت يتزايدون في جميع أنحاء العالم بأعدادٍ كبيرة يومًا بعد يوم، فمن السهل الوصول إلى أي معلومات في غضون ثوانٍ قليلة باستخدام الإنترنت الذي يعد وسيلة للمعلومات الضخمة وقاعدة كبيرة من الاتصالات حول العالم. يهدف هذا البحث إلى مناقشة الجرائم الإلكترونية وفئاتها وآلية منعها وإلقاء الضوء على المهن التي تولد الجرائم الإلكترونية وأثرها على الأعمال والإجراءات الوقائية الواجب اتخاذها للسيطرة على الجرائم الإلكترونية. وأظهرت النتيجة أن هناك حاجة لشرطة إلكترونية يتم تدريبها خصيصًا للتعامل مع الجرائم الإلكترونية في العراق. بالإضافة إلى ذلك، يجب أن يكون لدى الشرطة استجابة مركزية لجرائم الكمبيوتر للعمل كوكالة لتقديم المشورة للحكومة ووكالات التحقيق الأخرى لتوجيه وتنسيق التحقيق في جرائم الكمبيوتر.

الكلمات المفتاحية: الجرائم الإلكترونية، قوانين الإنترنت، القرصنة، الفيروسات.

Introduction

Technology plays an important role in both consumers' lives and the delivery of the services. The Iraqi government is working to establish a digital government, which is a step towards ensuring access to technology for all Iraqis. Technology-based services have made life easier in many areas, such as e-commerce, banking, and insurance. Technology can be considered a bridge to providing better service to the customers [1]. Due to the fast development of information technology in business, customers are now facing too many risks. E-commerce has become a new marketplace and a highly competitive environment for interactions between customers and sellers. Customers are making online purchases and are sometimes vulnerable to internet hackers. Unfortunately, many customers are not aware of such threats. The contrast lies in the fact that while business methods and procedures are improving every day, the laws related to business are not changing at the same speed. Under these circumstances, consumer protection may become a myth [2].

Cyberspace

The development of networks and telecommunications has led to the emergence of digital technologies and the creation of what is now known as cyberspace. It has become a foundation for human activities that increasingly converge on the internet. Today, cyberspace is one of the most active and dynamic environments. Communication is now widely conducted through the internet in areas such as advertising, banking, education, research and entertainment. It is difficult to find an activity that is not somehow linked to the internet. Technology offers something for everyone, and its influence continues to grow without signs of slowing down. Cyberspace has also evolved into a hub for a variety of activities, some of which are illegal [3].

It is increasingly being used for illegal purposes, including human organ trafficking, privacy violations, pornography, gambling, illegal drug trade, hacking, copyright infringement, money laundering, terrorism, fraud, software piracy, and corporate espionage, to name a few [4].

---

1. Bequai, (1998). A guide to cyber - crime investigations", Computers & Security, vol. 17, issue 7, pp.579-582.
2. N. Leontiadis, T. Moore, and N. Christin. (2011) "Measuring and analyzing search - redirection attacks in the illicit online prescription drug trade". In Proceedings of USENIX Security 2011, San Francisco, CA, August.
3. 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.
4. (Ibid).

Cybercrimes

Gordon states that cybercrime is not only a matter of concern for Iraq but a global problem; hence, the world should come together to combat this menace. One of the major challenges in combating cybercrime is legal jurisdiction. Similar to pollution control legislation, Iraq alone cannot effectively enact laws that comprehensively address the problem of internet crimes without international cooperation. While major global organisations like the G8 and OECD are seriously discussing cooperative strategies, many countries do not share the same urgency to fight cybercrimes due to various reasons, such as different attitudes toward piracy and espionage or the need to address more pressing social problems. Although the case of jurisdiction in cyberspace cannot be settled spontaneously, international collaboration remains essential [1].

Iraq has witnessed a tremendous increase in cybercrimes whether they involve Trojan attacks, salami attacks, email bombing, DoS attacks, information theft, or the most common offence, hacking data or systems to commit crimes. Despite technological measures being adopted by all organisations and individuals, the number of cybercrimes has increased over the last years.

Cybercrime refers to the act of doing an illegal activity using a computer or cyberspace (i.e., the internet) as the means of communication. Though there is no official technical explanation provided by any statutory body, the Computer Crime Research Centre generally defines cybercrime as "crimes committed on the internet using the computer either as a tool or a targeted victim". All forms of cybercrimes include two elements: a computer and a victim (i.e., the person behind the system); the distinction lies in which of the two is the main target. Cybercrime could include acts ranging from something as simple as downloading illegal music files to stealing millions of dollars from online bank accounts [2].

Cybercrime can also contain non-monetary offences, such as creating and distributing malicious programs (viruses) written by hackers or posting confidential business information online. A major type of cybercrime is identity theft, in which hackers use the Internet to steal private data from other users. Various social networking sites are exploited for this purpose to uncover the identities of targeted individuals. This can be done by two main methods: phishing and pharming. Both techniques deceive users into visiting fake websites where they

1. Neilson Ratings. (2011). Top ten global web parent companies, home and work. Retrieved February 24, 2012.
2. 91 S. Hinde, (2003) "The law, cybercrime, risk assessment and cyber protection", Computers & Security, vol. 22, issue 2, pp. 90-95, February.

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 sensitive information criminals can use to "steal" a person's identity [1].

Cybercrimes can be divided into two types based on their purpose, referred to as First Type and Second Type cybercrime [2].

First Type

This type has the following characteristics: It is usually a solo action from the victim's point of view. For example, the victim may unknowingly download or install a Trojan horse that installs a keystroke logger on their device. Instead, the victim might receive an email containing a fake link that appears to be from a trusted entity but actually leads to a malicious website. There are many types of keylogger software capable of performing such theft. Examples of this type of cybercrime include, but are not limited to phishing, data or services theft or manipulation via hacking or viruses, identity theft, and bank or e-commerce fraud.

Second Type

It consists of, but also is not limited to, activities such as computer-related fraud, fake antivirus, cyber-stalking and harassment, child predation, extortion, travel scams, 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 usually involves a continuousseries of actions, consisting of many interactions with the target. For example, the target may be approached 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, members of a terrorist cell or criminal organisation may use hidden messages to communicate in public forums in order to plan activities or discuss money laundering locations.
- It is usually facilitated by installations that do not fit into the classification of crimeware. For instance, conversations may occur via instant messaging, and clients or files may be transferred using FTP.

[1] Nilkund Aseef, Pamela Davis, Manish Mittal, Khaled Sedky, Ahmed Tolba (2005), Cyber-Criminal Activity and Analysis, White Paper, Group 2.

[2] N.A. Azeez, O. Osunade, (2009). Towards ameliorating cybercrime and Cyber security (IJCSIS) International Journal of Computer Science and Information Security, Vol. 3, No. 1.

Professions in Cybercrime

According to [1], there are three types of professionals in cyberspace:

1. **IT or Tech Professionals:** Since cybercrime primarily involves computers and networks (i.e., the Internet), many IT & technology professionals are quite prominently active in this field. These include, but are not restricted to:

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

2. **Cyber Law Experts:** Cyber law has become a multidisciplinary field, and specialisation in handling cybercrimes is required. Cyber law experts handle:

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

3. **Cyber Law Implementation Professionals**: Many organisations play a role in the implementation of cyber laws. These include the e-governance agencies, law enforcement agencies, cybercrime research cells, and cyber forensic labs. Each of these would have a different category of professionals.

Categories of Cybercrime

Cybercrimes can be divided into four major categories according to Shantosh (2008):

1- Cybercrimes against individuals

Cybercrimes committed against individuals include many crimes like the transmission of child pornography, cyber pornography, and harassment through email, as well as fake escrow scams. The trafficking, distribution, posting, and dissemination of obscene material, including pornography and indecent exposure, constitute some of the most serious cybercrimes known today.

- **Harassment via Emails**: This is a very common type of cyber harassment involving sending threatening or inappropriate messages, files, or attachments by email.

[1]. Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace (Santa Barbara, CA: Praeger, 2010), p313.

Nowadays, such harassment has become more widespread with the increasing use of social media platforms like Facebook, Twitter, and Telegram.

- **Cyber-Stalking**: It involves explicit or implicit physical threats that cause fear, using computer technology such as the internet, email, phones, text messages, webcams, websites or videos.
- **Defamation**: This involves a person intentionally attempting to damage someone's reputation by hacking their email account and sending messages containing vulgar language to unknown recipients.
- **Hacking**: This refers to gaining unauthorised control or access over a computer system. The act of hacking can completely destroy data and computer programs. Hackers usually target telecommunication and mobile networks.
- **Cracking**: It is the act of breaking into computer systems without the owner's knowledge or consent and tampering with valuable confidential data and information.
- **SMS Spoofing**: Spoofing involves sending spam or unwanted messages. In this cybercrime, an offender steals another person's identity by using their mobile phone number to send SMS messages via the internet, making the receiver believe the messages came from the victim's number. It is a very serious cybercrime against individuals.
- **Cheating & Fraud**: This refers to a person committing a cybercrime, such as stealing passwords or information storage, with a guilty mind, which leads to acts of fraud and cheating.
- **Child Pornography**: This type of cybercrime involves the creation, distribution, or access of materials that sexually exploit underage children.
- **Assault by Threat**: It refers to threatening a person or their family members with harm through the use of a computer network, such as email, videos or phones.

2- Cybercrimes against property

The second category of cybercrimes includes offences against all types of property. These crimes include computer vandalism (the destruction of others' property) and the transmission of harmful viruses or programs [1].

- **Intellectual Property Crimes**: Intellectual property includes a set of rights. Any unlawful act that completely or partially deprives the owner of these rights is considered a crime. The most common types of intellectual property rights (IPR)

[1] S Susan W. Brenner, op.cit, p314.

violations include software piracy, copyright infringement, trademark, patent, design and service mark violation, and theft of computer source code.

- **Cyber Squatting**: It involves two parties claiming the same domain name, either by claiming that they registered the name first, have prior rights to its use, or are using a name similar to one previously established. **Cyber Vandalism**: Vandalism means deliberately damaging property of another. Cyber vandalism, therefore, means destroying or damaging the data or information stored in a computer when a network service is stopped or disrupted.
- **Hacking Computer System**: Hackers attack computer systems, including popular platforms like Twitter and blogging sites, by gaining unauthorised access or control. Such hacking activities can result in data loss as well as damage to the computer systems.
- **Transmitting Virus**: Viruses are programs written by programmers that attach themselves to a computer or a file and then spread to other files and computers on a network. They mainly affect the data on a computer by either altering or deleting it.
- **Cyber Trespass**: This refers to accessing someone's computer or network without proper authorisation and disturbing, altering, misusing, or damaging data or the system, often through a wireless internet connection.
- **Internet Time Thefts**: Internet time theft falls under the category of hacking. It refers to the unauthorised use of Internet hours paid for by another person.

3- Cybercrimes against government

The third category of cybercrimes relates to offences committed against government. Cyberterrorism is a common example within this category. The growth of the internet has shown that cyberspace is increasingly being used by individuals and groups to threaten national governments and their citizens. This form of crime becomes linked to terrorism when an individual hacks into a government- or military-maintained website. According to [1], many Iraqi ministers or governmental officials fall under this category [2].

4- Cybercrimes against society at large:

An unlawful act done with the intention of causing harm to cyberspace will affect large number of people. These offences include [3]:

1. S Susan W. Brenner, op.cit, p315.
2. S.W. Brenner, op.cit, p31.
3. Gordon, L. A. et al., (2003) A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3): 81-85.

- **Child Pornography**: This involves the 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**: This refers to the trafficking of drugs, human beings, weapons, etc., which affects a large number of people. Cyber trafficking is considered one of the most serious forms of cybercrime.
- **Financial Crimes**: This type of offence is common due to the rapid growth in users of networking sites and mobile networks, where the perpetrator may attempt to commit fraud by sending bogus emails or messages via the internet. For example: Illegally using credit cards by obtaining passwords.
- **The Effect of Cybercrimes on Businesses:**

  With the rapid shift of all types of businesses toward online operations, where much of their work is conducted through websites, all sectors have become equally vulnerable to cybercrime. Cybercrimes affect companies of all sizes, as nearly every business now maintains an online presence and benefits from technological advancements. However, small and medium-sized enterprises (SMEs) in the IT industry are arguably the greatest stakeholders. Piracy and copyright infringement are among the major threats [1].

Prevention of Cybercrime:

Prevention is always better than cure. It is always better to take certain precautions while working on the internet. One should make them a part of his cyber life.

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, people they don't know, via email or while chatting on any social networking site.
3. One must avoid sending any photograph to strangers online, as incidents of photo misusing or modification are increasing day by day.
4. All netizens should use updated antivirus software to guard against virus attacks and also maintain backup volumes to avoid data loss in case of virus contamination.
5. A person should never send their credit or debit card number to any site that is not secured to guard against fraud.

[1]. Kerela (2006): Cyber Crimes on the rise in state - Kerala: The Hindu Monday Oct 30.

6. Website owners should monitor traffic and check for any irregularity on their site. It is the responsibility of website owners to adopt policies to prevent cybercrimes as the number of internet users grows day by day.
7. Web servers running public sites must be physically separated and protected from the internal corporate network.
8. It is better for the corporate body to use security programs to control information on the sites.
9. Strict statutory laws need to be passed by the legislatures, keeping in mind the interests of netizens.
10. IT departments should pass certain guidelines and notifications for the protection of computer systems and should also introduce stricter laws to combat criminal activities in cyberspace.
11. As cybercrime is a major threat to countries worldwide, certain steps should be taken at the international level to prevent it.
12. Complete justice must be provided to the victims of cybercrimes through appropriate compensation, and offenders should be punished with the highest type of punishment so that it will deter the criminals of cybercrime.

Conclusions and Recommendations

From our investigation into cybercrimes, we observed that they pose a significant threat to a nation's economy, as well as to its peace and security. Therefore, a holistic approach is needed to combat these crimes in all their forms. We propose the establishment of a cyber police force, specially trained to handle cybercrimes in Iraq. In addition, the police should have a Central Computer Crime Response unit to act as an agency that advises the government and other investigative agencies, guiding and coordinating computer crime investigations. We also propose that the government establish a National Computer Crime Resource Centre- an organisation comprising experts and professionals tasked with setting rules, regulations, and standards of authentication of each citizen's records, as well as the records of employees in establishments and recognised organisations, firms, industries, etc. A forensics commission should also be established to oversee the training of forensics personnel and law enforcement agencies. Above all, a comprehensive law should be enacted to combat computer- and cyber-related crimes and bring these phenomena to a halt. We recommend that before entering into any kind of financial deals with someone over the internet, individuals should use a search engine to verify the identity of the person involved.

Conflict of Interest Statement

All authors declare that they have no conflict of interest

References

1. Bequai, (1998). A guide to cyber - crime investigations", Computers & Security, vol. 17, issue 7.
2. Gordon, L. A. et al., (2003) A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3).
3. Kerela (2006): Cyber Crimes on the rise in state - Kerala: The Hindu Monday Oct 30.
4. 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.
5. N. Leontiadis, T. Moore, and N. Christin. (2011) "Measuring and analyzing search - redirection attacks in the illicit online prescription drug trade". In Proceedings of USENIX Security 2011, San Francisco, CA, August.
6. N.A. Azeez, O. Osunade, (2009). Towards ameliorating cybercrime and Cyber security (IJCSIS) International Journal of Computer Science and Information Security, Vol. 3, No. 1.
7. Neilson Ratings. (2011). Top ten global web parent companies, home and work. Retrieved February 24, 2012.
8. Nilkund Aseef, Pamela Davis, Manish Mittal, Khaled Sedky, Ahmed Tolba (2005), Cyber-Criminal Activity and Analysis, White Paper, Group 2.
9. S. Hinde, (2003) "The law, cybercrime, risk assessment and cyber protection", Computers & Security, vol. 22, issue 2, pp. 90-95, February.
10. S.W. Brenner, (2010) Cybercrime: Criminal Threats from Cyberspace, an Imprint of ABC-CLIO, LLC, Santa Barbara, CA, ISBN 978-0-313-365461.
11. Shantosh Rout (2008), Network Interferences, Available at: http://www.santoshraut.com/ forensic/ cybercrime.htm, Visited: 28/01/2012.
12. www.cyberlawportal.com.