



## CROSS-BORDER CYBERCRIME

Assistant Professor: ZAMAN HAMID HADI  
 University Teacher: HUSSAIN ALAA ABDULSAHIB  
 Assistant Teacher: SULAIMAN DAWOOD SALIM  
 Professors at the College of Law - Al-Iraqia University  
 2022-2023

### **Abstract**

*Electronic piracy is considered one of the electronic crimes sweeping our world today, and it is a crime of a material nature, which is represented in every illegal act or behavior related to any destination or in any way with computers and computer networks, that causes the victim to suffer a loss, and the perpetrator obtains or is able to obtain Any gain. These crimes often aim at stealing information in computer devices, or aim indirectly at the persons and parties concerned with that information. Crime of this kind has several names, including computer and Internet crimes, high-tech crimes, cybercrime, and white-collar crimes. Attacks are often against moral entities related to their strategic value, such as information stores, and this is the most important characteristic that distinguishes cybercrimes from other crimes. It relates to moral entities with material value or purely moral value or both together, and this is its basis without which it is not possible to imagine the existence of an electronic crime, and if it were not for this basis, it would be one of the ordinary crimes that are subject to the criminal law.*

### **Key Words**

- 1- *Electronic piracy: Electronic piracy or software piracy is the practice of downloading or hacking and distributing copyrighted works digitally without permission.*
- 2- *Computer networks: A computer network is a set of computers sharing resources located on or provided by network nodes.*
- 3- *Hacking: Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks.*
- 4- *Cybercrime: Cybercrime is a crime involving a computer or computer network. The computer may have been used in committing the crime, or it may be the target.*
- 5- *Internet: Internet is global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.*

### **INTRODUCTION**

The world has witnessed a great development and a qualitative leap in the way of communication between people, starting with simple means of fire and leaves of trees, leading to a tremendous development in technology represented in the emergence of computers and portable devices and the spread of a huge network of electronic information, which is known as the Internet, which made a



great difference in human life. It brought countless benefits, as this tremendous development brought distances closer, facilitated communication between the parts of the world and formed new friendships and acquaintances outside the family, but hardly anything without gaps and this is the case of that development that led to the emergence of many problems that have become an obstacle to achieving the goals of development and progress, and one of these problems is cybercrime.

Hacking is one of the electronic crimes that are sweeping our world today, and it is a crime of a physical nature, which is any illegal act or behavior associated with computers and computer networks, causing a harm or the possibility of causing harm, and the occurrence or possibility of the perpetrator getting for any gain. These crimes often aim to steal information from computer devices, or aim indirectly at the persons and entities concerned with that information. Crimes of this type have several names, including computer and Internet crimes, high-tech crimes, cybercrime, cybercrime, and white-collar crimes which are attacks on moral entities related to their strategic value, such as information stores, and this is the most important thing that distinguishes cybercrime from other crimes; It is related to the moral entities of material value or purely moral value or both, and this is the basis of which it is impossible to imagine the existence of an electronic crime without it. And its criminal description and the legal text on the criminalization of behavior and the imposition of punishment are of the basics of ordinary crime, and given the development of electronic crimes and the multiplicity of their forms and types as the world went deeper and used the computer, which led to the difficulty of enumerating them and establishing a legal system with a strong and solid foundation to which the information criminal is subject. The investigators' attempts failed, as the crime could be committed with the click of a button. The difficulty of identifying the perpetrator or the inability to know his whereabouts has led to controversy about these cyber-crimes and their forms, and whether they can be limited to certain types. Cybercrime ranges from sniping account numbers and credit cards, to sabotaging websites, posting pornographic images, false websites, money laundering, and espionage. etc. As cybercrimes are actual crimes, there must be legal penalties for them, which we will address in this research.

### RESEARCH AIMS

- 1- Learn about cybercrimes and the stages of their development that reach what they are now.
- 2- Knowing the causes of electronic crimes and the difference between them and traditional crimes.
- 3- Focusing on the factors that can contribute to driving crime levels is in the emergence of global interdependence in the context of the world's economic and demographic transformations.
- 4- Knowing whether the emergence of "cyberspace" creates new phenomena distinct from the existence of computer systems themselves, and the direct opportunities for crime that computers now provide.



5- To identify the possibility of limiting these electronic attacks that invade computers and information systems.

### **RESEARCH PROBLEM**

The problem of the research is related to the fact that there are a number of reasons that can be identified as causes of cybercrimes, some of which occur on a global and international level, some of which occur on a societal level, and some that occur at an individual or personal level. Also, the causes of cybercrimes vary according to their type, target and offender and the level of its implementation: individual, societal, or universal. The crimes of youth, amateurs and young people differ from the causes of professional crimes, and differ according to their goal of stealing, information, trading in information or personal.

### **Chapter One**

#### **What is cybercrime?**

The research into the nature of electronic crime requires defining its concept, elements and stages of development. We will discuss this in three requirements, respectively, as follows:

#### **The first requirement**

##### **The concept of cybercrime**

Hacking is the penetration of computers over the Internet, and this process is carried out by a person or group of people who have extensive experience in computer programs, as they can, through assistance programs, enter another computer and identify its contents.

Some are exposed to hacking e-mail or personal page on social networking sites, which is a breach of privacy and sometimes it is linked to material losses also when banking data is hacked through the Internet. Exposure to such hacking is a wake-up call to ensure the integrity of the antivirus software being used. Relying on free software downloaded from the Internet makes it easier for hackers to work because it does not provide the required protection for the data. (1).

The crime of electronic or information piracy is defined as the process of penetration of computers that takes place over the Internet, often; Because most of the world's computers are connected through this network, or even through internal networks in which more than one computer is connected, and this process is carried out by a person or several people who are skilled in computer programs and methods of managing them; That is: they are high-level programmers who, by means of assistance programs, can penetrate a specific computer and identify its contents, and through which the rest of the devices associated with it in the same network are penetrated. (2)

---

1- Ahmed Al-Mashad, Electronic Piracy and Information Security, The Arab Nation Foundation for Publishing and Distribution 2017, i 1, p. 59.

2- Dr. Jamil Abdel-Baqi Al-Saghir, The Internet and Criminal Law, Dar Al-Nahda Al-Arabiya, Egypt, 1999, p. 25.



## **The second requirement**

### **The stages of development of the crime of electronic piracy**

In this requirement, we will address the stages of the development of the crime of electronic piracy and the most important cases of piracy that have occurred throughout history in two branches, successively, as follows:

#### **First branch**

### **The stages of development of the crime of electronic piracy**

Once, electronic piracy has several stages and has developed historically, as pirates have become filling our world, and this is considered electronic piracy as one of the most important dangers facing our world from our electronic computers, and all our information is subject to piracy by these pirates who found in this process to make a lot of money easily, (1) and follow the development of the Internet With its inception through the wide interaction of users of this network, which led to the development of the first service on this network, represented by e-mail, as well as information items and the information exchange system. However, this development was not immune to criminal behavior, as it was accompanied by the emergence of a technically modern crime. It was later known as the information crime, and the spread of this crime helped the multiplicity of its causes, and this led to the emergence of risks to the information technology contained in the Internet, and the inability to prove this type of crime led to the difficulty of finding appropriate steps to combat it in electronic crimes. (2)

In the mid-sixties, when the Cold War between the Soviet Union and America was at its height, the US Department of Defense (Pentagon) wanted to establish a computer network for the purpose of command and control, as there was a nuclear war between America and the Soviet Union so that the communication between computers would not be interrupted if part of the network was hit and thought Army experts use telephone lines as a network between computers.

---

1- Samir Ibrahim Jamil, Criminal responsibility arising from the use of the Internet, a master's thesis submitted to the College of Law, University of Baghdad, 2005, p. 9.

But it does not achieve the ambition of the US Department of Defense, as hitting the switch leads to the interruption of all communications and the isolation of computers from each other. Therefore, the US Department of Defense referred this problem to the Advanced Research Projects Agency (ARPA).

ARPA was established in 1957 as a reaction to the Soviet Union's success in launching the Sputnik, as it was launched to carry out research devoted to serving the Soviet Union. There are no scientists and laboratories in ARPA, but research is transferred to scientists in universities and companies through contracts and grants (1). (ARPA) referred the issue of establishing a network that would not be affected by the Soviet strikes to universities and companies, as the opinion of scholars settled on developing an idea that the scientist (Paul Barn) from a pioneering company in the early sixties aimed at establishing a system of switching. subnet) (2) so that if a part of the network is hit, the information is transferred through



the remaining switches so that the connection between the computers connected to the network is not interrupted. In fact, the software was completed in January 1969 and the company was ready for segmentation and called the company (ARPA), and in 1983 the network split into two networks, the first network retained its basic name (ARPA NET) and its main purpose, which is to serve military uses, while the second network was named (MIL NET) and was designated for civilian uses, i.e. exchanging information and delivering e-mail, from which the term (Internet) appeared. It was possible to exchange information between these two networks, and in 1986 it was possible to link the networks of five centers for supercomputers and called it (NSF NET), which later became the backbone and the cornerstone for the growth and prosperity of the Internet in America and then other countries of the world (3), and the first service placed on The network is e-mail, and then quickly and growing information banks appeared, then a system for exchanging information and opinions appeared.

---

(1) Samir Ibrahim Jamil Al-Ghazawi, Criminal responsibility arising from the use of the Internet, a master's thesis submitted to the College of Law, University of Baghdad, 2005, pg. 9.

(2) What is meant by the switch here is not the telephone exchange, but rather it is a group of computers called (IMPS) (FACE Message processor INTER) connected to each other through communication lines, Samir Ibrahim Jamil Al-Azzawi, previous source, p. 9.

(3) Muhammad Abdullah Minshawi, the same previous source, p. 1.

Information thanks to the use of a unified protocol for mail, files, information and opinions, as well as data banks (1), and the Internet is a vital part of all business, entertainment and communication activities, and over time it becomes more active and provides more, faster and better services. Several techniques have been developed to work in the Internet environment to provide ease and speed of browsing and renting and to make the pages more attractive, movement and strength (2), and the spread of these technologies has also helped misuse them with some criminals and users, causing security problems on the Internet and the emergence of thieves and intruders and endangering the security of users Putting viruses, destroying files, distorting programs, making backups, scams, and cheating (3).

In 1981 a group of pirates was formed. (4) The Computer Chaos Club in Germany, and the Warlords Group in America which is made up of many teenage hackers, phone hackers, programmers, and a lot of computer hackers who work in the dark. In the summer of 1994, a Russian hacker named Vladimir Levin managed to hack into the American Citibank and transfer ten million dollars from customer accounts to his personal accounts in Finland and Israel. After his arrest, he was sentenced to three years in prison, and the authorities recovered all the stolen money except for four hundred thousand dollars.

In December 2006, NASA was forced to block e-mail messages that come with attachments before the launch of spacecraft for fear of being hacked, and the American magazine "Business Week" reported that plans to launch recent American spacecraft had been obtained by unknown foreign hackers. The Estonian government's computer networks were attacked by an unknown denial of service

attack, after an argument with Russia over the removal of a monument, and some government e-services and Internet banking were disrupted in the attack. Also, that year, hackers managed to break into an unclassified email account of the US Secretary of Defense, in a large series of attacks to gain access to Pentagon computer networks. The efforts of hackers to steal several accounts, websites and electronic files continued to escalate in the past years. The world recorded a lot of major piracy operations, and the largest piracy operations in the world vary from one site to another, but no party denied that the issue of piracy related to the American elections.

(1) Dhar Hassanein Al-Mayahi, legal theories in electronic commerce, lectures at the Faculty of Law, source without numbering.

(2) Abdel Hamid Bassiouni Al Mohandes, same previous source, p. 51.

(3) Abdel Hamid Bassiouni, The Engineer, Hackers' Path and Programs and Information Piracy, Dar Al Katheer Scientific for Publishing and Distribution, Cairo, p. 54.

(4) Same source, pg.32

In 2016, these attempts moved from a mere digital electronic manipulation to a massive global war. (1) Tampering with the elections Controversy escalated in the United States over Russia's accusations of hacking during the American elections, and according to American reports, Washington identified Russian agents responsible for electronic hacking, according to the American network "CNN". The data indicated that these people, whose names were not mentioned, sent Democratic Party emails to WikiLeaks, which publishes leaked documents, in an attempt to influence the vote in favor of Donald Trump and the overthrow of his rival Hillary Clinton. Candidates for the Democratic Party for congressional elections in many states, and Russian electronic hacking has caused an escalation of debate between the president-elect and national intelligence agencies after finding evidence confirming Russian President Vladimir Putin's attempt through intelligence services to distort American democracy, and determine the identity of the winner of the elections. The year 2013 witnessed cyber-attacks on famous websites and applications at different times, such as the New York Times, the Financial Times and its Twitter account, the Washington Post, the "New York Post" page on Facebook, the "Guardian" account on Twitter, the "Reuters feed" account on Twitter, "BBC Weather" on Twitter, "AP" on Twitter, NPR, Viber, Twitter, Tango, Outbrain.

Piracy operations are developing at a very fast speed using modern and complex techniques; Which made the view of it completely changed from what it was in the previous stages.

### Second Branch

#### **The most important cases of piracy crimes that occurred throughout history:**

In 1986, Roberto Soto stole a government telex line; To send a series of messages through it to banks in the United Kingdom, and from there to other countries, and these messages resulted in the transfer of 13.5 million dollars from the balances of the Colombian government.

In 1988 a Corle University student implanted Worm into a government computer network that spread to 6,000 computers.





A group of Russian hackers transferred \$10 million from City Bank to bank accounts around the world in 1994

- (1) Dr. Hisham Muhammad Farid Rostom, Penal Code and Information Technology Risks, Library of Modern Machines, 1992. p 58

## Chapter Two

### The negative effects of the electronic piracy crime on the national economy

#### First: the negative effects on the national economy

Cyber-piracy has a negative and significant impact on the economy as it threatens global financial stability, especially if it targets global financial institutions, such as major global banks. Altogether, and lead to a state of financial chaos, and may lead to the collapse of stock exchanges and financial markets, which leads to exorbitant financial losses for countries, and questioning their security system, especially if these attacks affect deposits and payments of individuals, who may rush to recover their money or cancel their accounts. banking. (2)

It also contributes to the escalation of trade and economic wars, especially as these electronic attacks sometimes penetrate the information systems of countries, and accordingly obtain some secrets and sensitive economic information, for example, the trade war between China and the United States, which erupted since the era of former US President Donald Trump. And it still exists under the administration of President Joe Biden, as it is mainly due to Washington's accusation of Beijing of stealing the secrets of American products and industries, and trying to imitate them and invade major markets with them, and then indirectly hit the American economy. Evidence of this is President Joe Biden's decision to extend the ban imposed by former President Donald Trump on Americans investing in Chinese companies linked to the Chinese military, in a clear indication that the United States is

---

(1) Samir Ibrahim Jamil Al-Azzawi - Criminal responsibility arising from Internet abuse - Master's thesis submitted to the Baghdad University Council, 2005 - p. 39.

(2) Abdul Rahman Al-Bahr, Obstacles to Internet Crime Investigation. Unpublished Master's Thesis." Riyadh, Naif Arab Academy for Security Sciences 1999, p. 21.

worried about Chinese companies. Perhaps it is remarkable in this context that Biden's decision has increased the number of Chinese companies prohibited from investing in them from 48 to 59 companies, in addition to that this decision also includes companies that develop and assist the Chinese government in the surveillance technology that it exercises on citizens, such as the technology used against Muslim minorities such as Uighur Muslims and opponents in Hong Kong, and many countries of the world resort to electronic attacks, as one of the important tools in modern wars, which mainly rely on electronic weapons, which are employed in a first strike on the enemy's computers, or even by targeting civilian life and infrastructure. Informatics, security and strategy experts point out that countries that have advanced technological infrastructure have greater chances of achieving broad electronic dominance if they enter into a war or conflict of interests with any other countries. Instead of using traditional military tools, it is



possible by pressing the panel. The keys are to destroy the information infrastructure in the targeted countries, and to achieve destructive effects that exceed those in which military force is used, as a cyber attack can be launched targeting closing vital sites and paralyzing command, control and communications systems, cutting communication networks between units and central commands, disabling air defense systems, derailing missiles, controlling air and sea navigation lines, penetrating the banking system and harming the operations of banks and financial markets. All of these actions affect the economy and their impact is considered a negative impact. (1)

#### **Second: the negative effects on investment**

The crime of electronic piracy has significant negative effects on investment within the state. This cross-border crime, if not faced with a proper legislative regulation, may push investment companies, especially multinationals, to avoid investing and working within the state because we are not confronted by legislation and therefore the lack of legal protection for these companies, and the negative effects of piracy appear. electronic investment through the following:

1. Using special programs to embezzle funds: This is done through specific programs aimed at making money transfers from one account to another, whether from the same bank or from another.

---

(1) Adel Abdel Sadiq, *America and the formation of a military leadership in cyberspace*, Cairo, Al-Ahram Center, 2009, p. 22.

Another bank, provided that this is done at a specific time determined by the program designer. One of the most famous examples of this is that one of the workers in the computer center contracted with the Commercial Bank of Kuwait to develop information systems seizes huge amounts of money from the bank after he was able to choose five dormant accounts in five local branches of the bank. A program was prepared for her, whose mission was to transfer certain amounts from these accounts to other accounts opened in his name in the same branches, provided that the transfer process takes place while he is on the plane taking him to Britain back home after the expiry of his work contract. Then he opens other accounts upon his arrival and asks the bank to transfer these amounts to his new accounts in Britain (1).

2. Direct transfer of balances: This is done through hacking computer systems or passwords. A famous example of this is that an expert in the field of computers in the United States of America hacked the information system of a bank and transferred an amount of (12) million dollars to his own account in three minutes, and this is usually also done by entering false information and creating fake accounts and salaries and transferring it to the offender's account, and direct transfer can be done by capturing radiation from the device if the information system is connected to a network that operates via satellite, if there are systems that use prints. Fast emitting electromagnetic radiation during its operation. It has been proven that it can be intercepted and captured during the transmission of waves, deciphering them by means of a special device to decipher codes and re-





broadcast them again after being modified. This is what Article (5) of the Budapest Convention mentioned (2).

3. Manipulation of financial cards: This type of electronic crime appeared by capturing the secret numbers of credit cards and various loyalty cards from ATMs for money until the ATM appeared. As for the crimes of assaulting these cards, they are used by someone other than the official card holder after Theft or stealing of their secret numbers, and then hacking some commercial sites in which the credit card may be registered, and in this type of crime there is no difficulty in

---

(1) Abdullah Daghash Al-Ajmi, Practical and Legal Problems of Cybercrime - A Comparative Study, Master's Thesis, Middle East University, Amman, 2014, pp. 49-50.

(2) The same previous source, p. 51.

Applying the legal texts related to theft or fraud, whether the person of the card holder or the ATM was attacked. (1)

4. The seizure of electronic money: The monetary value of these currencies is shipped on a plastic card or on the hard disk of the consumer's personal computer, and thus it differs from credit cards, as it is closer to tourist instruments than credit cards, meaning that it is a floating entitlement on financial institutions that takes place between two parties: The merchant and the customer, without the intervention of a third party, it is a set of protocols and digital signatures that allow electronic messages to replace the exchange of cash, and therefore the crimes committed against them are represented in the process of seizing the plastic card or the computer hard drive charged to it (2).

We conclude from the foregoing that if it is possible to confront the previous crimes through the special provisions in the Penal Code No. (111) of 1969 as amended that regulate the crimes of theft, fraud and fraud, the nature and privacy of these crimes requires a special law for them, especially since the aforementioned law was initiated at a time when These crimes did not exist, and that is why we call on the Iraqi legislator to enact a law on cybercrime and tighten penalties for perpetrators in order to reassure investors and encourage investment in Iraq in order to achieve development.

### **Chapter Three**

#### **Ways to reduce cybercrime:**

Day by day, the risks of information crimes are increasing and their scope is expanding to include all public life facilities and began to threaten the global economy as a result of the great losses resulting from them. their electronic systems (3).

---

(1) Abdullah Daghash Al-Ajmi, previous source, pp. 51-52.

(2) See: Dr. Abdel Fattah Hegazy, The Computer and Internet Struggle, House of Legal Books, Cairo, 2007, 609.

(3) Mohamed, Moulay 2010: Difficulties of applying electronic management in Algeria: Cybercrime as a model, the First International Conference on Electronic Management, City Center for Multimedia, 01-03/06/2010, Tripoli, Libya, p. 11.



What is worrying is that many countries, including Iraq, do not yet have an explicit legislation criminalizing the phenomenon of piracy, with some attempts to issue a unified Arab law regarding information crimes in all its branches. Piracy and hacking crimes, and this does not mean that there are no information crimes, but that quite a few Iraqi websites are attacked annually, especially the websites of news agencies and government websites, and the reason for not filing lawsuits is due to the difficulty of knowing the perpetrator. Therefore, we will divide this topic into two demands as follows:

### **The first requirement**

#### **Reducing the crime of piracy in the legislation of some countries of the world**

If we looked into the legislation of the developed countries of the world, we would have found many texts that punish piracy crimes and penetration of electronic systems, while many other countries still live in complete electronic darkness, so we do not see any legislation related to this type of crime (1) in the State of Sweden, for example:

Article (21) of Law No. (289) issued on April 2, 1973 concerning data states that “anyone who has illegally accessed a registry designated for automatic data processing shall be punished. Denmark, according to Article (263) of the law issued on June 1, 1985 - it is considered a crime to access information or programs stored in computers, as well as France introduced the French law issued on January 5, 1988 under Article (462), the second paragraph of the Penal Code, The crime of illegal access to information systems, which was amended by the law issued on March 29, 1993 in Article (331), the first paragraph of the Penal Code, which states: “Whoever is present or stays in an irregular manner, shall be punished by imprisonment for a period of one year and a fine of up to one hundred thousand francs. A project in an automated treatment system, whether in whole or in part, and the penalty is increased by imprisonment

- (1) Al-Badayna, Diab Mousa (2014), “Electronic Crimes: Concept and Causes”, Scientific Forum on New Crimes in the Light of Regional and International Changes and Changes during the period from 02-04/09/2014, College of Strategic Sciences, Amman, Jordan, p. 28.

for a period of two years and a fine of (200,000) francs, if this results in the cancellation or modification of the data contained in this system or due to the different function of this system, and England:

In 1990, a law was introduced dealing with the misuse of information systems. Under this legislation, the process of accessing any person to data stored in a computer or software was criminalized, as well as the process of illegally modifying it or any attempt to do so. The law stipulated three crimes, namely:

- 1- Intentional unlawful entry.
- 2- Illegal entry, which takes place with the intention of committing many crimes.
- 3- Doing any intentional act that results in an unlawful modification of the contents of computer equipment.

The same is the case in the United States of America, where the Artificial Computer Access Law was issued in October 1984, which punishes whoever intentionally accesses a computer without permission or was permitted, and takes

advantage of the opportunity given to him for purposes not covered by the permission, and intentionally, through this means, uses, alters, or destroys Or disclose information stored in the computer whenever the latter is working for the US government and as long as these actions affect the performance of his job. (1)

### **The second requirement**

#### **The role of laws and legislation in reducing cybercrime in some Arab countries (2)**

The delay in the use of computer technologies in the Arab countries compared to the rest of the world may have a significant impact on the delay in issuing legislation regarding providing legal protection for computer programs from theft and penetration.

However, most Arab countries paid much attention to intellectual protection laws, to the extent that some of them have contributed significantly to the international effort to protect intellectual property since the nineteenth century.

---

(1) Al-Bushri, Mohamed Al-Amin (2008), (The Internet and Terrorism: Qualifying Investigators in Computer and Internet Crimes), Cairo: Ain Shams University, p. 45.

(2) Shaaban, Samir (2009) Cybercrime, an analytical approach to defining the concept of crime, International Forum on Legal Regulation of the Internet and Cybercrime during the period from 27-28/04/2009, University of Djelfa, Algeria, p. 67.

The fifties of the last century witnessed a wide wave of legislation concerned with the protection of patents, trademarks and industrial designs, and the eighties witnessed the issuance of legislation related to the protection of copyright and related rights. As for the nineties, it witnessed the adoption of laws or the amendment of previous laws to include computer programs and databases. The following are some examples of such legislation.

In Iraq, the (dissolved) Coalition Provisional Authority issued Order No. (83) for the year 2004, which is an amendment to the Copyright Law No. (3) for the year 1971, where one of its paragraphs included (computer programs, whether with source or machine code that should be protected as literary works.

As for Egypt, it was stipulated in Law No. (38) for the year 1992, which is an amendment to Law No. (354) for the year 1954, in which intellectual protection includes computer works, including programs, databases and the like. As for the UAE, Law No. (40) for the year 1992 Article Two (Enjoy the intellectual protection established in this law authors of innovative intellectual works in literature, arts and sciences - Paragraph (g) of this law included computer programs. As for Jordan, it was mentioned in the Copyright Law No. 22 of 1992 and its amendments for the years 1998, 1999 and 2001 legal protection for literary and artistic works, as well as ensuring the protection of computer programs and databases. As for Lebanon, it stipulated in Law No. 2385 of 1924, as amended by Law No. (75) of 1999, that it protects all productions of the human mind, which were specified in Article Two of computer programs, regardless of their languages. Including the preparatory work. (1)

### **CONCLUSION**

At the end of this research, our aim is to shed light on cybercrime in cyberspace, the reasons behind the crime, and to suggest some solutions that would reduce and



combat this phenomenon. The study, the research confirmed that the real driving reasons

(1) Mustafa Saadoun, Salman Mahmoud, Abdul Rahman Hassan (2011), "Cybercrime via the Internet, its impact and ways to confront it", Technical College, Kirkuk, Iraq, p. 35.

### **Conclusions:**


- 1 - Legislations and laws are an important factor in confronting cybercrime (information) that is committed in cyberspace.
- 2 - Lack of experience among workers in the information security sector causes cybercrime
- 3 - Lack of attention to devices for digital forensic expertise enables categories of information criminals who have the skill, knowledge and intelligence to commit information crimes.
- 4- The failure of educational institutions and civil society to play their awareness and preventive role in combating these crimes.
- 5- Judicial bodies lack experience in preparing qualified judicial and control systems in dealing with cybercrime.
- 6- Combating information crimes in Libya is still without legislative cover that defines it and criminalizes all its forms.
- 7- Weak international cooperation to combat cybercrime, especially among Arab countries.

### **RECOMMENDATIONS:**

- 1- The necessity of the legal legislator's intervention to confront the cybercrime (information) that is committed in the cyberspace.
- 2- Qualifying and training workers in the information security sector in financial organizations in order to protect the electronic system, and to deal professionally with information and communication technology.
- 3 - Activating the devices related to the criminal expertise of cybercrime (information), whose members consist of a technically specialized team in communications and information technology, because proving cybercrime requires special rules for dealing with evidence in these crimes.
4. Work to reconsider the university curricula, and the necessity of including a general article on computers and information networks and how to deal with electronic devices.
5. We call on the Iraqi legislator to enact a law on cybercrime and tighten penalties for perpetrators in order to reassure investors and encourage investment in Iraq in order to achieve development.

### **REFERENCES:**

- [1] Ahmed Al-Mashad, Electronic Piracy and Information Security, Arab Nation Foundation for Publishing and Distribution 2017, first edition.

- 
- [2] Obesity, Diab Moussa (2014), (Electronic Crimes: Concept and Causes), Scientific Forum on New Crimes in the Light of Regional and International Changes and Changes during the period from 02-04/09/2014, College of Strategic Sciences, Amman, Jordan.
- [3] Al-Bishri, Mohamed Al-Amin (2008) "The Internet and Terrorism: Qualifying Investigators in Computer Crimes and Internet Networks", Cairo: Ain Shams University.
- [4] Cybercrime, by the author: Mustafa Samara - Informatics magazine, issue 29 - July 2008.
- [5] Hassanein Al-Mayahi, Legal Theories in Electronic Commerce - Lectures given to graduate students at the Faculty of Law - Al-Nahrain University 2018.
- [6] Dr. Jamil Abdel-Baqi Al-Saghir - The Internet and Criminal Law - Dar Al-Nahda Al-Arabiya - 1999.
- [7] Dr. Abdel Fattah Hegazy, The Computer and Internet Struggle, House of Legal Books, Cairo, 2007.
- [8] Dr. Hisham Muhammad Farid Rostom - Penal Code and Information Technology Risks - Library of Modern Machines - 1992.
- [9] Samir Ibrahim Jamil - Criminal responsibility arising from the use of the Internet - a master's thesis submitted to the College of Law - University of Baghdad - in 2005.
- [10] Samir Ibrahim Jamil Al-Ghazawi - Criminal responsibility arising from the use of the Internet - a master's thesis submitted to the College of Law - University of Baghdad - in 2005.
- [11] Shaaban, Samir (2009) Cybercrime, an analytical approach to defining the concept of crime, International Forum on Legal Regulation of the Internet and Cybercrime during the period from 27-28/04/2009, University of Djelfa, Algeria.
- [12] Adel Abdel Sadiq, America and the formation of a military leadership in cyberspace, Cairo, Al-Ahram Center, 2009.
- [13] Abdel Hamid Bassiouni, The Engineer, Hackers' Path and Programs and Information Piracy, Dar Al Katheer Al-Alamia for Publishing and Distribution, Cairo.
- [14] Abdullah Daghash Al-Ajmi, Practical and Legal Problems of Cybercrime - A Comparative Study, Master's Thesis, Middle East University, Amman, 2014.
- [15] 15- Mohamed, Moulay 2010: The Difficulties of Applying Electronic Management in Algeria: Cybercrime as a Model", the First International Conference on Electronic Management, City Center for Multimedia, 03/01/06/2010, Tripoli, Libya.
- [16] Mustafa Saadoun, Salman Mahmoud, Abdul Rahman Hassan (2011), (Cybercrime via the Internet, its impact and ways to confront it), Technical College, Kirkuk, Iraq.
- [17] Mustafa Alawi, The concept of security in the post-Cold War era, Cairo, 2004.